_____ / _____ / _____

Cifras de Playfair

Uma das últimas cifras usadas antes de inventarem-se 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.

Possui as fraquezas de sempre: sucumbe a uma análise de frequência, mas por trabalhar com dígrafos (2 letras), a análise tem que ser feita sobre tais grupos. Em contrapartida, tem algumas vantagens: não precisa de tabelas, usa chaves fáceis de memorizar e trocar quando necessário, é simples de operar e consequentemente é pouco sujeita a erros. Por isso esta cifra é ótima para ser usada como "cifra de campo".

Na cifra Playfair as letras do texto plano são usadas duas a duas (o que caracteriza um bloco dígrafo). O alfabeto cifrante é colocado em uma grade 5×5, o que implica em matar uma letra. Pode-se excluir o K (substituindo por C), o W (por V) ou o Y (por I). Há ainda quem mate o J e deixe I e J valerem I. Nesta folha, vai-se excluir a letra Y substituindo-a quando necessário por I.

O alfabeto começa com as letras da chave, sem repetições. As demais casas são preenchidas com o alfabeto (menos as letras da chave) em ordem alfabética. Por exemplo, se a chave for `CURITIBAPARANA`, o início do alfabeto cifrante é `CURITBAPN`. Eis como fica o alfabeto cifrante:

C	U	R	I	T
B	A	P	N	D
E	F	G	H	J
K	L	M	O	Q
S	V	W	X	Z

A seguir, a mensagem a criptografar deve ser dividida em grupos de 2 caracteres. Esses dois caracteres formarão a linha e a coluna da resposta. Em outras palavras, vai-se consultar cada bloco destes no alfabeto cifrante: 3 casos podem ocorrer:

1. As duas letras estão na mesma linha: cada letra é substituída pela sua vizinha da direita
2. As duas letras estão na mesma coluna: cada letra é substituída pela sua vizinha de baixo Nestes dois casos, a linha ou a coluna formam um anel, ligando o último ao primeiro.
3. As duas letras formam os vértices de um retângulo. O grupo é substituído pelos outros dois vértices do retângulo (cada letra é substituída pela letra que está na mesma linha)

Precisa-se designar uma letra CORINGA para auxiliar nesta codificação. Embora a mensagem possa incluir este coringa, ao fazer isto, é necessária uma melhor especificação para este caso. Assim, para facilitar nossa vida, vai-se EXCLUIR este coringa da mensagem. Portanto, aqui, já são 2 letras as excluidas: a 26^a letra e o coringa.

Escolheu-se aqui o coringa `W` e para sua aplicação, vão ser usadas duas regras:

1. Letras dobradas (SS, RR ou mesmo AA ou OO) impedem a aplicação da cifra. Se ocorrer um grupo assim, colocar o coringa entre o par. Nesta folha, esta regra vai ser ligeiramente modificada a fim de auxiliar na implementação em computador. Quando uma letra estiver dobrada, estas duas letras vão ser substituídas por letra+coringa e letra+coringa.
2. Se o ultimo grupo tiver uma única letra, colocar um coringa também para completar o grupo

Continuando o exemplo: seja criptografar a mensagem MINHA TERRA TEM PALMEIRAS ONDE CANTA O SABIA. Formando os blocos fica: MI NH AT ER RA TE MP AL ME IR AS ON DE CA NT AO SA BI A. O último bloco como se viu deve ser AW.

Veja-se o primeiro grupo que é `MI`. Localizando este grupo na tabela de cifragem ve-se que as duas letras formam um retângulo. Devem ser substituídas por `OR`. O próximo grupo é `NH` que estão na mesma coluna. O `N` deve ser substituído po `H` e o `H` por `O`. Depois vem o grupo `AT` que deve ser substituído por `DU`. Depois `ER`, que vira `GC`. Depois RA, que vira UP. Depois TE que vira CJ. depois MP que vira WG. Depois AL que vira FV. Depois ME que se torna KG. E, assim por diante.

A decriptografia segue os mesmos passos, agora em ordem inversa.

Cifra Playfair de 4 grades

É uma variação da cifra estudada, na qual usam-se 4 cifras, dispostas assim $\frac{1|2}{3|4}$. No método devem ser fornecidas 4 senhas (que podem ser iguais, ou vazias) mas que permitem a construção das 4 cifras mencionadas no método. Agora cada grupo (2 letras) da mensagem clara deve ser buscado nas cifras 1 e 4. A mensagem cifrada correspondente será encontrado nas cifras 2 e 3. A grande vantagem desta variante é que:

- Não há porque tratar duplas de letras iguais. O problema desaparece.
- As 3 regras (mesma linha, mesma coluna e retângulo) se convertem em apenas 1: em todos os casos o resultado é um retângulo.

Veja-se o exemplo: Seja criptografar a mensagem OUVIRAM DO IPIRANGA AS MARGENS PLACIDAS. Manuseado o texto fica OU VI RA MD OI PI RA NG AA SM AR GE NS PL AC ID AS Se usarmos as senhas ('OLIVIAPALITO' 'RECRUTAZERO' 'CARMENSANDIEGO' e 'TIGREHAROLDO'), as cifras ficarão

```
OLIVA|RECUT|
PTBCD|AZOBD|
EFGHJ|FGHIJ|
KMNQR|KLMNP|
SUWXZ|QSVWX|
------------
CARME|TIGRE|
NSDIG|HAOLD|
OBFHJ|BCFJK|
KLPQT|MNPQS|
UVWXZ|UVWXZ|
```

e a mensagem cifrada será RUEMLGPSECZCLGMREGQKUEJRPPBNEJTDTT

Exemplo Completo

Fazendo um exemplo completo, usando estrofes da maravilhosa poesia de Manoel Bandeira (Vou me embora para Passárgada), eis algumas criptografias:

- A criptografia Playfair da frase
  MAS TRISTE DE NAO TER JEITO, com a senha CELULASTRONCO gerou
  PUTRSKTRTJATUNDTTKCJRN.
- A decriptografia de
  FGTJAGNWMBGWEGCGJX com a senha GRADEESPERTA, gerou
  SUBIREINOPAUDESEBO.
- A descompressão usando 4 grades senhas:
  LIVROVERDE,
  GRAMPEADOR,
  OITONOVEDEZ e
  SACOLACHEIA de
  LWEMBIDDSIPLCCCEBK deu
  QUANDODENOITEMEDER.

Apenas para conferir, eis as 4 grades do exemplo acima

```
LIVRO|GRAMP|
EDABC|EDOBC|
FGHJK|FHIJK|
MNPQS|LNQST|
TUWXZ|UVWXZ|
------------
OITNV|SACOL|
EDZAB|HEIBD|
CFGHJ|FGJKM|
KLMPQ|NPQRT|
RSUWX|UVWXZ|
```

☞ Para você fazer

1. Playfair com 1 senha Criptografe a frase, também obtida da poesia de Manoel Bandeira, Vou me embora para Passárgada:

`ANDAREIDEBICICLETA`

com a senha

`JANTARDELICIOSO`

e responda abaixo com o sexto, décimo e décimo quarto caracteres da resposta.

6	10	14

2. Playfair com 1 senha Decriptografe a frase

`FVIPLPCJLESMFVKZER`

com a senha

`LAPISDECOR`

Responda a frase encontrada aqui

3. Playfair com 4 senhas Use as senhas

`NEZINHOXAROPE`
`MADRESSELVA`
`QUEMSABEOQUE`
e
`ALGORITMOBRABO`

Para decriptografar a frase

`RUUOSMFBTCKOMEFUVT`

Responda a frase encontrada aqui

.