UD 4.- Blockchain

DASP DAM1

Criptografía y criptoanálisis

Criptografía

Escribir mensajes que nadie pueda entender, a menos que tenga un elemento secreto, llamado *clave*

Criptoanálisis

Atacar y descifrar los mensajes cifrados sin el conocimiento de la clave

Criptografía

Al utilizar la criptografía conseguimos *cifrar* (no encriptar) y que un mensaje esté *cifrado* (no encriptado)

Para descifrar un mensaje se utiliza una *clave* (no una llave)

Criptografía

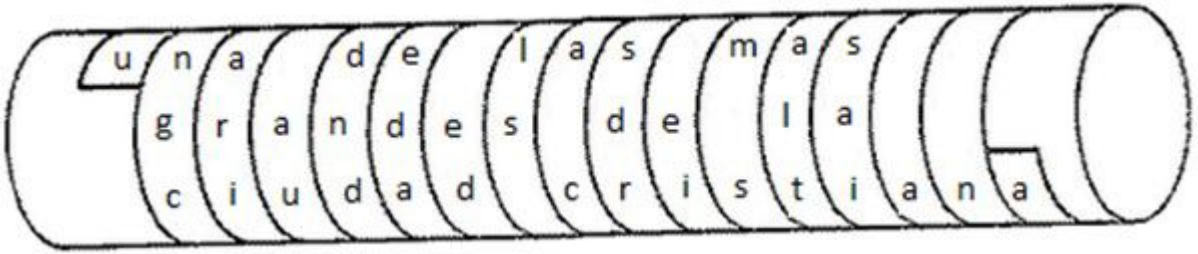
La criptografía está obligada a evolucionar constantemente

Cifrados de no muchos meses, están «rotos» por criptosistemas

Aplicaciones de mensajería instantánea como *WhatsApp*, no basan sus actualizaciones periódicas en simples activaciones de tics a la lectura de mensajes o métodos de borrado, dichas actualizaciones tienen misiones mucho más importantes como la actualización de los algoritmos de cifrado, base de la credibilidad del secreto de las comunicaciones en este tipo de mensajería.

Orígenes de la criptografía

Escítala



Mensaje cifrado: “**ungcariaudndedaedlsacsdreimsaltwaiana**”

Mensaje en claro: “**una de las más grandes de la ciudad cristiana**”

Para poder leer el mensaje, el receptor debía utilizar otro bastón del mismo diámetro y enrollar la cinta de papel escrita alrededor de él

Tipos de cifrado

Cifrado de sustitución: cada una de las letras del mensaje original tiene una correspondencia fija en el mensaje cifrado

Cifrado de transposición: as letras simplemente cambian de sitio o se transponen, por tanto, las letras son las mismas en el mensaje original y en el cifrado

Cifrado de Vigénere

Texto en claro: TOBEORNOTBETHATISTHEQUESTION ...

Clave: RUN (se repite hasta completar el texto en claro)

Criptograma: KIOVIEEIGKIOVNURNVJNUVKHVMGZIA

T = 19 R=17 → (19 + 17) mod 26 = 10

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cifrado de Vigénere

Es importante observar que letras repetidas del texto en claro se cifran habitualmente de forma distinta, en función de su posición respecto a la clave.

Tabla cifrado de Vigénere

	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	J	I	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	J	I	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

Criptonálisis

Para llevar a cabo el descifrado de un mensaje haciendo uso de una tabla de Vigenère, no hay más que proceder de forma inversa. Ahora los papeles de filas y columnas se intercambian respecto al cifrado:

- Comenzamos buscando en la fila de *Texto en claro* el primer carácter de la clave, y bajamos ahora por su columna hasta encontrar el primer carácter del criptograma.
- En ese momento, nos movemos hacia la izquierda, hasta llegar a la columna de Clave de cifrado, donde encontraremos ya la letra correspondiente del mensaje descifrado.