CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76506 CARLOS EDUARDO ANTAO
24CC2504 - 1 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 375,3127), Bento=(1433,5893)`
   `Carlos=( 587,3053), Dante=(1267,6499)`
   `Erasmo=(1213,3763), Frida=( 197,1457)`
2. Sua chave pública é (287,1517)
   * e sua chave secreta é (863)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de dante
   Mensagem:
   ```
   4265 5354 4989 5610 5354 4265 3066  285 4047 6174
   3672 4265 5354 6099 4246  285 5354  522  285 4246
   4989 5354 3066  198  285 5354  522  285 3672 6025
   5610 4246
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para erasmo
   Mensagem:
   `NO/CENTRO/DA/TABA/SE/ESTENDE/UM/TERREIRO`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
    435 1117 1192 1040 1117  723 1180 1117 1197 1040
   1117  116  348  808 1040  907 1040  723 1364  899
   1040 1470  907 1040  116  907 1117 1040  435  100
    116 1140  100  723  907
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `A/DURA/CORDA/QUE/LHE/ENLACA/O/COLO`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[18]	A[32]	B[9]	B[40]

C[1]	C[35]	D[25]	D[34]

504-76506 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76663 DANILO DEPETRIS SOARES
24CC2504 - 2 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 577,4183), Bento=( 739,3827)`
   `Carlos=( 427,3127), Dante=( 247,1829)`
   `Erasmo=( 331,1763), Frida=( 503,4171)`
2. Sua chave pública é (1093,3403)
   * e sua chave secreta é (3277)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de erasmo
   Mensagem:
   ```
    285  416  127  868  390  594  262  416  390 1486
   1350  416 1350  285  390  416  127  479  364  479
    416  262  416  479  390  594  485  285 1218 1057
    262  416  479  416  390  285  568  556  262
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para alice
   Mensagem:

   `E/AS/DURAS/FADIGAS/DA/GUERRA/PROVEI`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   3262 1336 2967 3262 2329 2745 2329  897 1588 2745
   1336 1588 2998 2967 2866 1072 3262 2866  897 1588
   3262 2866  981 1336 2967 2998 2866  897 1588 2745
   1336 1588 2185 2676 2866 2967 1336  897
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

   `LEDO/CAMINHA/O/FESTIVAL/TIMBIRA`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[33]	A[39]	B[1]	B[35]

C[1]	C[38]	D[22]	D[31]

504-76663 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76513 EDUARDO CAVALHEIRO DIAS
24CC2504 - 3 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

☞ Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 463,2419), Bento=( 433,3149)`
   `Carlos=( 205,1739), Dante=( 297,2173)`
   `Erasmo=(1123,8051), Frida=( 401,3337)`
2. Sua chave pública é (729,5251)
   * e sua chave secreta é (5097)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de dante
   Mensagem:
   ```
   654  730 2061 1507 1533  654  730 2061  673 2168
   515  220  108  730 2061 1445  220  673 2061 2168
   673  108  730 2061  875  730 1533 2168 2061 1397
   108  673 1507  673 2061  654  119
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para erasmo
   Mensagem:
   `QUE/FOI/TUPA/MANDOU/QUE/ELE/CAISSE`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   2057 2583 3889 3911  987 3806 1705 2583 1705 2100
   3806 5220 1705 2583 1705 2734 5145 2716 1516 2716
   1705 4343  987 2057 5008  987 1705  987 1705 3911
   5041 2822 4211  987
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `DA/SUA/NOITE/LUGUBRE/E/MEDONHA`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[21]	A[37]	B[6]	B[34]

C[11]	C[34]	D[6]	D[30]

504-76513 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76520 ERIC CORDEIRO
24CC2504 - 4 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 431,3139), Bento=( 367,1927)`
   `Carlos=( 463,2911), Dante=( 193,1643)`
   `Erasmo=(1433,5893), Frida=(1687,8633)`
2. Sua chave pública é (1117,6887)
   * e sua chave secreta é (373)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de frida
   Mensagem:
   ```
   8206 6677 6963 6042 5994 7345 2015 8239 5994   13
   4711 7306 8430 6677 5994 8239 5994 6042 8239   15
   5994 5345 4711 6963 7716 6677 5994 8239 5994 6042
   8239   15 5994   13 7306   15 6963 5813 6963 7306
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para bento
   Mensagem:
   `ASSIM/LA/NA/GRECIA/AO/ESCRAVO/INSULANO`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   1232 2722 4129 3514  656 4129 5806 6641 3508  578
   3508 4129 3995 3514 2722 6641 6641 2722 4059 6641
   3508 4129  578 3508  656 4129 3969 3514 2722 4129
    656 2722 4129 2722 5794  578 3508 5794 5806 6641
   3508
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `SOLTO/APENAS/DOS/NOS/QUE/O/SEGURAVAM`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[24]	A[40]	B[26]	B[38]

C[18]	C[41]	D[25]	D[36]

504-76520 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76537 FELIPE EIJI KANO
24CC2504 - 5 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa
$(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

☞ Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 415,2183), Bento=( 261,1927)`
   `Carlos=( 851,4399), Dante=( 367,1927)`
   `Erasmo=( 607,3149), Frida=( 849,5251)`
2. Sua chave pública é (545,3953)
   * e sua chave secreta é (3533)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de dante
   Mensagem:

```
   69 1554   87 1828  541  413 1285 1554   87 1828
  413 1465   87 1773  955  221   69 1713 1554   87
 1828  130 1554  193 1828  221   69 1220  221 1554
   87 1828 1704  541  413  221   69 1713 1554   87
```

   Qual é a mensagem ?

   A=_____.

   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para erasmo
   Mensagem:

   `ORA/NAO/PARTIREI/QUERO/PROVARTE`
   B=_____.

   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:

```
 1679 1051 2668 3506   53 2668 1679 1051 2486 2839
  227 1051 3705 1679 1051  370  227   53 1679  370
 1051   53  227  370  370 3705 3359 3705 1051 1679
 2440 1051 1679 2155 3146 1679 2440
```

   C=_____.

   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

   `GUERREIROS/DESCENDO/DA/TRIBO/TUPI`
   D=_____.

   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[29]	A[40]	B[28]	B[31]

C[15]	C[37]	D[21]	D[33]

504-76537 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76544 FELIPE JESMIEL LEITE
24CC2504 - 6 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 331,2449), Bento=(1093,3403)`
   `Carlos=( 613,2573), Dante=( 733,3053)`
   `Erasmo=( 271,2279), Frida=( 811,4187)`
2. Sua chave pública é (613,3827)
   * e sua chave secreta é (205)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de bento
   Mensagem:
   ```
   1542 2470 1544  193 2222 1541 3175 1673 2222  835
    193 2136 2470  588  193  283 1124  835  193 2470
   1673  193 2127 1823 3175 1544 2470 1673  193 1542
   2470 1544 2470 2136  835
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para dante
   Mensagem:
   `E/TU/CHORASTE/PARTE/NAO/QUEREMOS`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
    347 1380 1952 2930 3153 1798 2930  244 2392 1380
    244 1798 3753 1380 3153  299 1380  244 3685 2072
   2930  244 3073 2930  599 2392  347  347 2392  244
   1380  347  244 2392 3753 2930  347
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `MEDROSOS/DAS/GUERRAS/QUE/OS/FORTES`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[11]	A[35]	B[17]	B[32]

C[21]	C[37]	D[22]	D[34]

504-76544 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76551 GABRIELA BERNARDO PASQUALOTTO
24CC2504 - 7 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto

Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \ \Rightarrow \ b^x \equiv a \ mod \ n$$

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

☞ Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 951,4897), Bento=(1025,5293)`
   `Carlos=(1525,4717), Dante=( 603,3763)`
   `Erasmo=( 791,4897), Frida=( 841,6059)`
2. Sua chave pública é (303,1927)
   * e sua chave secreta é (1087)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de bento
   Mensagem:
   `3805 2499 5205 4037 3117 2467 1482 942 5205 3981`
   `3711 1965 5022 942 3117 2499 5205 3805 2499 3981`
   `5205 4037 3117 2467 1482 942 3981 5205 3981 3711`
   `3117 371 2467 3981`

   Qual é a mensagem ?

   A=_____.

   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para frida
   Mensagem:

   `EM/NOSSOS/CORPOS/RESTA/MAS/TU/TREMES`
   B=_____.

   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   `1014 1541 1461 480 488 791 619 488 1541 488`
   `1541 1727 1014 791 1541 679 1238 673 488 480`
   `1541 1621 1238 1541 1727 1656 1545 1922 488 1541`
   `1238 430 488 480 1238`

   C=_____.

   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

   `CAMINHA/O/TIMBIRA/QUE/A/TURBA/RODEIA`
   D=_____.

   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[7]	A[34]	B[9]	B[36]

C[21]	C[35]	D[23]	D[36]

504-76551 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76737 GRAZIELLY A. L. VALICOSKI
24CC2504 - 8 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 281,2077), Bento=( 377,2747)`
   `Carlos=( 797,2491), Dante=( 375,3127)`
   `Erasmo=( 471,3901), Frida=(1123,8051)`
2. Sua chave pública é (733,5293)
   * e sua chave secreta é (2725)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de bento
   Mensagem:
   ```
    181  978 1486 1163  279  978 2301 1308 2553  978
    279 1308 2553  925  665  181 2604 1308 2553 1486
   1163  279  235 2553  487  181  526  279 2553 1720
   1902 1544  181 1902
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para alice
   Mensagem:
   `POR/CASOS/DE/GUERRA/CAIU/PRISIONEIRO`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
    760 3197  262 5128  211 3902 1718  760 3197 1946
    211 1783 4407  760 1783 3988  760 3197 5128  760
   5285 1724 4407  760 3197 1783  760 3798 3902 1724
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `SOLTAI/O/DIZ/O/CHEFE/PASMA/A/TURBA`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[28]	A[34]	B[9]	B[36]

C[22]	C[30]	D[17]	D[34]

504-76737 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76568 GUILHERME VITOR DA SILVA
24CC2504 - 9 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

☞ Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 691,3589), Bento=( 811,4187)`
   `Carlos=( 695,2183), Dante=( 583,2449)`
   `Erasmo=( 377,2747), Frida=( 433,1829)`
2. Sua chave pública é (501,3127)
   * e sua chave secreta é (301)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de erasmo
   Mensagem:
   ```
    181 2553  925 1308 2638 2553  665 1308  978 1830
    279 2553 2638  279 1902 1308 1830 2553  487  181
   2553  279  925  279  487 1308 2553 1308 2553 2081
    181  978  925  181 2638
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para alice
   Mensagem:
   `ENTAO/FORASTEIRO/CAI/PRISIONEIRO`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   2345 1897 2700 2345 2116 1157 3046 2045 1157 2843
     86 3064 1457 3064 3019 1157 1226 2045  230 2345
   1931 2116 1157 2045 1226 2045 1841 2045 1457
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `JA/CEGO/E/QUEBRADO/QUE/RESTA/MORRER`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[30]	A[35]	B[12]	B[32]

C[13]	C[29]	D[20]	D[35]

504-76568 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76706 KAWAN DAIKI HASEGAWA
24CC2504 - 10 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa
$(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 905,6497), Bento=(1405,8633)`
   `Carlos=(1285,5293), Dante=( 433,1829)`
   `Erasmo=( 493,2077), Frida=( 571,3569)`
2. Sua chave pública é (347,2537)
   * e sua chave secreta é (695)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de bento
   Mensagem:
   ```
   7341 7004 7605 7692 3095 6358 3579 6773 4080 2088
   4080 3579 8383 3126 6358 5261 4080 2088 3579  598
   2088 4458  598 7004 5261  598 2088 7692 3095 4080
   2088 4458 7605 3579 1825 4080 2792
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para carlos
   Mensagem:
   `QUASE/BRADAR/LHE/OUVIA/INGRATO/INGRATO`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   1788  423  279  520  786  423  786  534  423  832
    786  423  786 2228   51 2131 1446  786  908   51
    423  786 2482  520  534  786 1446  725  109  832
   2397  423
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `AQUI/VOS/TRAGO/PROVISOES/TOMAI/AS`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[9]	A[37]	B[18]	B[38]

C[29]	C[32]	D[26]	D[33]

504-76706 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76575 LAURA PACHECO DELATTRE
24CC2504 - 11 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

☞ Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 677,5609), Bento=( 829,5963)`
   `Carlos=( 313,1333), Dante=( 379,3149)`
   `Erasmo=(1173,3649), Frida=( 595,4307)`
2. Sua chave pública é (287,1517)
   * e sua chave secreta é (863)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de bento
   Mensagem:
   ```
   1097  488  332  787 4432 1070 4681  488  787 1097
   4685 1097 4603  631  787 4685  332  787 4603 3543
    488 2845  488  787 4681  631 4476  787 1775  631
   2430  787 1070 4476 4681  488  332
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para erasmo
   Mensagem:
   `AS/SETAS/DA/AFLICAO/JA/SE/ESGOTARAM`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
     907 1117 1197 1040  348 1364 1260 1117 1197 1040
     125 1364  808 1260 1260  808  100 1260 1117 1197
    1040 1197 1364 1470  808  100 1140 1117 1197 1040
     116  907 1040  505  907  899
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

`COMO/QUE/POR/FEITICO/NAO/SABIDO`
D=_____.

Dica: codifique com a sua CS
Agora responda as questões, usando A, B, C e D calculados acima

A[7]	A[37]	B[8]	B[35]

C[35]	C[36]	D[24]	D[31]

504-76575 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76694 LAURO HENRIK RUTZ
24CC2504 - 12 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 817,5893), Bento=(1597,6557)`
   `Carlos=(1213,3763), Dante=( 901,4661)`
   `Erasmo=( 849,5251), Frida=(1349,4183)`
2. Sua chave pública é (487,3053)
   * e sua chave secreta é (163)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de erasmo
   Mensagem:
   ```
   1808 1737 1399 1737 3829 1399 1116 4675 2527 1549
    449 1737 1808 1737  785 1399 1737 3965 1399 1500
   5153 1399 2830 3965 1808 1737 1116  756 4675 3965
    449
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para frida
   Mensagem:
   `DA/TRIBO/PUJANTE/QUE/AGORA/ANDA/ERRANTE`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   2084 1145 1147 2185 2807 1787  263 1165 1147  605
   1941 1605 2003 1165 2807 1145 1147 2084 1145  605
   1147 2185 2807 1787  263 1165  605 1147  605 1941
   2807 1674 1787  605
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `NAS/MAOS/DOS/TIMBIRAS/NO/EXTENSO/TERREIRO`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[8]	A[31]	B[9]	B[39]

C[18]	C[34]	D[6]	D[41]

504-76694 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76582 LUIZ MIGUEL OLINEK
24CC2504 - 13 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 653,3403), Bento=( 753,3901)`
   `Carlos=( 551,2881), Dante=( 517,1643)`
   `Erasmo=( 271,1457), Frida=( 661,3431)`
2. Sua chave pública é (239,1517)
   * e sua chave secreta é (1199)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de frida
   Mensagem:
   ```
   1420 3340 2758 3190 1041  774 1041 1236 1041 2403
   1158 1419 1158 2995 1236 1249 3041 3340 1778 1420
   1041 1236 3340 1236 1158  929 3340 1249 1041  929
   1236 1206 1158 1206 3340
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para bento
   Mensagem:
   `GUERREIROS/NAO/CORO/DO/PRANTO/QUE/CHORO`
   D=_____.
   Dica: codifique com a sua CS
   Agora responda as questões, usando A, B, C e D calculados acima

A[9]	A[35]	B[24]	B[30]

C[3]	C[32]	D[27]	D[39]

504-76582 - gar a

5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
    279  253  965 1054  253  790 1374 1351  965  792
   1374  224 1374  279  551  965  416 1062  792 1192
   1374   66 1374  965 1351  253  965  253 1192  965
   1192 1062
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76599 NICOLE DA SILVA DE AZEVEDO
24CC2504 - 14 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 757,3149), Bento=( 935,7663)`
   `Carlos=( 595,4307), Dante=( 677,4891)`
   `Erasmo=( 757,3149), Frida=( 673,4183)`
2. Sua chave pública é (953,6887)
   * e sua chave secreta é (3977)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de dante
   Mensagem:
   ```
   1890 3070 4044 3443 4485 1494 3928 4485  337 1494
   3255 4485 2068 4485  337 1494  547 4504 1644 1494
   4044 4485  337 3433 1644 3443 1494 3255 1644 1494
    663 4589 3443 4485 1201
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para carlos
   Mensagem:

   `ENQUANTO/DESCREVE/O/GIRO/TAO/BREVE`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   1818 3641 3641 5050 4254 1818 5883 3641 5933 5883
   5050 5883 4045 5933 4045 5050 5883 1728 2253 5933
   5883 5050 5883 4045 5933 6555 5933 5883 5933  401
   5883 6688  515 1612 3641 1818 5050
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

   `O/ACERBO/DESGOSTO/COMIGO/SOFRI`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[9]	A[35]	B[33]	B[34]

C[30]	C[37]	D[22]	D[30]

504-76599 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76601 PAULO JOSE FREIRE CORREA
24CC2504 - 15 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 311,1961), Bento=(1129,4661)`
   `Carlos=( 583,2449), Dante=( 673,4183)`
   `Erasmo=( 713,5141), Frida=( 401,3337)`
2. Sua chave pública é (877,2759)
   * e sua chave secreta é (2053)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de carlos
   Mensagem:
   ```
   1837  820   12 1743 1756 1661 1756 1837 1728  285
   1756 1743 1837  820 1225   52 1811 2019  820  112
   1837 1743  166  285  820 2019 1728 1661  285 1756
   2019  112  820 1661  285 1728  166 2019  873 1837
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para frida
   Mensagem:
   `CAMINHA/O/TIMBIRA/QUE/A/TURBA/RODEIA`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   2243  640 1507  389  640  193  345 1223 2361  640
    604 1223 1558 1223  640 2441 2361  640 1558 1223
   1773 2441 2243 1773  193 2441 1773  388  640 2361
   1558
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `NOS/RESTA/DE/SOFRER/QUE/NOVAS/DORES`
   D=_____.

Dica: codifique com a sua CS
Agora responda as questões, usando A, B, C e D calculados acima

A[35]	A[40]	B[15]	B[36]

C[20]	C[31]	D[28]	D[35]

504-76601 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)

VIVXq84a V: 1.02

76618 PEDRO HENRIQUE PIEKARSKI DE OL 24CC2504 - 16 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=(2405,7387), Bento=( 277,1763)`
   `Carlos=( 713,5141), Dante=( 259,2183)`
   `Erasmo=( 985,7081), Frida=( 395,2881)`
2. Sua chave pública é (1147,5893)
   * e sua chave secreta é (3443)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de carlos
   Mensagem:
   ```
   2691 4234 2147 3217 2515  262 1321  903 1073 2380
   2691 4234 2129 1053 2691 2953 1321 4576 3217 2301
   4234 4576 1073 4234  903 1073 2380  262 1073 4234
   2515 2691 4234 2343  903 1073 2515  262 3217
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para erasmo
   Mensagem:
   `AO/VELHO/COITADO/DE/PENAS/RALADO`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   1515 2848 2645 5279 3943 2848 1995 5279 1010 1995
   5107 2276 2848 5279 1021 4036 1021 2848  884 1995
   5279 1010 1995 4036 1692 2848 2276 1021 3943 1995
   1010 1995 3656 1010 2276 2276 2848 2276
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `CUIDOSOS/SE/INCUBEM/DO/VASO/DAS/CORES`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[38]	A[39]	B[20]	B[32]

C[11]	C[38]	D[11]	D[37]

504-76618 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76625 RAUL KNAPKI CUNHA
24CC2504 - 17 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

☞ Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 577,4183), Bento=( 761,4717)`
   `Carlos=( 587,3053), Dante=( 983,3071)`
   `Erasmo=(1443,7387), Frida=( 533,2773)`
2. Sua chave pública é (1081,5561)
   * e sua chave secreta é (3865)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de dante
   Mensagem:
   ```
   773    3 2804  512  779 1033  773    3 1234  773
     3  512 1234    4   42 1234    4  773    3 2461
   773 1008  533  512 1234  797  773    3 1396   42
     3    4   42 1234    4  773
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para alice
   Mensagem:
   `A/DURA/CORDA/QUE/LHE/ENLACA/O/COLO`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   1119  936  697 3838  657 4924  936 2927 1323  594
   3838 1323 3838 2927 3025 1356 2504 2002  936 2927
   1323 1119 2002 3838 2723  564  801  936 2927 1323
    564  245 2675 1356
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `LEDO/CAMINHA/O/FESTIVAL/TIMBIRA`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[7]	A[36]	B[20]	B[34]

C[10]	C[34]	D[22]	D[31]

504-76625 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76632 VICTOR BRONDANI DOS SANTOS
24CC2504 - 18 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 493,2077), Bento=(1351,5561)`
   `Carlos=( 571,3569), Dante=( 677,4891)`
   `Erasmo=( 685,3551), Frida=( 817,2573)`
2. Sua chave pública é (217,1829)
   * e sua chave secreta é (433)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de dante
   Mensagem:
   ```
   4589 4044 3255 1644 4589 3443 4485 1494 1644 1494
   3255 4485 3070 1494 3433 3443 4504 1644 1037 1494
    547 4504 4485 1037 1494 3255 4589 4044 1890 4485
   1494  337 4589 3928 3070
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para bento
   Mensagem:
   `POR/FADO/INCONSTANTE/GUERREIROS/NASCI`
   D=_____.
   Dica: codifique com a sua CS
   Agora responda as questões, usando A, B, C e D calculados acima

A[29]	A[35]	B[19]	B[32]

C[18]	C[35]	D[10]	D[37]

504-76632 - gar a

5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   1504 1372 1507   45 1376  115  903 1504 1694  966
   1372   45  906 1372  638  507 1372   45  638  347
    906  347  116 1372   45  347   45 1504 1372 1507
   1376 1372  638  507 1372
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)
VIVXq84a V: 1.02
76649 VICTOR HUGO DOS SANTOS DE CAMA
24CC2504 - 19 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lãmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 463,2911), Bento=(1267,6497)`
   `Carlos=( 607,2537), Dante=( 933,2911)`
   `Erasmo=( 511,3713), Frida=( 643,4661)`
2. Sua chave pública é (817,5893)
   * e sua chave secreta é (2733)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de bento
   Mensagem:
   ```
   2227 2318 2258 2835  828 4776 5022 6299 6294  359
   6003 6183  359 5022  828 5022 4790 6294 5022 4816
   2180  828 5022 2258 2318 2835 2318 5269 5022 4776
   6294 4711  828 5269
   ```
   Qual é a mensagem ?
   A=_____.
   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para frida
   Mensagem:
   `GUERREIROS/DESCENDO/DA/TRIBO/TUPI`
   B=_____.
   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   ```
   1295 5025 5563 5707 2586  691 5707 2586  691 4714
   4451  787 4420 5707 2586  691 5475 4451 5707  691
   5563 2495 2586 5028 2495 4695 4695 4451 1295  691
   1196 5025 2495 4420 2826 4451 2586
   ```
   C=_____.
   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:
   `ANTE/OS/OLHOS/DO/CORPO/AFIGURADA`
   D=_____.
   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[5]	A[34]	B[29]	B[33]

C[30]	C[37]	D[31]	D[32]

504-76649 - gar a

CEP-UFPR-UTFPR-PUC/Pr-UP Sistemas de Informação 27/10/2024 - 09:51:40.2
Matemática aplicada Prof Dr P Kantek (pkantek@gmail.com)

VIVXq84a V: 1.02

76656 VITOR EDUARDO DE GOES FONTES
24CC2504 - 20 entregar ate 14/nov/24 _____ / / _____

Criptografia

Criptografia é a arte e a ciência de transformar informações legíveis (texto simples) em um formato codificado (texto cifrado) que só pode ser decifrado por alguém que possua informações adicionais corretas. É como escrever uma mensagem secreta que só pode ser lida por um destinatário específico.

Em termos mais simples: Imagine que você quer enviar uma carta para um amigo, mas não quer que ninguém mais leia o conteúdo. Você então escreve a carta usando uma linguagem codificada, onde cada letra é substituída por outra. Seu amigo, que conhece o código, consegue decifrar a mensagem e ler o que você escreveu. A criptografia funciona de forma semelhante, mas com códigos muito mais complexos e seguros.

Por que a criptografia é importante?

- Privacidade: Protege informações confidenciais, como senhas, dados bancários e informações pessoais.
- Integridade: Garante que os dados não sejam alterados durante a transmissão.
- Autenticidade: Verifica a identidade do remetente e do receptor.
- Não repúdio: Impede que alguém negue ter enviado ou recebido uma mensagem.

Como funciona a criptografia? Existem diversos métodos de criptografia, mas todos envolvem o uso de algoritmos e chaves. Os algoritmos são as fórmulas matemáticas que transformam o texto simples em texto cifrado e vice-versa. As chaves são sequências de bits que servem como "chave"para desbloquear a mensagem.

Tipos de criptografia:

Criptografia simétrica Utiliza a mesma chave para cifrar e decifrar os dados. É mais rápida, mas a chave precisa ser compartilhada entre os comunicantes, o que pode ser um problema em ambientes não seguros.

Criptografia assimétrica Utiliza um par de chaves: uma pública e uma privada. A chave pública é distribuída para todos, enquanto a privada é mantida em segredo. A mensagem é cifrada com a chave pública e só pode ser decifrada com a chave privada.

Certificação Invertendo-se a sequência acima (criptografa com a privada), todos podem ler a mensagem, mas a simples leitura garante que ela foi enviada pelo remetente (possuidor da chave privada)

Onde a criptografia é utilizada?

A criptografia está presente em diversas áreas do nosso dia a dia, como:

Comunicações online: Protege suas conversas em aplicativos de mensagens e e-mails. Transações financeiras: Garante a segurança de seus pagamentos online. Armazenamento de dados: Protege seus arquivos em nuvem e dispositivos. Autenticação: Protege suas senhas e permite o acesso a sistemas restritos.

A palavra criptografia tem suas raízes no grego antigo e traz consigo uma história rica e fascinante.

Kryptós: Essa parte da palavra significa "oculto"ou "secreto". Ela nos remete à ideia de esconder informações, tornando-as incompreensíveis para aqueles que não possuem a chave para decifrá-las. *Graphía*: Essa parte significa "escrita". Junta à parte anterior, forma a ideia de uma "escrita secreta".

A propósito, um conceito próximo, mas diferente, é o de criptoanálise, que vem a ser o esforço de decifrar a criptografia usada por alguém. soma de criptografia+criptoanálise dá-se o nome de criptologia.

Um pouco de história:

A prática de criptografar mensagens é tão antiga quanto a escrita. Desde os tempos antigos, pessoas utilizavam métodos simples de codificação para proteger informações importantes, como mensagens militares e segredos de estado. A Cifra de César, por exemplo, um método de substituição de letras, é um dos exemplos mais antigos de criptografia, atribuído ao imperador romano Júlio César.

O citale espartano (vivxz35) é um exemplo de criptografia antiga.

Antes do advento do computador, as iniciativas de criptografia dependiam do cérebro humano, e eram esquemas engenhosos, porém simples. Eis alguns exemplos:

A cifra de Viginère

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar segredos. Neste caso, a mensagem 'ivoviuauvaeamelancia' criptografada com a chave

```
alfabeto = ABCDEFGHIJKLMNOPQRSTUVWXYZ
chave    = EWTKIYVPXGOZNJLMRHDCABQFSU
```

Daria origem à mensagem: XBLBXAEABEIENIZEJTXE. O desenvolvimento subsequente da análise de frequência, primeiro no mundo árabe e depois na Europa (entre os séculos XII e XVII). Para maiores detalhes da cifra de Viginère, veja VIVX709. [1] destruiu sua segurança.

Criptografia One Way

Este método é muito adequado para criptografar um único texto. Usa como chave um outro texto, que pode ser famoso e bem conhecido (por exemplo, o Hino Nacional Brasileiro) ou então um texto especialmente preparado para ser chave.

A mensagem cifrada usa números como elementos da mensagem. Cada número destes remete à letra inicial da palavra que tem este número no chave original.

Por exemplo, usando como chave o texto
Ouviram[1] do[2] Ipiranga[3] as[4] margens[5] plácidas[6]
De[7] um[8] povo[9] heróico[10] o[11] brado[12] retumbante[13],
E[14] o[15] sol[16] da[17] Liberdade[18], em[19] raios[20] fúlgidos[21],
Brilhou[22] no[23] céu[24] da[25] Pátria[26] nesse[27] instante[28].
Se[29] o[30] penhor[31] dessa[32] igualdade[33]
Conseguimos[34] conquistar[35] com[36] braço[37] forte[38],
Em[39] teu[40] seio[41], ó[42] Liberdade[43],
Desafia[44] o[45] nosso[46] peito[47] a[48] própria[49] morte[50]!
Ó[51] Pátria[52] amada[53],
Idolatrada[54],
Salve[55]! Salve[56]!

Poderia se criptografar a seguinte frase: 55,30,34,42,13,20,45

Que seria traduzida por "SOCORRO". Note-se que letras repetidas, vêm escritas com números diferentes, já que existem diversos locais no texto original onde a mesma letra pode ser pinçada. Este fato inviabiliza o ataque por freqüência de letras.

A cifra ADFGVX

A cifra ADFGVX foi introduzida no dia 5 de março de 1918, um pouco antes da ofensiva alemã de 21 de março. Tal cifra fora selecionada por um comitê de criptógrafos alemães especialmente para dar garantia a este avanço. Nessa época a artilharia alemã estava a menos de 100Km de Paris e se preparava para o assalto final. A esperança dos franceses era descobrir o ponto de suas defesas que os alemães pretendiam quebrar.

Cifras de Playfair

Uma das últimas cifras usadas antes de inventaremse os computadores, chegou a ser operada ainda na Segunda Grande Guerra. Proposta por volta de 1850, fez sua estréia na Guerra dos Boers. Idealizada por Charles Wheatstone, quem convenceu o Governo Inglês a usar foi o Barão de Playfair, daí o nome com que ficou conhecida. Mais detalhes em vivx708.

Enigma

Em 1918 o alemão Arthur Scherbius começou o desenvolvimento de uma máquina criptográfica. Ele havia estudado os fracassos da criptografia durante a primeira grande guerra e pretendia desenvolver um produto superior. Nasceu a **ENIGMA**. Embora cara (cerca de US$ 35.000 por máquina em valores atualizados), nas duas décadas seguintes ela acabou sendo adotada por todos os corpos militares alemães. Mais de 30.000 ENIGMAS foram construídas e vendidas. Era uma caixa de madeira de 24 x 28 x 15cm pesando 12 quilos com as baterias incluídas. Formada por um teclado contendo as 26 letras e 26 lâmpadas (uma para cada letra), a ENIGMA tinha várias etapas lógicas: Logos depois do teclado, havia uma etapa em que 6 pares de letras eram invertidas por meio de fiaç es convencionais. Havia um conjunto de 5 rotores, cada um com as 26 letras representadas. Durante a operação, escolhiam-se 3 deles, que eram carregados em uma certa ordem dentro da enigma. Depois que o sinal elétrico passava pelos 3 rotores, um último estágio, denominado refletor, mandava o sinal de volta usando outro caminho, até que uma lâmpada acendesse. Mais detalhes vivx715.

simétrico: DES

O DES (Data Encryption Standard) foi um dos primeiros algoritmos de criptografia simétrica amplamente utilizado. Embora tenha sido considerado obsoleto devido ao tamanho curto de sua chave (56 bits), que o torna vulnerável a ataques de força bruta com a tecnologia computacional atual, o DES ainda possui valor histórico e didático. Veja vivx710.

simétrico: TEA

O TEA (Tiny Encryption Algorithm) é um algoritmo de criptografia simétrica de bloco, projetado para ser simples e eficiente. Ele foi criado com o objetivo de oferecer uma solução de criptografia leve para sistemas com recursos limitados, como microcontroladores.

Estrutura: O TEA opera em blocos de 64 bits, utilizando uma chave de 128 bits. A estrutura básica do algoritmo envolve várias rodadas de operações simples, como adições e rotações de bits, sobre os dados de entrada.

Simplicidade: Uma das principais características do TEA é sua implementação simples. Ele utiliza operações aritméticas básicas, o que o torna fácil de entender e implementar em diferentes plataformas. Eficiência: O TEA é relativamente rápido, especialmente em plataformas com hardware limitado. No entanto, sua segurança pode ser questionada em comparação com algoritmos mais modernos e robustos. Veja vivx711.

Criptografia El Gamal

Veremos que a segurança do método RSA reside na dificuldade (esperada, mas ainda não provada) de fatorar números grandes. Outros problemas difíceis de resolver também podem dar origem a outros métodos de criptografia. Um desses métodos, que recebeu o nome de seu descobridor (Taher El Gamal), está na dificuldade esperada para resolver o problema conhecido como *logaritmo discreto*. Quando se trabalha com números reais, o $\log_b a$ é o número x para o qual a é igual a b^x. Lembrando através de uma fórmula:

$$\log_a b = c \quad \Rightarrow \quad a^c = b$$

Usando-se a aritmética dos ponteiros do relógio, também é possível definir um logaritmo (agora chamado *discreto*). Note que para este tipo de problema só intervem números inteiros, como convém à aritmética discreta. Dados os inteiro b e n com $b < n$, o logaritmo discreto de um inteiro a na base b é o inteiro x tal que $b^x \equiv a \ mod \ n$ usando uma fórmula:

$$\dagger \log_{b,n} a = x \quad \Rightarrow \quad b^x \equiv a \ mod \ n$$

[1] A propósito, quem se interessar pelo método da análise da frequência, leia o conto de Conan Doyle "Os dançarinos", onde Sherlock Holmes descreve o método de maneira magistral.

Lembrando, na criptografia assimétrica, as chaves vem em pares, e tudo que é criptografado com uma chave precisa da outra chave para ser descriptografado. As chaves vão ser chamadas de pública e privada. Primeiro deve ser gerada a chave privada (um número completamente aleatório) e depois a chave pública pode ser facilmente calculada usando a chave privada. O caminho inverso (da pública → privada) revela-se computacionalmente intratável.

Aqui, a principal funcionalidade perseguida não é exatamente a criptografia e sim a assinatura digital, que vem a ser a contrapartida do mesmo método. Ela garante que o possuidor da chave é o único legítimo proprietário dos direitos (neste caso, direito aos bitcoins).

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a "quebrar" o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decriptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \ mod \ n$	$3^5 \ mod \ 21 = 12$, $14^5 \ mod \ 21 = 14$, $9^5 \ mod \ 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \ mod \ n$	$12^{17} \ mod \ 21 = 3$, $14^{17} \ mod \ 21 = 14$, $18^{17} \ mod \ 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1
4:     devolva (X mod N) {em C ou Python: X % N}
5: senão
6:     se (Y mod 2) = 0
7:         TMP ← XELEVADOAY (X, (Y/2), N)
8:         devolva (TMP * TMP) mod N
9:     senão
10:        TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11:        TMP ← (TMP * TMP) mod N
12:        TMP ← (TMP * X) mod N
13:        devolva TMP
14:    fim{se}
15: fim{se}
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa $(2^3) \ mod \ 20 = 8$
$(5387^{2189}) \ mod \ 3311 = 1668$
$(7752^{4156}) \ mod \ 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular $(numero^a) \ mod \ b$ e enviar o resultado

Para decriptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular $(numero^c) \ mod \ d$
3. Recuperar o caractere usando a tabela

		D	5	H	9	L	13	P	17	T	21	X	25
A	2	E	6	I	10	M	14	Q	18	U	22	Y	26
B	3	F	7	J	11	N	15	R	19	V	23	Z	27
C	4	G	8	K	12	O	16	S	20	W	24	/	28

Exemplo

Erasmo (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS"para a Frida (chave pública da Frida é [763,3953]). Como fica ?
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?
Resposta: 1375 e 390

☞ Para você fazer

1. Eis as chaves públicas conhecidas
   `Alice=( 593,4897), Bento=(1005,3127)`
   `Carlos=( 169,1457), Dante=(1069,7663)`
   `Erasmo=( 677,4891), Frida=( 933,2911)`
2. Sua chave pública é (643,3337)
   * e sua chave secreta é (1287)
   Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.
3. Você recebeu a seguinte mensagem (alfabética) de erasmo
   Mensagem:
   `3443 1644 3433 4504 4485 1494 4485 4105 1037 4589`
   `3255 3070 1494 1644 1494 3438 4485  663 4589 3928`
   `3070 1494 3433 3070 2068 3443 4589 4044 3928 3070`

   Qual é a mensagem ?

   A=_____.

   Dica: decodifique usando a CP do remetente
4. Você quer mandar a mensagem abaixo para carlos
   Mensagem:

   `QUE/LHE/ORNA/O/COLO/E/O/PEITO/RUGE`
   B=_____.

   Dica: codifique com a CP do destinatário
5. A mensagem abaixo só deve ser lida por você. Qual é?
   Mensagem:
   `3138 2917 3295 1029 3223 2938 1758 2917 1029 2665`
   `2889 2362 2917 2889 1168  291 2938 2889  291 2687`
   `1029 1933 2553 2687 3295 3295 2687 2665 3295 2917`
   `1168 1029 2889 2938 1168 2362 2665`

   C=_____.

   Dica: decodifique usando a sua CS
6. Esta mensagem vai assinada por você
   Mensagem:

   `NAO/CONHECES/TEMOR/E/AGORA/TEMES`
   D=_____.

   Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

A[4]	A[30]	B[7]	B[34]

C[4]	C[37]	D[10]	D[32]

504-76656 - gar a