Técnicas Criptográficas

Uno de los mayores desafíos para la informática en general es proporcionar un entorno seguro para las aplicaciones; más teniendo en cuenta que existen multitud de ellas que se sirven de Internet. La restricción de acceso, la custodia de contraseñas o el almacenamiento y transmisión de información de datos son procesos que deben de contar con mecanismos que aseguren **seguridad** e **integridad** de la información.

Introducción a la criptografía

El término **criptografía** es un derivado de la palabra griega kryptos, que viene a significar "oculto". El objetivo de la criptografía es ocultar el significado de un mensaje mediante el cifrado o codificación del mensaje. En castellano se deben de usar las palabras cifrar/descifrar; las palabras encriptar/desencriptar hacen referencia a meter ni sacar cosas de criptas...

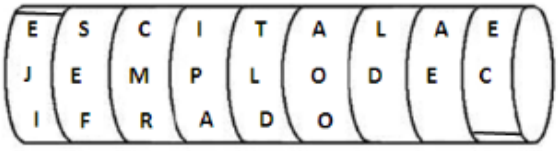
La escítala espartana

Se trata de uno de los sistemas criptográficos más antiguos que se conocen, utilizado en el siglo V a.C. en las guerras entre Atenas y Esparta, y era un sistema de transposición, es decir, sólo el orden de cada carácter del texto en claro resultaba alterado en el texto cifrado, sin que existiera ninguna sustitución de éstos por otro u otros caracteres.


Una escítala
Fuente: wikipedia.org

El sistema era muy simple. Consistía en que el emisor y el receptor del mensaje disponía de varas de similar grosor o diámetro. El mensaje se escribía tal cuál sobre largas cintas de cuero o papiro, de forma que sólo podía entenderse el mensaje si se enrollaba a lo largo de la vara. Obviamente, en esta época muy poca gente sabía leer, lo que ayudaba bastante a que nadie descifrase los mensajes.

Por ejemplo, partamos del mensaje en claro: "ESCITALAEJEMPLODECIFRADO":

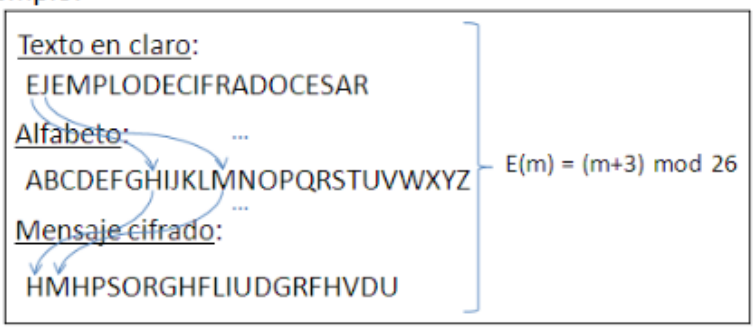


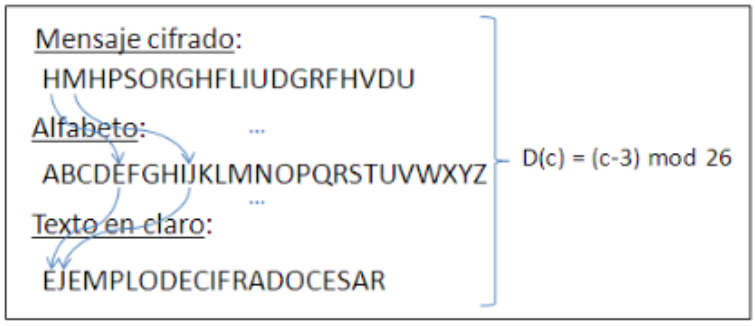
Si algún ateniense interceptaba el mensaje, no podía entenderlo puesto que leería en la cinta desenrollada: "EJISEFCMRIPATLDAOOLDAEEC".

El cifrado César

Éste es otro de los sistemas criptográficos más antiguos, utilizado en el siglo I a.C. Debe su nombre a Julio César. Era un sistema de sustitución mono alfabética. En este caso cada carácter del texto en claro es sustituido por otro carácter del alfabeto situado un número fijo de posiciones por delante (típicamente tres posiciones), y es mono alfabético porque se emplea un único alfabeto, es decir, cada carácter del texto en claro se sustituye siempre por el mismo carácter en el texto cifrado.

Ejemplo:





El método Vigenère:

El método de Vigenère es un sistema de sustitución poli alfabético, lo que significa que cada carácter del texto a cifrar NO se sustituye siempre por el mismo carácter en el texto cifrado, es decir, es un sistema en el que hay implicados varios alfabetos y dependiendo de ciertas circunstancias se aplica uno u otro.

Se trata también de un sistema de cifrado simétrico, es decir, el emisor del mensaje lo cifra utilizando una clave y el receptor debe descifrarlo utilizando esa misma clave. Por tanto, el emisor y el receptor se tienen que poner de acuerdo en la clave a utilizar.

Un ejemplo de cifrado:

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

Para cifrar el mensaje "EJEMPLO CIFRADO" con la clave "CLAVE", ponemos la clave encima del texto a cifrar repitiendo la clave tantas veces como haga falta hasta cubrir completamente el texto a cifrar, de la siguiente manera:

Clave -->	C	L	A	V	E	C	L	A	V	E	C	L	A	V
Texto a cifrar -->	E	J	E	M	P	L	O	C	I	F	R	A	D	O

Y ahora para obtener el texto cifrado sólo queda sustituir cada carácter del texto a cifrar por el carácter de la tabla anterior que se encuentra en la intersección entre la columna que corresponde al carácter a cifrar y la fila correspondiente al carácter de la clave que está justo encima; como en el juego de los barcos.

Por ejemplo: a la primera “E” del texto a cifrar, que tiene justo encima la “C” de la clave, le correspondería como carácter en el texto cifrado la letra “G”. Si repetimos esto para cada uno de los caracteres del texto a cifrar obtenemos el siguiente mensaje cifrado o criptograma:

Clave -->	C	L	A	V	E	C	L	A	V	E	C	L	A	V
Texto a cifrar -->	E	J	E	M	P	L	O	C	I	F	R	A	D	O
Texto cifrado -->	G	U	E	H	T	N	Z	C	D	J	T	L	D	J

Para **descifrar** sólo tenemos que poner la clave encima del texto cifrado repitiendo la clave tantas veces como haga falta hasta cubrir completamente el texto cifrado, de la siguiente manera:

Clave -->	C	L	A	V	E	C	L	A	V	E	C	L	A	V
Texto cifrado -->	G	U	E	H	T	N	Z	C	D	J	T	L	D	J

Y ahora para descifrar el texto sólo queda sustituir cada carácter del texto cifrado por el carácter de la columna que le corresponde al carácter cifrado en la fila correspondiente al carácter de la clave que está justo encima.

Por ejemplo: a la letra “G” del texto cifrado, que tiene justo encima la “C” de la clave, le correspondería como carácter en el texto descifrado la letra “E”.

Si repetimos esto para cada uno de los caracteres del texto cifrado obtenemos el siguiente mensaje descifrado o texto en claro:

Clave -->	C	L	A	V	E	C	L	A	V	E	C	L	A	V
Texto cifrado -->	G	U	E	H	T	N	Z	C	D	J	T	L	D	J
Texto descifrado -->	E	J	E	M	P	L	O	C	I	F	R	A	D	O

Obviamente, **si no se dispone de la clave**, es (teóricamente) imposible descifrar el mensaje por mucho que se disponga de la tabla.