

Nome: _____ Data: ____/Maio/2018

CRIPTOGRAFIA (códigos e cifras)

Criptografia é a arte de criar cifras e códigos para esconder a mensagem que queremos transmitir; é a arte de criar mensagens secretas. A palavra vem do grego *kryptos* (secreto, escondido, oculto) e *grapho* (escrita grafia), ou seja, escrever escondido!

CIFRAS DE FORMATO

Por vezes, para esconder uma mensagem, basta-nos organizar as letras de tal maneira que, para quem a tente ler, a mensagem não seja óbvia. Vimos vários exemplos disso nas aulas: inverter as palavras, inverter as frases, escrever em blocos, escrever em bloco e ler noutra direção.



Let's give it a try...

Exercises

Descobre as mensagens escondidas com os seguintes métodos:

1. Palavras invertidas

MOB ODUTSE!

ARFIC SELPMIS

2. Frases invertidas

!EDRAT AOB

SELPMIS SIAM

3. Escrita em blocos

C I F R
A S S Ã
O G I R
A S !

4. Escrita em blocos mas lida noutra direção

IMF SUÁ TIC OTI ÉOL

ETMTP IAÉOL SMMSE TBUIS OÉIM!

CIFRAS DE SUBSTITUIÇÃO - CIFRAS DE CÉSAR

Nas cifras de formato as letras estão lá todas, visíveis, mas são arrumadas de forma a que seja difícil ler a mensagem. Nas cifras de substituição as letras são trocadas por outras de acordo com um sistema previamente definido.



Júlio César (100 aC – 44 aC) usava um método de substituição simples para esconder as mensagens que enviava aos seus generais: trocava cada letra de uma mensagem pela **terceira letra seguinte (+3)**. Ou seja:



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

Let's give it a try...

Exercises

E consegues decifrar o seguinte código?

R	V	D	O	X	Q	R	V	Q	D	R	S	R	G	H	P	O	H	U	L	V	W	R

CIFRAS DE SUBSTITUIÇÃO – CIFRAS MONOALFABÉTICAS

A Cifra de César pode ser alterada variando o número de letras que avançamos para fazer a substituição.

Também podemos inverter o alfabeto (alfabeto invertido):

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

Let's give it a try...

Exercises

Descobre as seguintes mensagens cifradas com os seguintes métodos:

1. Cifra de César (+3, A→D)

X P D F L I U D G H F H V D U

H P D L V R X W U D D L Q G D

4. Ordem posicional (A→01, B→02, ...)

16 18 15 07 18 01 13 01 18 05 02 15 13

09 14 20 05 12 09 07 05 14 03 09 01

2. Alfabeto meio-quebrado (+13, A→N)

H Z N P V S E N Q R P R F N E

Z R G N Q R Q B N Y S N O R G B

5. Alfabeto invertido (A↔Z)

T L H G L W V X R U I Z H

X L W R T L H U Z X V R H

3. Cifra de César (+4, A→E)

Y Q E G M J V E H I G I W E V

E K S V E Í H M J I V I R X I

CIFRAS POLIALFABÉTICAS

Para tornarmos a nossa cifra mais segura, uma coisa que podemos fazer é utilizar vários alfabetos, criar uma cifra que seja polialfabética em vez de ser monoalfabética como as que utilizámos até aqui.

Uma forma simples é somar um número diferente a cada letra de forma a introduzir variabilidade.

Por exemplo, podemos utilizar a data da conquista de Lisboa: 25 de outubro de 1147.

Mensagem original: L i s b o a é n o s s a ! (mensagem que queremos enviar)

Mensagem a cifrar: L I S B O A E H N O S S A (removemos acentos e substituímos por Hs)

Data (chave): + 2 5 1 0 1 1 4 7 2 5 1 0 1 (alinhamos os algarismos da data com as letras; repetimos se necessário)

Mensagem cifrada: N N T B P B I O P T T S B (para cada letra avançamos o número de letras correspondentes ao algarismo da data)

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

Para ler uma mensagem destas que nos tenham enviado fazemos o processo inverso. Subtraímos a data:

Mensagem cifrada: R F S A C F R Z C K P N T P (mensagem recebida)

Data (chave): - 2 5 1 0 1 1 4 7 2 5 1 0 1 1 (alinhamos os algarismos da data com as letras; repetimos se necessário)

Mensagem decifrada: P A R A B E N S A F O N S O (para cada letra recuamos o número de letras correspondentes ao algarismo da data)

Se quisermos, em vez de uma data fixa, podemos usar a data do dia em que a mensagem foi enviada..



Let's give it a try...

Exercises

Decodifica a seguinte mensagem utilizando a data de envio (25 de dezembro de 2017)

I T T V Q M V P V T E G R R P N T F N C E A P L F J S Q D O U P E F
- 2 5 1 2 2 0 1 7 2 5 1 2 2 0 1 7 2 5 1 2 2 0 1 7 2 5 1 2 2 0 1 7 2 5