

Criptografia Simétrica (DES)

Este exercício simula uma criptografia de chave simétrica com princípio (apenas o princípio !) similar ao *DES = Data Encryption Standard*, padrão do governo americano para criptografia simétrica.

Para converter uma mensagem, a primeira coisa que emissor e receptor devem combinar é a respeito de uma chave comum.

Neste exemplo, usaremos a *chave = AYAHOUSQ*. Note que a chave tem 8 caracteres, o que caracteriza a criptografia em bloco, neste caso, bloco de 8 caracteres.

A chave deve ser convertida em um vetor de 8 números, usando a convenção seguinte:

/	0	E	5	J	10	O	15	T	20	Y	25
A	1	F	6	K	11	P	16	U	21	Z	26
B	2	G	7	L	12	Q	17	V	22		
C	3	H	8	M	13	R	18	W	23		
D	4	I	9	N	14	S	19	X	24		

Neste caso, tem-se como resultado: 1 25 1 8 15 21 19 17

O texto plano que deve ser criptografado deve ser separado em blocos de 8 caracteres também. Seja a seguinte mensagem que deve ser criptografada

NAO/VOLTAR/JAMAIS/OU/NUNCA (espaço é igual a /)

E, fica:

NAO/VOLT AR/JAMAI S/OU/NUN CA////////

(Note o preenchimento com espaços ao final)

Deve-se primeiro inverter os pares da mensagem, e fica:

AN/OOVTL RAJ/MAIA /SUON/NU AC////////

Agora, deve-se converter cada bloco em seu equivalente numérico:

1 14 0 15 15 22 20 12 18 1 10 0 13 1 9 1
0 19 21 15 14 0 14 21 1 3 0 0 0 0 0

Deve-se fazer 2 somas agora: primeiro deve-se somar a chave a cada grupo, e fica

2 39 1 23 30 43 39 29 19 26 11 8 28 22 28 18
1 44 22 23 29 21 33 38 2 28 1 8 15 21 19 17

A próxima soma é com o deslocamento de cada caracter na chave (somar 0 1 2 3 4 5 6 7 a cada grupo), e fica:

2 40 3 26 34 48 45 36 19 27 13 11 32 27 34 25
1 45 24 26 33 26 39 45 2 29 3 11 19 26 25 24

A seguir, calcule o resto da divisão de cada número por 27:

2 13 3 26 7 21 18 9 19 0 13 11 5 0 7 25
1 18 24 26 6 26 12 18 2 2 3 11 19 26 25 24

Lembre de desconverter os pares. Fica:

13 2 26 3 21 7 9 18 0 19 11 13 0 5 25 7
18 1 26 24 26 6 18 12 2 2 11 3 26 19 24 25

Finalmente, converta a mensagem numérica em caracteres usando a tabela original.

MBZCUGIR /SKM/EYG RAZXZFRL BBKCSXY

Que é a mensagem devidamente criptografada.

Note que para decryptografar uma mensagem cifrada o mesmo método deve ser empregado, só que em ordem inversa.



Para você fazer

- Use a chave: AGXDNGQM
- Criptografe a mensagem: SE/PERMITIRMOS/QUE/SUPONHA/TAL//
 1. Transforme a chave em números:
 2. Separe a mensagem em grupos de 8, completando com brancos:
 3. Inverta os pares de caracteres
 4. Transforme a mensagem em números
 5. Some a chave aos caracteres da mensagem
 6. Some o deslocamento na chave
 7. Ache o resto da divisao por 27.
Regra: ate 26 inclusive não precisa fazer nada. Depois, use a tabela

27=0, 28=1, 29=2, 30=3, 31=4, 32=5, 33=6,
34=7, 35=8, 36=9, 37=10, 38=11, 39=12, 40=13,
41=14, 42=15, 43=16, 44=17, 45=18, 46=19, 47=20,
48=21, 49=22, 50=23, 51=24, 52=25, 53=26, 54=0,
55=1, 56=2, 57=3, 58=4, 59=5, 60=6, 61=7
- 8. Converta os números em caracteres
- 9. Desinverta os pares e junte tudo. O resultado é:
- Considere a mensagem que você acabou de cifrar como o vetor C

Responda agora:

1. C[8] _____ 2. C[23] _____ 3. C[31] _____

- Use a mesma chave e decryptografe ITZDYTEAZALZPWTYIJDNLBRMMGZLRTW
 1. Separe a mensagem em grupos de 8. Não é necessário completar brancos
 2. Inverta os pares
 3. Converta os caracteres em números. Subtraia de cada um o valor da chave e depois o deslocamento (0 1 2 3 4 5 6 7) na chave. Se o resultado for negativo, some 27 ao resultado
 4. Converta em caracteres, usando a tabela
 5. Desinverta os pares e responda. A mensagem plena é:
- Considere a mensagem que você acabou de decifrar como o vetor P

Responda agora:

4. P[3] _____ 5. P[27] _____ 6. P[28] _____

1



- 1 - /