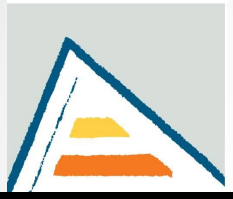


Introducción a la criptografía

Elementos de la Seguridad Informática

- Confidencialidad:
  - El acceso a la información se permite únicamente a entidades autorizadas

mantener el mensaje secreto

- Disponibilidad:
  - La información ha de estar siempre accesible para entidades autorizadas

mantener el servicio funcional

- Integridad:
  - La información puede ser creada o modificada únicamente por entidades autorizadas

mantener el mensaje intacto

- Autenticidad:
  - No hay duda del origen de la información

evitar la suplantación de identidad

Criptosistema Clásicos

Escítal espartana

- Descrita por Plutarco (Grecia, siglos I-II d. C.)
- Consiste en dos varas idénticas: una para el emisor y otra para el receptor
- Para escribir el mensaje, se enrollaba alrededor de la vara una tira larga y se escribía de arriba abajo y de derecha a izquierda
- Para descifrar el mensaje, se enrolla el papiro sobre una vara idéntica
- El primer ejemplo de escritura secreta del que se tiene constancia es del siglo V a. C. (Guerra entre Atenas y Esparta)
- Cifrado por transposición

Escítal espartana

Cifrado d Polybios

- Del siglo II a. C., es el cifrador por sustitución más antiguo que se conoce.
- El texto cifrado duplica en tamaño al texto en claro:

no es un buen sistema

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

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

M_1 = QUE BUENA IDEA

C_1 = DA DE AE AB DE AE

CC AA BD AD AE EA

?

M_2 = LA DEL GRIEGO

C_2 = 31 11 14 15 31 22

42 24 15 22 34

Cifrado de Julio César

- El historiador romano Suetonio, contemporáneo de Plutarco, nos describe un sistema de ***cifrado*** utilizado por ***Julio César*** (siglo I a.C.):
  - "...Para quienes deseen saber más diré que sustituía la primera letra del alfabeto, A, por D y así sucesivamente con todas las demás...".
- También el emperador Augusto parece que utilizaba un sistema muy similar:
  - "...cada vez que escribía en código, ponía una B en lugar de A, C en lugar de B y así sucesivamente con todas las letras restantes...".
- El sistema de cifrado de César o de Augusto se basa en la sustitución de letras.

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

Cifrado de Julio César

- La frase que pronunció en una expedición militar cuando tras bajarse de una barca cayó de bruces

  TENEO TE AFRICA

  en lenguaje cifrado se escribe como:

  AHQHR AH DIVMFD

- Para descifrar un mensaje en clave bastaba con girar, para cada letra, el círculo cifrario tres posiciones en el sentido contrario al de las agujas del reloj. Así

  BOHM BMGM BMFM

  significa

  VENI VIDI VICI

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

Cifrado de Julio César

- Es un cifrador por sustitución en el que las operaciones se realizan módulo n, con n siendo el número de elementos del alfabeto.

m = **E**L PATIO D**E** MI CASA **E**S PARTICULAR

c = **H**Ñ SDWLR D**H** OL FDVD **H**V SDUWLFXÑDU

Cada letra se cifrará siempre igual: es una debilidad

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

Atbash hebreo

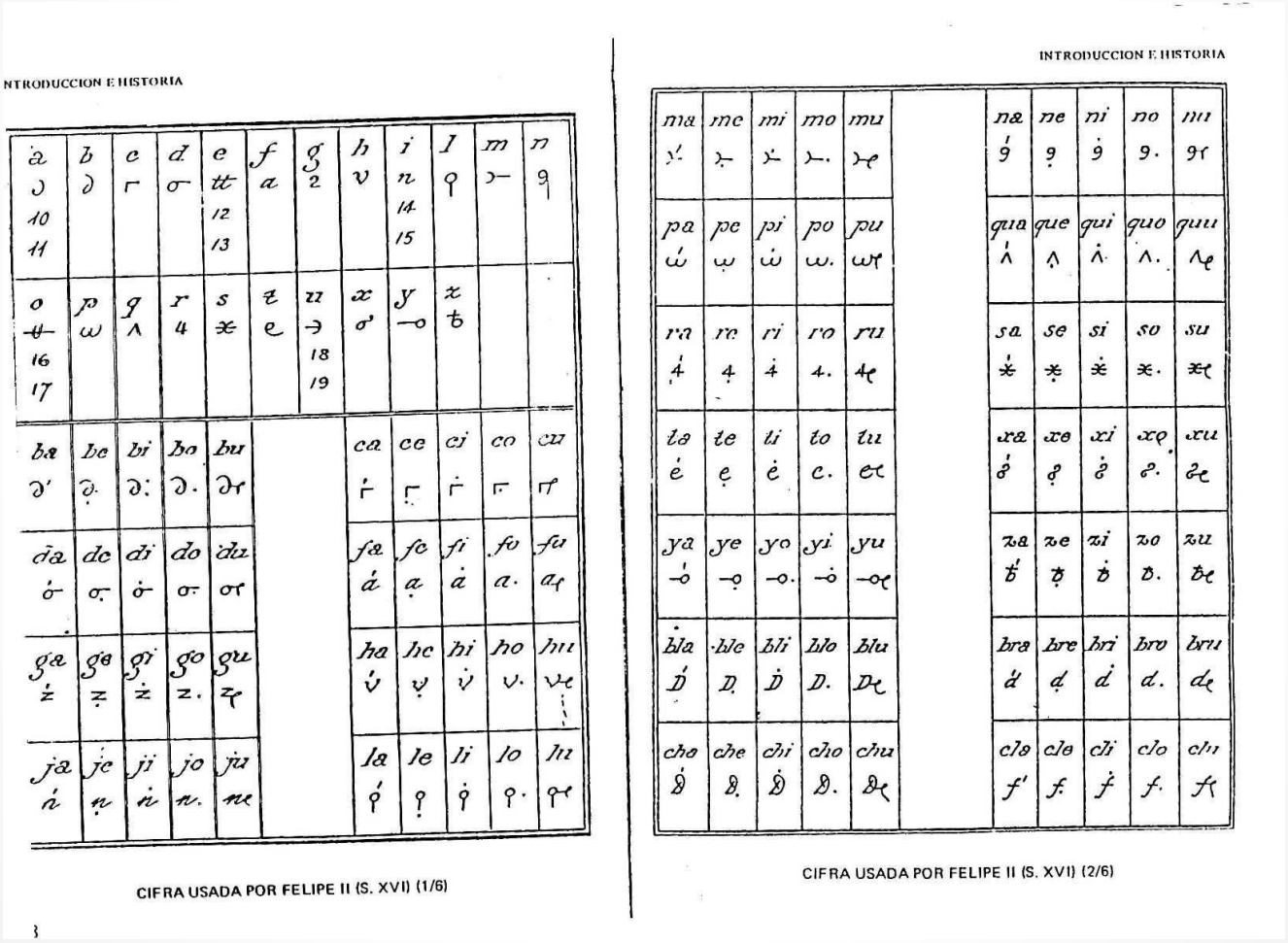
- Se escriben las letras del alfabeto en 2 líneas
- La primera mitad en la primera línea de izquierda a derecha
- La segunda mitad en la segunda línea de derecha a izquierda
- Cada letra se sustituye por la situada en la otra línea:

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

La cifra de Felipe II

- En España, como en el resto de Europa, el uso de información cifrada era generalizado en el ámbito diplomático y militar.
- Merece especial mención la cifra, utilizada por Felipe II (siglo XVI) en la correspondencia con el Duque de Alba en las importantes misiones exteriores de éste.
- Se compone de seis tablas divididas en cuatro grupos de casillas en los que aparecen las letras del alfabeto, las parejas y los tríos de letras más comunes y las palabras que se supone se van a utilizar con más frecuencia.
- A cada casilla corresponde uno o más signos no convencionales formados por letras, números o trazos especiales.

La cifra de Felipe II



NTRODUCCION E HISTORIA

a 10 11	b	c	d	e tt 12 13	f a	g 2	h v	i n 14 15	l ϙ	m	n ϥ
o 16 17	p ω	q ʌ	r 4	s ϰ	t e	u 18 19	x σ'	y	z b		

ba ∂'	be ∂.	bi ∂:	bo ∂.	bu ∂ר		ca ⊢	ce ⊢	ci ⊢	co ⊢	cu ⊓
da ȯ	de σ.	di ȯ	do σ.	du σר		fa ȧ	fe ȧ	fi ȧ	fo a.	fu aϥ
ga ż	ge ż	gi ż	go z.	gu zϥ		ha v̇	he v̇	hi v̇	ho v.	hu vϵ
ja ṅ	je ṅ	ji ṅ	jo n.	ju nϵ		la ϙ́	le ϙ	li ϙ	lo ϙ.	lu ϙר

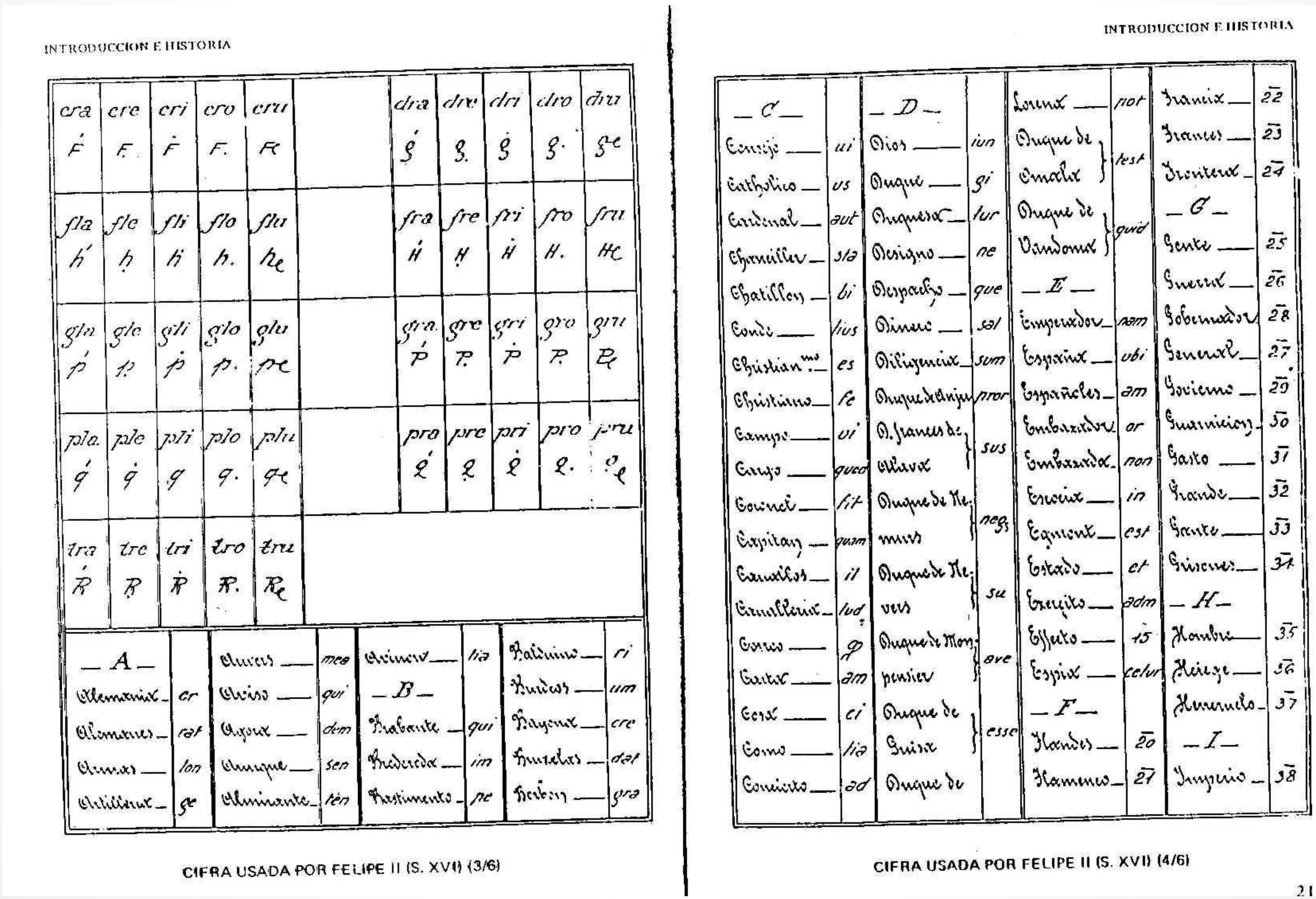
CIFRA USADA POR FELIPE II (S. XVI) (1/6)

INTRODUCCION E HISTORIA

ma ɔ́	me ɔ	mi ɔ	mo ɔ.	mu ɔϵ		na ϥ́	ne ϥ	ni ϥ	no ϥ.	nu ϥר
pa ώ	pe ω	pi ώ	po ω.	pu ωר		qua ʌ́	que ʌ	qui ʌ̇	quo ʌ.	quu ʌϥ
ra 4́	re 4	ri 4̇	ro 4.	ru 4ϥ		sa ϰ́	se ϰ	si ϰ̇	so ϰ.	su ϰר
ta ė	te ę	ti ė	to c.	tu eר		xa ȯ́	xe ȯ	xi ȯ	xo ȯ.	xu ȯר
ya ó	ye ǫ	yo o.	yi ȯ	yu oר		za b́	ze b	zi ḃ	zo b.	zu bϵ
bla D́	ble D	bli Ḋ	blo D.	blu Dϵ		bra d́	bre d	bri ḋ	bro d.	bru dϵ
cha ∂̇	che ∂.	chi ∂̇	cho ∂.	chu ∂ϵ		cla f'	cle f.	cli ḟ	clo f.	clu fϵ

CIFRA USADA POR FELIPE II (S. XVI) (2/6)

La cifra de Felipe II



La cifra de Felipe II

Italia	39	Ministro	lum	— P —		Rey	79
Inglaterra	40	Moulac	id	Papa	63	Reyno	81
Ingleses	41	Montigni	mel	Principe	64	Republica	82
Infantes	42	Mas	fa	Provincia	65	Remedio	83
Infanteria	43	Menos	ciet	Persona	66	Respuesta	84
Inquisicion	44	— N —		Provision	67	Resolucion	85
Intelligencia	45	Negocio	51	Porque	68	Raistres	86
Importancia	46	Necesidad	52	Para	69	Reyna	80
— L —		Navio	53	Paraque	70	— S —	
Lucemburg	47	Nuncio	54	Pero	71	Su Mag.d	87
Lutherano	48	Noncarme	55	Puerto	72	Su Alt.a	88
Liga	49	Navarra	56	— Q —		Su Exc.a	89
Libertad	50	Ni una	57	Quando	73	Savoya	90
Lorena	sed	— O —		Quanto	74	Suyo	91
Licencia	qu	Obispo	58	Qualidad	75	Suyos	92
Luego	od	Oracion	59	Quantidad	76	Señor	93
— M —		Orden	60	Qual	77	Servicio	94
Memoransi	csl	Officio	61	Quan	78	Secretario	95
Monpensier	amo	Oranges	62	— R —		Secreto	96

CIFRA USADA POR FELIPE II (S. XVI) (5/6)

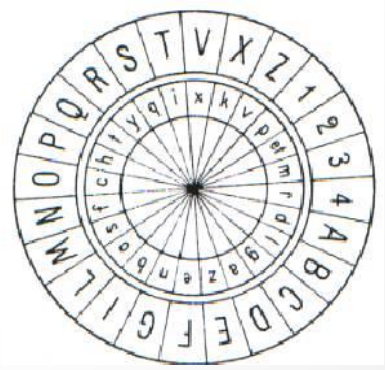
Suceso	97	Tratado	99	V. Mag.d	cre	Villa	fri
Siempre	98	Turco	bli	V. Exc.a	cri	Virrey	fro
— T —		Tanto	blo	V. S.a	cro	Venecia	fru
Tercio	98s	Todo	blu	V. m.	cru	Vejenote	gui
Tierra	bla	Toda	cra	Vuestro	fra		
Tiempo	ble	— V —		Vuestra	fre		

Nulas seran todas las letras dictiones o numeros despues de los quales se siguiere una ·S· entre dos puntos y todo el renglon que comencare en una :N· entre dos puntos, o parte del hasta topar una +.

CIFRA USADA POR FELIPE II (S. XVI) (6/6)

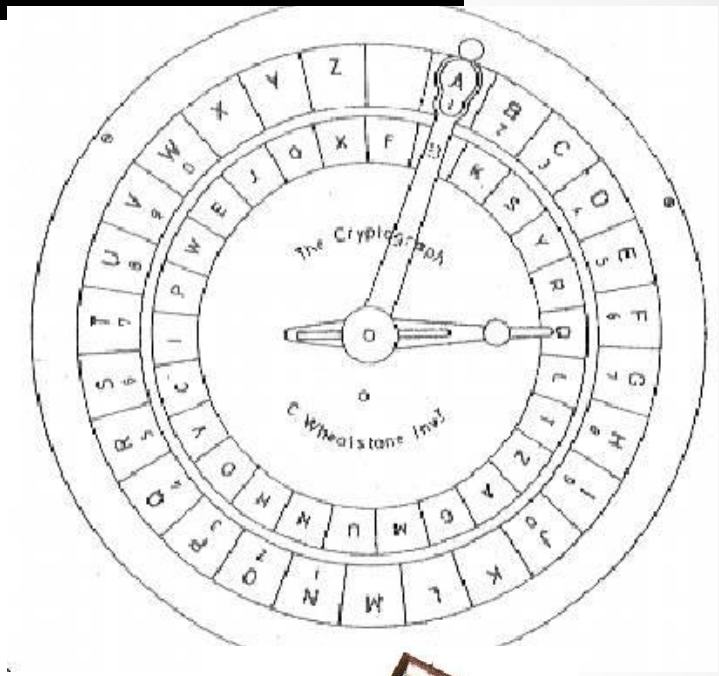
E cifrado de Alberti

- En los siglos XVI y XVII se utiliza muy activamente la Criptología, pero no hay grandes progresos en la aparición de nuevos métodos, todos están basados en la sustitución.
- Leon Battista Alberti diseña en el siglo XVI un disco para cifrar en el que ya no hay una correspondencia única entre el carácter del texto en claro a cifrar y el criptograma obtenido.
- Como este tipo de cifradores hacía uso de más de un alfabeto, se les conoce como polialfabéticos; en contraste con los anteriores que se denominan monoalfabéticos.
- En este caso, se hace uso ya de una clave secreta al ajustar en una posición los discos antes de cifrar



Cifradore del siglo XIX

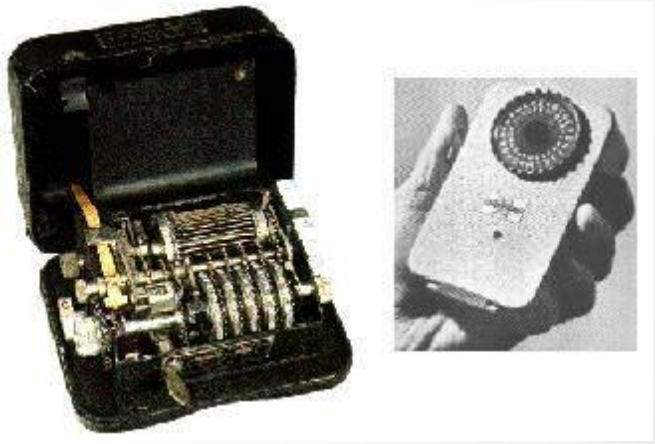
- En el siglo XIX aparece una nueva técnica (ya utilizada en cierto modo por los griegos) consistente en la alteración del orden de los símbolos del mensaje. Esta técnica es combinada con la sustitución.



- Se utilizan máquinas de cifrar, como las de *Wheatstone* y *Brazeries*.

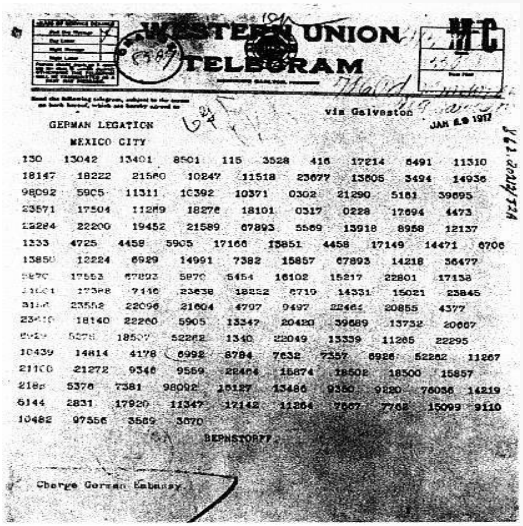
Siglo XX: antes del ordenador

- El empujón decisivo para la criptología se produce en el siglo pasado con motivo de las Guerras Mundiales.
- Se desarrollan diversas máquinas de cifrado con rotores que permiten un cifrado polialfabético.
- De estas máquinas, cuyo papel principal fue su utilización para enviar mensajes cifrados precisamente en la Segunda Guerra Mundial, destacan tanto por sus características como por el halo de misterio que rodeaba a dos de ellas:
  - la máquina Enigma y la de Hagelin.



Siglo XX: antes del ordenador

- Durante la Primera Guerra Mundial los ingleses consiguieron averiguar el método de cifrado del telegrama ***Zimmerman***.
  - Utilizado por los alemanes, usaba un código para asignar cifras a las palabras de acuerdo con un libro de claves que poseían el emisor y el receptor del mensaje.
- Los franceses desmantelaron otro método utilizado por los alemanes, el sistema ***ADFGX.***
  - Usaba tan solo esas letras para sustituir cada letra del mensaje sin cifrar por una combinación de dos de esas cinco letras, realizando posteriormente una transposición de longitud 20. La sustitución se hacía con la tabla


WESTERN UNION TELEGRAM

via Galveston

JAN 16 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
15224 22290 19452 21589 67893 5569 13918 8958 12137
1233 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
9870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7110 23638 18552 6719 14331 15021 23845
3110 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5870 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52282 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
6144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070

BERNSTORFF

Charge German Embassy

	A	D	F	G	X
A	n	b	x	r	u
D	q	o	k	d	v
F	a	h	s	g	f
G	m	z	c	l	t
X	e	i	p	j	w

Siglo XX: antes del ordenador

ADFGX

El mensaje

PETAIN MONTAG ATTENTAT

(Petain Lunes Atentado)

una vez hecha la sustitución, quedaría como

XFXAGXFAXDAA GGAXAAGX|FAFG FAGXGXXAAAGXFAGX

y realizando la transposición

XFFAXFAGGFXAFGAXXGDXAXAAGAGAAGXXAFAAGGXX

Siglo XX: después del ordenador

- Aparecen los ordenadores:
  - los métodos de cifrado anteriores resultan sumamente vulnerables por la capacidad de cálculo de los mismos.

- Los criterios utilizados para cifrar mensajes:
  - se establecen pensando en el posible ataque al sistema mediante un ordenador.

- Se habla así de sistemas:
  - computacionalmente seguros
  - computacionalmente inseguros

Visión histórica

- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.

- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
  - En el año 1948 se publica el estudio de C. Shannon sobre la Teoría de la Información.
  - En 1974 aparece el estándar de cifrado DES.
  - En el año 1976 se publica el estudio realizado por W. Diffie y M. Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.

Terminología

- Cifrar / Descifrar

*(no se **usaba** encriptar, pero ahora lo admite la RAE, desencriptar no está aceptado)*

- Texto en claro / Texto cifrado (o criptograma)

el texto en claro se cifra para obteniendo texto cifrado y viceversa

- Criptosistema / Cifrador

todo algoritmo de cifrado es un criptosistema, también hay otras primitivas criptográficas (herramientas útiles en criptografía) que no son cifradores

- Clave / Espacio de claves

La clave es la entrada que determina la transformación realizada por un criptosistema, una contraseña es una entrada del usuario (que generalmente se transforma en una clave).

El espacio de claves es el número de claves posibles y determina la dificultad inicial de romper el criptosistema por fuerza bruta (búsqueda exhaustiva)

- Criptología / Criptografía / Criptoanálisis

La criptografía estudia el diseño de criptosistemas y el cifrado de mensajes; el criptoanálisis estudia como romper criptosistemas y obtener los mensajes cifrados sin conocer la clave; la criptología es la ciencia que combina el estudio de ambas.

Primitivas criptográficas

Disponemos de las siguientes primitivas o herramientas que estudiaremos a lo largo del curso:

- Criptografía simétrica (clave privada):
  - Cifrado en flujo
  - Cifrado en bloque
- Criptografía asimétrica (clave pública):
  - Cifrado
  - Firma digital
- Primitivas auxiliares:
  - PRNG (pseudoaleatoriedad)
  - Funciones Hash (resumen)
  - Funciones MAC (autentificación)
  - PBKDF (contraseñas)

Ampliación

Otros materiales

- Se puede consultar el capítulo 9 del libro de Lucena
(en los materiales de UACloud)

Cuestiones

- ¿Serían seguros los esquemas de criptografía clásica en la actualidad? ¿Por qué?

- ¿Cuáles son las principales diferencias entre los algoritmos clásicos y los modernos basados en computación?