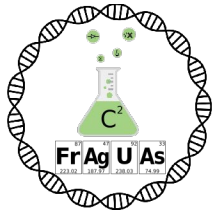


Club de Ciencias
IES Antonio Fraguas

FRAGOLIÑOS

Criptoloxía

Definición

A **criptoloxía** (do grego cryptos = oculto e logos = ciencia)
A criptología moderna ten dous obxectivos fundamentales:

- **Criptografía**: Permitir que duas ou máis persoas poidan comunicarse de forma secreta utilizando canais de comunicación inseguros (teléfono, correo, fax, correo electrónico, etc.)

- **Criptoanálese**: Analizar cómo poden ser vulneradas estas comunicacións para coñecer o seu contido. (hacker, crackers)

Criptografía

Chamamos **texto plano** ou claro a un texto sen cifra**r**
Texto cifrado é aquel que está codificado (encriptado)
A regla para cifrar e descifrar o mensaxe chámase **algoritmo**
A maioría dos algoritmos teñen un método que permite descifrar con maior rapidez, que se chama **chave**.

Os métodos máis antiguos que se coñecen son de dous tipos:

- Cambiar unhas letras por outras ou por simbolos
- Desordenar as letras

Criptografía

Cambiar letras por outras

A **criptografía Cesar** consiste en desprazar as letras do alfabeto un número de posicións. Ese desprazamento é a chave. Chámase así porque o utilizaba **Julio Cesar** para enviar mensaxes aos seus xenerais.

OLA
ALUMNOS

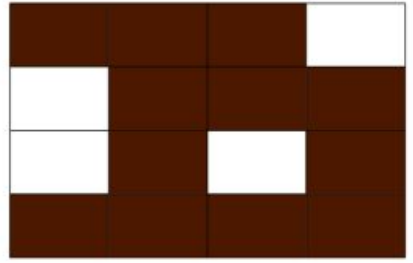
cifrar: chave 2

QNC
CNWOPQU

Outros parecidos poden ser:

- Cambiar a primeira letra pola seguinte no alfabeto, a segunda pola segunda seguinte, a terceira pola terceira seguinte, etc.
- Cambiar as letras que ocupen posicións impares pola n-ésima seguinte, e as que ocupen posicions pares por la n-ésima anterior.
- O código morse.
- **¿Que máis se vos ocurren?**

A rexilla xiratoria



Este sistema permite desordenar a mensaxe xirando unha rexilla con ocos. Tal como vimos no xogo.

A escítala espartana

Consiste en escribir a mensaxe nunha tira de papel que despois se enrrolla nun bastón.
https://www.youtube.com/watch?v=Z0WgfYGb2rE

Criptografía

Cifrado Vigénere

O **cifrado de Vigenere** estivo máis de 2 siglos sen poder romperse, consiste en utilizar unha palabra como chave e tantos alfabetos Cesar como letras ten a palabra.

Se a palabra chave é **SOL** usaríamos o alfabeto que fai coincidir a A coa S, o que a fai coincidir coa O e o que a fai coincidir coa L.

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

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

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

Cifrado Vigénere

O **cifrado de Vigenere**

Agora colocamos a palabra SOL repetida debaixo da frase que queremos cifrar, así:

H	O	L	A		A	L	U	M	N	O	S
S	O	L	S		O	L	S	O	L	S	O

Para cada letra usamos o alfabeto Cesar que corresponde a letra de SOL que hai debaixo, e quedaría:

ZDVA AVNAXHH

Criptoanálese

Análese de frecuencias

O primeiro libro coñecido de criptoanálise é unha obra do filósofo árabe do siglo IX, AlKindi. Douse conta de que "en todas as línguas hai unhas letras que aparecen máis a miudo que outras". Por exemplo, en galego, as letras máis frecuentes son:

Moi frecuentes	Frecuentes	Pouco frecuentes	Escasas
A 12.26% E 11.98% O 11.49% I 8.28% S 7.81% N 7.04%	R 6.6% T 5.99% D 5.77% C 5.28%	U 3.37% L 3.07% P 2.81% M 2.65% G 1.49%	X 0.92% B 0.81% V 0.77% F 0.71% Q 0.48% Z 0.3% H 0.08%

Criptoanálese

Análese de frecuencias

Se analizamos unha das mensaxes do xogo:

QFRIJN QQQHHH PJCNTRFWNTX F PTNYFW HTRYWF TX LFPTX, XT IZFX YJWHJNWFX UFWYJX ATPAJWTR F HFXF

Sae que as máis frecuentes son F (12 veces) T (9 veces)

Podemos supoñer que a F é polo tanto a A, e que por tanto o desprazamento sería de 5 letras, usámolo e sae:

MANDEI CCCXXX LEXIONARIOS A LOITAR CONTRA OS GALOS, SO DUAS TERCEIRAS PARTES VOLVERON A CASA.

Outras formas de facer análeses de frecuencias poden ser:

- Se duas palabras seguidas acaban na mesma letra, e a primeria é corta, é probable que a letra sexa a S (plurais)
- As palabras dunha letra soen ser unha vogal. Dúas letras soen ser conxuncións ou preposicións, de, ao, si, en…
- Detrás de unha Q sempre vai unha U, así que parellas de dúas letras sempre xuntas poden ser QU. O mesmo se pode facer con parellas ou trios de letras que soen sair xuntos (palabras rematadas en ción, en,...)

Criptoanálese

Enigma

Na segunda guerra mundial os alemanes tiñan unha máquina de encriptar que permitía 12 millóns de combinacións distintas.

ENIGMA

Cada día usaban un sistema de codificación distinto, co cal era imposible con análeses de frecuencias conseguir descifrar os mensaxes, ata que apareceu...