BORRADOR ACTUALIZABLE

15-abr-19

Estrategias de Seguridad

Antonio Zamora Gómez
José Vicente Aguirre Pastor
Departamento de Ciencia de la Computación e Inteligencia Artificial
Unidad de Criptología y Seguridad Computacional
Universidad de Alicante

Tema 1
Introducción a la Seguridad de la Información

1.1) La frase que pronunció Julio César cuando decidió atravesar el Rubicón con sus legiones para llegar a Roma: "*La suerte está echada*", en lenguaje cifrado se escribe

DOHD MDFAD HXA

Descífrala para obtener la frase original en latín.

Solución:

Obtengamos en primer lugar la tabla de cifrado

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

El mensaje original es

ALEA IACTA EST

1.2) ¿Cuál de los siguientes criptogramas fue enviado por Julio César y cuál por César Augusto?
a) DBGHQAHX IRVABQD MBBDA
b) GFTVKOB MFOVF

Solución:

Obtengamos en primer lugar las tablas de cifrado

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

a) Utilizando el cifrado de Julio Cesar obtenemos

AVDENTES FORTVNA IVVAT*

mientras que con el cifrado de Cesar Augusto obtenemos

CAFGPX....

b) Utilizando el cifrado de Julio Cesar obtenemos una secuencia de letras sin sentido

DCQ....

En cambio, con el cifrado de Cesar Augusto obtenemos

FESTINA LENTE†

1.3) Utilizando una scitala de ocho filas y seis columnas cifra:

a) La frase que coreaban los soldados de Julio César en su triunfo sobre las Galias: *"Ciudadanos, guardad vuestras mujeres: llevamos un libertino calvo"*

VRBANI, SERVATE VXORES: MOECHVM CALVOM ADDVCIMVS

b) La frase que dijo de él Curio padre en un discurso: *"Marido de todas las mujeres y mujer de todos los maridos"*

OMNIVM MVLIERVM VIRVM ET OMNIVM VIRORVM MVLIE-REM

Solución:

a) Escribimos la frase en la tabla

V	S	V	M	C	D
R	E	X	O	A	D
B	R	O	E	L	V
A	V	R	C	V	C
N	A	E	H	O	I
I	T	S	V	M	M
,	E	;	M	_	V
_	_	_	_	A	S

y obtenemos

VSUMCDREXOADBROELVAURCVCNAEHOIITSVMM,E:M_V____AS

* La suerte ayuda a los audaces.

† Apresúrate con lentitud.

b) De igual forma, utilizando la tabla

O	V	V	_	V	M
M	L	I	O	I	V
N	I	R	M	R	L
I	E	V	N	O	I
V	R	M	I	R	E
M	V		V	V	R
_	M	E	M	M	E
M	_	T	_	_	M

obtenemos
OVV_VMMLIOIVNIRMRLIEVNOIVRMIREMV_VVR _MEMMEM_T__M

1.4) Encuentra el texto en claro correspondiente al criptograma
c=AE_NMHIIOMNRVIRSSE_STME_
sabiendo que se ha utilizado una scitala de ocho filas y tres columnas.

Solución:

Distribuimos los símbolos del criptograma en una tabla de ocho filas y tres columnas como sigue.

A	E	_
N	M	H
I	I	O
M	N	R
V	I	R
S	S	E
_	S	T
M	E	_

Realizando la lectura por columnas obtenemos el siguiente texto en claro
ANIMVS MEMINISSE HORRET*

* Mi ánimo tiembla de horror al recordar.

1.5) Utiliza el sistema de cifrado ADFGX para cifrar el mensaje
m=ARBEIT MACHT FREI*
escrito en la entrada del campo de concentración de Auschwitz.

Solución:

Utilizamos la tabla

	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

para obtener el criptograma

FAAGADXAXDGX_GAFAGFFDGX_FXAGXAXD

FAAGADXAXDGXGAFAGFFD
GXFXAGXAXD

c= FGAXAFGXAADGXXAAXXDDGXGAFAGFFD

1.6) Enumera y describe a grandes rasgos qué tres aspectos fundamentales hay que garantizar para mantener un sistema seguro (o fiable).

Solución:

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.
La confidencialidad exige que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.
La integridad significa que los objetos sólo pueden ser creados o modificados por elementos autorizados y de una manera controlada.
La disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

* El trabajo nos hace libres.

1.7) Enumera y describe a grandes rasgos los tres principales elementos a proteger en cualquier sistema informático.

Solución:

Debemos proteger principalmente el hardware, el software y los datos.
Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario o tarjetas de red.
Por software entendemos el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones.
Por datos entendemos el conjunto de información lógica que manejan el software y el hardware
(como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos).

1.8) Enumera y describe a grandes rasgos los cuatro grandes grupos de amenazas a la seguridad.

Solución:

Generalmente, la clasificación más elemental de las amenazas a la seguridad se divide en cuatro grandes grupos: interrupción, interceptación, modificación y generación. Un ataque se clasifica como interrupción si hace que un objeto del sistema no esté disponible; como interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema; como modificación si además de conseguir el acceso consigue modificar el objeto y como generación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el fabricado

1.9) Decribe, brevemente, los términos criptografía, criptoanálisis y criptología.

Solución:

La ciencia que estudia el diseño de criptosistemas es conocida como criptografía.
La ciencia que intenta romper los criptosistemas, descifrando en un tiempo razonable el contenido de un mensaje sin conocer la clave, es llamada criptoanálisis.
Los campos de la criptografía y el criptoanálisis, son conocidos en su conjunto como criptología

1.10) La seguridad perfecta requiere que la longitud de la clave sea mayor o igual que la del texto en claro. ¿Porqué este resultado teórico hace que los criptosistemas con seguridad perfecta sean inútiles en la práctica?

Solución:

Porque si la clave debe ser tanto o más larga que el texto en claro, a la hora de protegerla nos encontraremos con el mismo problema que teníamos para proteger el texto en claro.

Tema 2
Criptografía clásica

2.1) La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX. El punto de inflexión en la clasificación de los criptosistemas como clásicos o modernos lo marcan tres hechos relevantes acaecidos en 1948, 1974 y 1976. Explica en qué consistieron.

Solución:

En el año 1948 se publica el estudio de C. Shannon sobre la Teoría de la Información que sienta las bases para el tratamiento científico de la criptología.
En 1974 aparece el estándar de cifrado DES que de facto a sido el estándar mundial hasta hace poco.
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. Este hecho ha revolucionado las comunicaciones modernas ya que permite compartir claves a través de canales inseguros.

2.2) Un criptoanalista afirma que el criptograma

c=ALXB TH HKRRRRRYV

ha sido obtenido cifrando mediante un sistema de sustitución simple un mensaje escrito en castellano. ¿Es cierto?

Solución:

No es cierto.
Observamos que la letra R aparece repetida 5 veces. Si el método de cifrado fuese de sustitución simple, la cadena de caracteres

HKRRRRRYV

correspondería a una palabra en castellano en la que una letra se repite cinco veces.
Las cinco R deben corresponder, por tanto, a símbolos distintos.

Nota:
Si R corresponde al espacio en blanco, puede ser cierto.

2.3) Cifra tu nombre y apellidos utilizando un método de sustitución simple en el que se aplica la transformación $c_i=E_k(m_i)=(11m_i+2) \bmod 28$ al alfabeto
A={_ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}
Obtén la transformación de descifrado D_k.

Solución:

Aplicamos la siguiente asignación numérica

_	A	B	C		D	E	F	G	H	I	J	K	L	M
0	1	2	3		4	5	6	7	8	9	10	11	12	13

N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26	27

para obtener el criptograma de ANTONIO ZAMORA GOMEZ

	A	*N*	*T*	*O*	*N*	*I*	*O*	*_*	*Z*	*A*	*M*	*O*	*R*	*A*	*_*	*G*	*O*	*M*	*E*	*Z*
m_i	1	14	21	16	14	9	16	0	27	1	13	16	19	1	0	7	16	13	5	27
c_i	13	16	9	10	16	17	10	2	19	13	5	10	15	13	2	23	10	5	1	19
	M	O	I	J	O	P	J	B	R	M	E	J	Ñ	M	B	V	J	E	A	R

La función de descifrado se obtiene haciendo uso de la aritmética modular, se tiene $c_i= (11m_i+2) \bmod 28 \rightarrow c_i-2 = 11m_i \bmod 28 \rightarrow m_i= [(c_i-2)11^{-1}] \bmod 28$, luego

$$D_k(c_i) = m_i= [(c_i-2)11^{-1}] \bmod n$$

El inverso de 11 mod 28 es 23 ya que $11\cdot 23 = 253$ y $253 \bmod 28 = 1$

$28 = 2 \cdot 11 + 6 \rightarrow 6 = 28 - 2 \cdot 11 \bmod 28 = (-2) \cdot 11 \bmod 28;$
$11 = 1 \cdot 6 + 5 \rightarrow 5 = 11 - 6 \bmod 28 = 11 - (-2) \cdot 11 \bmod 28 = 3 \cdot 11 \bmod 28;$
$6 = 1 \cdot 5 + 1 \rightarrow \mathbf{1} = 6 - 5 \bmod 28 = (-2) \cdot 11 - 3 \cdot 11 \bmod 28 = (-5) \cdot 11 \bmod 28 =$
$= \mathbf{23} \cdot 11 \bmod 28.$

Por tanto

$$D_k(c_i) = [(c_i-2)23] \bmod 28$$

Así, por ejemplo

$D_k(M) = D_k(13) = [(13-2)23] \bmod 28 = 1 = A$
$D_k(O) = D_k(16) = [(16-2)23] \bmod 28 = 14 = N$
$D_k(I) = D_k(9) = [(9-2)23] \bmod 28 = 21 = T$
⋮

La tabla de sustitución (cifrado-descifrado) general es la que sigue

Claro		*Cifrado*	
_	0	2	B
A	1	13	M
B	2	24	W
C	3	7	G
D	4	18	Q
E	5	1	A
F	6	12	L
G	7	23	V
H	8	6	F
I	9	17	P

Claro		*Cifrado*	
J	10	0	_
K	11	11	K
L	12	22	U
M	13	5	E
N	14	16	O
Ñ	15	27	Z
O	16	10	J
P	17	21	T
Q	18	4	D

Claro		*Cifrado*	
R	19	15	Ñ
S	20	26	Y
T	21	9	I
U	22	20	S
V	23	3	C
W	24	14	N
X	25	25	X
Y	26	8	H
Z	27	19	R

2.4) Repite el ejercicio anterior con el alfabeto
A={ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}
utilizando módulo 27.

Solución:

En este caso la tabla de sustitución (cifrado-descifrado) es

m_i		c_i	
A	0	2	C
B	1	13	N
C	2	24	X
D	3	8	I
E	4	19	S
F	5	3	D
G	6	14	Ñ
H	7	25	Y
I	8	9	J

m_i		c_i	
J	9	20	T
K	10	4	E
L	11	15	O
M	12	26	Z
N	13	10	K
Ñ	14	21	U
O	15	5	F
P	16	16	P
Q	17	0	A

m_i		c_i	
R	18	11	L
S	19	22	V
T	20	6	G
U	21	17	Q
V	22	1	B
W	23	12	M
X	24	23	W
Y	25	7	H
Z	26	18	R

y el criptograma correspondiente a

m=ANTONIO ZAMORA GOMEZ

es

c = CKGFKJF_RCZFLC_ÑFZSR

El inverso de 11 mod 27 es 5, ya que 11·5= 55 y 55 mod 27 = 1

$27 = 2 \cdot 11 + 5 \rightarrow\ 5 = 27 - 2 \cdot 11 \text{ mod } 27 = (-2)\, 11 \text{ mod } 27;$
$11 = 2 \cdot 5 + 1 \rightarrow\ 1 = 11 - 2 \cdot 5 \text{ mod } 27 = 11 - 2\,(-2)\, 11 \text{ mod } 27 = \mathbf{5} \cdot 11 \text{ mod } 27;$

Por tanto

$$D_k(c_i) = [(c_i - 2)5] \text{ mod } 27$$

Así, por ejemplo

$D_k(C) = D_k(2) = [(2\text{-}2)5] \bmod 27 = 0 = A$

$D_k(K) = D_k(10) = [(10\text{-}2)5] \bmod 27 = 13 = N$

$\vdots$

2.5) Un equipo de delincuentes informáticos ha interceptado un mensaje cifrado que se transmite entre dos sucursales bancarias, tras meses de intento. El mensaje contiene la clave de acceso a las bases de datos para el día. Se sabe que el sistema criptográfico que utilizan es de sustitución simple y que a las letras C e I del texto en claro le corresponden C y Z respectivamente en el criptograma. El alfabeto utilizado es

A={ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}

a) ¿Pueden obtener la clave utilizada con estos datos?

b) Si la clave es cambiada y sólo se conoce que la letra M del texto en claro se corresponde con la M del texto cifrado, ¿pueden obtener la clave?

Solución:

a) Supongamos que se ha realizado la siguiente asignación numérica al alfabeto de 27 letras

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
14	15	16	17	18	19	20	21	22	23	24	25	26

La función de cifrado debe tener la forma

$$E_k(m_i) = (r\, m_i + k) \bmod 27$$

Sabemos que

$$E_k(2) = (2r + k) \bmod 27 = 2 \bmod 27$$
$$E_k(8) = (8r + k) \bmod 27 = 26 \bmod 27$$

Resolviendo el sistema

$$\left.\begin{array}{l} 2r + k = 2 \bmod 27 \\ 8r + k = 26 \bmod 27 \end{array}\right\}$$

obtenemos

$$6\,r = 24 \bmod 27 \longrightarrow \quad r = 4 \bmod 27$$
$$y = -6 \bmod 27 = 21 \bmod 27$$

Por tanto la función de cifrado es

$$E_k(m_i) = (4m_i + 21) \bmod 27$$

b) No es posible ya que basta tomar r tal que

$$\text{mcd}(r,27) = 1$$

para que exista D_k.

Si r=2 entonces

$$E_k(M) = E_k(12) \quad = 2\ 12 + k = 12 \bmod 27$$
$$\Rightarrow\ k = -12 = 15 \bmod 27$$

Si r=4 entonces

$$E_k(M) = E_k(12) \quad = 4\ 12 + k = 12 \bmod 27$$
$$\Rightarrow k = -36 = 18 \bmod 27$$

Tenemos 2 claves

$$r = 2 \quad k = 15$$

y

$$r = 4 \quad k = 18$$

Por este mismo procedimiento se pueden obtener todas las posibles claves.

2.6) Consideremos el alfabeto

A={_ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}

Mediante un método de sustitución simple en el que

$$c_i = 3m_i + 8 \bmod 28$$

a) Obtén la tabla de sustitución (cifrado-descifrado).

b) Cifra el mensaje m=ESTA_NOCHE_FUEGO.

c) Sin hacer uso del apartado a), descifra el criptograma

c=CKIFQVHSVHN_RNVI_L

d) Realiza un estudio sobre las frecuencias de aparición de letras en el texto en claro del apartado b) y del criptograma en el apartado c) e intenta obtener la clave.

Solución:

a) La tabla de sustitución (cifrado-descifrado) es la que sigue

_	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
0	1	2	3	4	5	6	7	8	9	10	11	12	13
8	11	14	17	20	23	26	1	4	7	10	13	16	19
H	K	N	P	S	V	Y	A	D	G	J	M	O	R

N	*Ñ*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
14	15	16	17	18	19	20	21	22	23	24	25	26	27
22	25	0	3	6	9	12	15	18	21	24	27	2	5
U	X	_	C	F	I	L	Ñ	Q	T	W	Z	B	E

b) Sustituyendo en la tabla, el criptograma que obtenemos es

c = VLÑKHU_PDVHYQVA_

c) El inverso de $r = 3 \bmod 28$ es $r^{-1} = 19$, por lo que la función de descifrado viene dada por

$$m_i = D_k(c_i) = [(c_i-8)19] \bmod 28$$

28 = 9 ·3 + 1 → 1 = 28 - 9·3 mod 28 = 19·3 mod 28.

Por tanto

$$
\begin{aligned}
D_k(C) &= D_k(3) = 17 = P\\
D_k(K) &= D_k(11) = 1 = A\\
D_k(I) &= D_k(9) = 19 = R\\
D_k(F) &= D_k(6) = 18 = Q\\
D_k(Q) &= D_k(18) = 22 = U\\
D_k(V) &= D_k(23) = 5 = E\\
D_k(H) &= D_k(8) = 0 = \_\\
D_k(S) &= D_k(20) = 4 = D\\
D_k(V) &= D_k(23) = 5 = E\\
D_k(H) &= D_k(8) = 0 = \_\\
D_k(N) &= D_k(14) = 2 = B\\
D_k(\_) &= D_k(0) = 16 = O\\
D_k(R) &= D_k(19) = 13 = M\\
D_k(N) &= D_k(14) = 2 = B\\
D_k(V) &= D_k(23) = 5 = E\\
D_k(I) &= D_k(9) = 19 = R\\
D_k(\_) &= D_k(0) = 16 = O\\
D_k(L) &= D_k(12) = 20 = S
\end{aligned}
$$

Luego

m = PARQUE_DE_BOMBEROS

d) Para el texto en claro, m, obtenemos las siguientes frecuencias

Letra	E	S	T	A	_	N
Frecuencia	3	1	1	1	2	1
%	18'75	6'25	6'25	6'25	12'5	6'25

Letra	O	C	H	F	U	G
Frecuencia	2	1	1	1	1	1
%	12'5	6'25	6'25	6'25	6'25	6'25

y para el criptograma, c, obtenemos

Letra	C	K	I	F	Q	V
Frecuencia	1	1	2	1	1	3
%	5’55	5’55	11’1	5’55	5’55	16'7

Letra	H	S	N	_	R	L
Frecuencia	2	1	2	2	1	1
%	11’1	5’55	11’1	11’1	5’55	5’55

Si suponemos que a la letra más frecuente en m se le asocia la más frecuente en c tendremos

$$C_k(E) = C_k(5) = V = 23$$

En m, los símbolos _ y O son igual de frecuentes y están en segundo lugar. En c, ocurre esto con I,H,N y _.

En total hay 4 posibilidades de asociación para _. Supongamos que

$$C_k(\_) = C_k(0) = H = 8^{*}$$

Tendremos que si $C_k(m_i) = rm_i + k \bmod 28$ es la función de cifrado, entonces

$$\left.\begin{array}{l} 5r + k = 23 \bmod 28 \\ 0r + k = \ \ 8 \bmod 28 \end{array}\right\} \Rightarrow r = 3 \ \ k = 8$$

Luego la clave es r=3 y k=8.

2.7) Se desea cifrar el mensaje
"ES EVIDENTE QUE UN GOBIERNO NO PUEDE DECIR LO QUE PIENSA A LOS MERCADOS FINANCIEROS, PERO NO ES MENOS OBVIO QUE RESULTA SUICIDA MANTENER UNA DIVISA CONTRA VIENTO Y MAREA. APUESTO POR TOMAR UNA DECISIÓN VALIENTE, AUNQUE ARRIESGADA, QUE NO ES OTRA QUE DEVALUAR SIN ESPERAR A QUE LOS MERCADOS OBLIGUEN A ELLO, SIN AGUARDAR POSTERIORES CONDICIONAMIENTOS"
mediante un sistema mixto: las consonantes se cifrarán mediante un sistema de sustitución simple y las vocales mediante uno homofónico.
a) Obtén las frecuencias de aparición de las vocales en el texto en claro.
b) Describe el método que utilizarías para que las frecuencias obtenidas en el apartado anterior no sean significativas en el criptograma.

Solución:

a) Obtenemos

Vocal	A	E	I	O	U
Frecuencia	31	41	23	29	18
%	21’8	28’9	16’2	20’4	12’7
% Aproximación	20	30	15	20	15

b) Para cifrar las vocales utilizaría 20 símbolos: las 5 letras que no tuviesen descifrado al utilizar sustitución simple con las consonantes y quince números. Si esas letras son $l_1,...,l_5$ y los números 1,...,15, usaría la siguiente tabla de cifrado para equilibrar las frecuencias.

* Tenemos la ventaja de conocer el apartado a).

Texto en claro	A	E	I	O	U
Criptograma	l_1 1 2 3	l_2 4 5 6 7 8	l_3 9 10	l_4 11 12 l3	l_5 14 15

De esa manera los 20 símbolos aparecerán un 5% de veces aproximadamente.

2.8) Si se pretende utilizar el método Vigenère para cifrar un mensaje, ¿qué palabra clave resulta más conveniente?

TE, CAFETÍN, POLEO o MANZANILLA

Solución:

Resulta más conveniente CAFETÍN ya que tiene siete letras distintas, mientras que MANZANILLA (palabra más larga) sólo posee seis.

2.9) El siguiente criptograma se ha cifrado utilizando el método Vigenère.

PL ÑGTMCG OIY RPL KSE

Se sabe que la clave está guardada en un cajón que contiene las siguientes palabras

CAJA, LOZA, MAYO, MOTO, CALA, META, LAZO, MOYA

Averigua cuál es la clave utilizada y obtén el texto en claro.

Solución:

Observemos que todas las claves tienen longitud 4 por lo que se han utilizado cuatro alfabetos.
Suponemos que el espacio en blanco no está cifrado y dividimos el criptograma en bloques de cuatro letras.

	PLÑG	***TMCG***	***OIYR***	***PLKS***	***E***
Clave 1	CAJA	...	...	...	...
sin sentido	ÑLFG	...	...	...	...
Clave 2	LOZA	...	...	...	...
sin sentido	FWOG	...	...	...	...
Clave 3	MAYO	MAYO	MAYO	MAYO	M
	ELPR	IMER	DIAD	ELME	S

Luego la clave es

k = MAYO

y el texto en claro

m = EL PRIMER DIA DEL MES

2.10) Utilizando el código ASCII binario cifra el mensaje m=SAL mediante el método Vernam. La clave utilizada es YES.

Solución:

Obtengamos en primer lugar los códigos ASCII

LETRA	*ASCII*	*BINARIO*
S	83	01010011
A	65	01000001
L	76	01001100
Y	89	01011001
E	69	01000101

La codificación la obtenemos en la siguiente tabla.

SAL	83 65 76	01010011	01000001	01001100
YES	89 69 83	01011001	01000101	01010011
LF│EOT│ US	10 04 31	00001010	00000100	00011111

2.11) Sabiendo que se ha usado el método Vernam para aplicar un doble cifrado con claves k_1=10011100 y k_2=00111100, ¿cuál es el texto en claro del criptograma c=00001111?

Solución:

En el método de Verman el algoritmo de descifrado es idéntico al de cifrado. Tenemos por tanto.

c	0	0	0	0	1	1	1	1	=	15	⟶	SI
k_1	1	0	0	1	1	1	0	0	=	156	⟶	£
	1	0	0	1	0	0	1	1	=	147	⟶	ô
k_2	0	0	1	1	1	1	0	0	=	60	⟶	$<$
	1	0	1	0	1	1	1	1	=	175	⟶	»

Luego el texto en claro es

10101111

2.12) En el cifrado de Vernam con clave binaria aleatoria, ¿que tiene que ocurrir para que el criptograma obtenido al cifrar sea una serie de unos binarios?

Solución:

La clave debe ser el complemento a uno del texto en claro.

Tema 3
Cifrado en flujo con clave secreta

3.1) Descifra el criptograma c = |^M|É| = 13 144(ASCII) sabiendo que se ha utilizado el método Vernam con la secuencia cifrante de 16 bits obtenida mediante el algoritmo RC4 con 3 bits de salida por iteración y semilla k = [7,6,5,4,3,2,1,0].
El texto en claro corresponde a un elemento de la tabla periódica.
Ten en cuenta la siguiente tabla:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78
HEX	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E

	O	P	Q	R	S	T	U	V	W	X	Y	Z	^M	É
ASCII	79	80	81	82	83	84	85	86	87	88	89	90	13	144
HEX	4F	50	51	52	53	54	55	56	57	58	59	05	0D	90

Solución:

En este caso trabajaremos en 9_8 = {0,1,2,3,4,5,6,7}, la semilla es k=[7,6,5,4,3,2,1,0] y el algoritmo se utiliza con una salida de 3 bits por cada iteración del siguiente modo:

<u>Key Scheduling Algorithm (KSA)</u>

Para calcular los valores iniciales de la S-Caja, se hace lo siguiente:
1. S(i) = i $\forall$i{0,1,2,3,4,5,6,7}
2. Rellenar el array K(0) a K(7) repitiendo la clave tantas veces como sea necesario.
3. j = 0
4. Para i = 0 hasta 7 hacer:

j = [j + S(i) + K(i)] mod 8
Intercambiar S(i) y S(j) .

Pseudo-Random Generation Algorithm-PRGA

Se inicializan los índices i=0 y j=0.
En la iteración r, cada bloque de 3 bits, O_r, de la secuencia cifrante se calcula como sigue:
1. i = (i + 1) mod 8
2. j = [j + S(i)] mod 8
3. Intercambiar los valores de S(i) y S(j)
4. t = [S(i) + S(j)] mod 8
5. $O_r = S(t)_{(2)}$
6. Mientras se necesite secuencia cifrante volver a 1

Como por cada iteración obtenemos 3 bits y el criptograma tiene 16, necesitamos iterar 6 veces en el PRGA.

Key Scheduling Algorithm (KSA)

1. S=[S(0),S(1),S(2),S(3),S(4),S(5),S(6),S(7)]= [0,1,2,3,4,5,6,7]
   Semilla =[7,6,5,4,3,2,1,0]
2. K=[K(0),K(1),K(2),K(3),K(4),K(5),K(6),K(7)]= [7,6,5,4,3,2,1,0]
3. j= 0
4. i=0 (j=0, S=[0,1,2,3,4,5,6,7])
   j=[j+S(i)+K(i)] mod 8=[0+S(0)+K(0)] mod 8=(0+0+7) mod 8=7
   Intercambiar S(0) con S(7)
   S=[7,1,2,3,4,5,6,0]
4. i=1 (j=7, S=[7,1,2,3,4,5,6,0])
   j=[j+S(i)+K(i)] mod 8=[7+S(1)+K(1)] mod 8=(7+1+6) mod 8=6
   Intercambiar S(1) con S(6)
   S=[7,6,2,3,4,5,1,0]
4. i=2 (j=6, S=[7,6,2,3,4,5,1,0])
   j=[j+S(i)+K(i)] mod 8=[6+S(2)+K(2)] mod 8=(6+2+5) mod 8=5
   Intercambiar S(2) con S(5)
   S=[7,6,5,3,4,2,1,0]
4. i=3 (j=5, S=[7,6,5,3,4,2,1,0])
   j=[j+S(i)+K(i)] mod 8=[5+S(3)+K(3)] mod 8=(5+3+4) mod 8=4
   Intercambiar S(3) con S(4)
   S=[7,6,5,4,3,2,1,0]
4. i=4 (j=4, S=[7,6,5,4,3,2,1,0])
   j=[j+S(i)+K(i)] mod 8=[4+S(4)+K(4)] mod 8=(4+3+3) mod 8=2
   Intercambiar S(4) con S(2)
   S=[7,6,3,4,5,2,1,0]
4. i=5 (j=2, S=[7,6,3,4,5,2,1,0])
   j=[j+S(i)+K(i)] mod 8=[2+S(5)+K(5)] mod 8=(2+2+2) mod 8=6
   Intercambiar S(5) con S(6)

S=[7,6,3,4,5,1,2,0]
4. i=6 (j=6, S=[7,6,3,4,5,1,2,0])
j=[j+S(i)+K(i)] mod 8=[6+S(6)+K(6)] mod 8=(6+2+1) mod 8=1
Intercambiar S(6) con S(1)
S=[7,2,3,4,5,1,6,0]
4. i=7 (j=1, S=[7,2,3,4,5,1,6,0])
j=[j+S(i)+K(i)] mod 8=[1+S(7)+K(7)] mod 8=(1+0+0) mod 8=1
Intercambiar S(7) con S(1)
S=[7,0,3,4,5,1,6,2]

Pseudo-Random Generation Algorithm (PRGA)

S=[S(0),S(1),S(2),S(3),S(4),S(5),S(6),S(7)]= [7,0,3,4,5,1,6,2]
i=0,j=0

Iteración 1 (i=0, j=0, S=[7,0,3,4,5,1,6,2])
1. i=(i+1) mod 8=(0+1) mod 8=1
2. j=[j+S(i)] mod 8=[0+S(1)] mod 8=(0+0) mod 8=0
3. Intercambiar S(1) con S(0) -> S=[0,7,3,4,5,1,6,2]
4. t=[S(i)+S(j)] mod 8=[S(1)]+S(0)] mod 8=(7+0) mod 8=7
5. O1=S(t)=S(7)=2=$010_{(2)}$

Iteración 2 (i=1, j=0, S=[0,7,3,4,5,1,6,2])
1. i=(i+1) mod 8=(1+1) mod 8=2
2. j=[j+S(i)] mod 8=[0+S(2)] mod 8=(0+3) mod 8=3
3. Intercambiar S(2) con S(3) -> S=[0,7,4,3,5,1,6,2]
4. t=[S(i)+S(j)] mod 8=[S(2)]+S(3)] mod 8=(4+3) mod 8=7
5. O2=S(t)=S(7)=2=$010_{(2)}$

Iteración 3 (i=2, j=3, S=[0,7,4,3,5,1,6,2])
1. i=(i+1) mod 8=(2+1) mod 8=3
2. j=[j+S(i)] mod 8=[3+S(3)] mod 8=(3+3) mod 8=6
3. Intercambiar S(3) con S(6) -> S=[0,7,4,6,5,1,3,2]
4. t=[S(i)+S(j)] mod 8=[S(3)]+S(6)] mod 8=(6+3) mod 8=1
5. O3=S(t)=S(1)=7=$111_{(2)}$

Iteración 4 (i=3, j=6, S=[0,7,4,6,5,1,3,2])
1. i=(i+1) mod 8=(3+1) mod 8=4
2. j=[j+S(i)] mod 8=[6+S(4)] mod 8=(6+5) mod 8=3
3. Intercambiar S(4) con S(3) -> S=[0,7,4,5,6,1,3,2]
4. t=[S(i)+S(j)] mod 8=[S(4)]+S(3)] mod 8=(6+5) mod 8=3
5. O4=S(t)=S(3)=5=$101_{(2)}$

Iteración 5 (i=4, j=3, S=[0,7,4,5,6,1,3,2])
1. i=(i+1) mod 8=(4+1) mod 8=5
2. j=[j+S(i)] mod 8=[3+S(5)] mod 8=(3+1) mod 8=4
3. Intercambiar S(5) con S(4) -> S=[0,7,4,5,1,6,3,2]

4. t=[S(i)+S(j)] mod 8=[S(5)]+S(4)] mod 8=(6+1) mod 8=7
5. O5=S(t)=S(7)=2=010$_{(2)}$

Iteración 6 (i=5, j=4, S=[0,7,4,5,1,6,3,2])
1. i=(i+1) mod 8=(5+1) mod 8=6
2. j=[j+S(i)] mod 8=[4+S(6)] mod 8=(4+3) mod 8=7
3. Intercambiar S(6) con S(7) -> S=[0,7,4,5,1,6,2,3]
4. t=[S(i)+S(j)] mod 8=[S(6)]+S(7)] mod 8=(2+3) mod 8=5
5. O6=S(t)=S(5)=6=110$_{(2)}$

La secuencia de salida en 9_8 es 2,2,7,5,2,6; o sea: 010,010,111,101,010,110$_{(2)}$.

Nos quedamos con los 16 primeros bits como secuencia cifrante, esto es,
k_1= |0100|1011| |1101|0101|$_{(2)}$= 4B D5$_{(HEX)}$

Para descifrar c = | ^M|É| = 13 144$_{(ASCII)}$ = 0D 90$_{(HEX)}$ aplicamos Vernam

c = 0D 90$_{(HEX)}$ = |0000|1101| |1001|0000|$_{(2)}$
k_1 = 4B D5$_{(HEX)}$ = |0100|1011| |1101|0101|$_{(2)}$
m = 46 45$_{(HEX)}$ = |0100|0110| |0100|0101|$_{(2)}$ = 70 69$_{(ASCII)}$ = FE

3.2) Descifra el criptograma c = |^E|,|~| = 05 44 126$_{(ASCII)}$ sabiendo que se ha utilizado el método Vernam con la secuencia cifrante de 24 bits obtenida mediante el algoritmo RC4 con 2 bits de salida por iteración y semilla k = [2,1,3].
El texto en claro corresponde a un condimento de cocina.
Ten en cuenta la siguiente tabla:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78
HEX	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E

	O	P	Q	R	S	T	U	V	W	X	Y	Z	^E	,	~
ASCII	79	80	81	82	83	84	85	86	87	88	89	90	05	44	126
HEX	4F	50	51	52	53	54	55	56	57	58	59	05	20	2C	7E

Solución:

En este caso trabajaremos en 9_4= {0,1,2,3}, la semilla utilizada es k = [2,1,3] y el algoritmo se utiliza con una salida de 2 bits por cada iteración del siguiente modo:

<u>Key Scheduling Algorithm (KSA)</u>

Para calcular los valores iniciales de la S-Caja, se hace lo siguiente:

1. $S(i) = i \quad \forall i \in \{0,1,2,3\}$
2. Rellenar el array K(0) a K(3) repitiendo la clave tantas veces como sea necesario.
3. j = 0
4. Para i = 0 hasta 3 hacer:
   j = [j + S(i) + K(i)] mod 4
   Intercambiar S(i) y S(j) .

Pseudo-Random Generation Algorithm-PRGA

Se inicializan los índices i=0 y j=0.
En la iteración r, cada bloque de 2 bits, O_r, de la secuencia cifrante se calcula como sigue:
1. i = (i + 1) mod 4
2. j = [j + S(i)] mod 4
3. Intercambiar los valores de S(i) y S(j)
4. t = [S(i) + S(j)] mod 4
5. $O_r = S(t)_{(2)}$
6. Mientras se necesite secuencia cifrante volver a 1

Como por cada iteración obtenemos 2 bits y el criptograma tiene 24, necesitamos iterar 12 veces en el PRGA.

Key Scheduling Algorithm (KSA)

1. S=[S(0),S(1),S(2),S(3)]= [0,1,2,3]
   Semilla =[2,1,3]
2. K=[K(0),K(1),K(2),K(3)]= [2,1,3,2]
3. j= 0
4. i=0 (j=0, S=[0,1,2,3])
   j=[j+S(i)+K(i)] mod 4=[0+S(0)+K(0)] mod 4=(0+0+2) mod 4=2
   Intercambiar S(0) con S(2)
   S=[2,1,0,3]
4. i=1 (j=2, S=[2,1,0,3])
   j=[j+S(i)+K(i)] mod 4=[2+S(1)+K(1)] mod 4=(2+1+1) mod 4=0
   Intercambiar S(1) con S(0)
   S=[1,2,0,3]
4. i=2 (j=0, S=[1,2,0,3])
   j=[j+S(i)+K(i)] mod 4=[0+S(2)+K(2)] mod 4=(0+0+3) mod 4=3
   Intercambiar S(2) con S(3)
   S=[1,2,3,0]
4. i=3 (j=3, S=[1,2,3,0])
   j=[j+S(i)+K(i)] mod 4=[3+S(3)+K(3)] mod 4=(3+0+2) mod 4=1
   Intercambiar S(3) con S(1)
   S=[1,0,3,2]

Pseudo-Random Generation Algorithm (PRGA)

S=[S(0),S(1),S(2),S(3)]= [1,0,3,2]
i=0,j=0

Iteración 1 (i=0, j=0, S=[1,0,3,2])
1. i=(i+1) mod 4=(0+1) mod 4=1
2. j=[j+S(i)] mod 4=[0+S(1)] mod 4=(0+0) mod 4=0
3. Intercambiar S(1) con S(0) -> S=[0,1,3,2]
4. t=[S(i)+S(j)] mod 4=[S(1)]+S(0)] mod 4=(1+0) mod 4=1
5. O_1=S(t)=S(1)=1=$01_{(2)}$

Iteración 2 (i=1, j=0, S=[0,1,3,2])
1. i=(i+1) mod 4=(1+1) mod 4=2
2. j=[j+S(i)] mod 4=[0+S(2)] mod 4=(0+3) mod 4=3
3. Intercambiar S(2) con S(3) -> S=[0,1,2,3]
4. t=[S(i)+S(j)] mod 4=[S(2)]+S(3)] mod 4=(2+3) mod 4=1
5. O_2=S(t)=S(1)=1=$01_{(2)}$

Iteración 3 (i=2, j=3, S=[0,1,2,3])
1. i=(i+1) mod 4=(2+1) mod 4=3
2. j=[j+S(i)] mod 4=[3+S(3)] mod 4=(3+3) mod 4=2
3. Intercambiar S(3) con S(2) -> S=[0,1,3,2]
4. t=[S(i)+S(j)] mod 4=[S(3)]+S(2)] mod 4=(2+3) mod 4=1
5. O_3=S(t)=S(1)=1=$01_{(2)}$

Iteración 4 (i=3, j=2, S=[0,1,3,2])
1. i=(i+1) mod 4=(3+1) mod 4=0
2. j=[j+S(i)] mod 4=[2+S(0)] mod 4=(2+0) mod 4=2
3. Intercambiar S(0) con S(2) -> S=[3,1,0,2]
4. t=[S(i)+S(j)] mod 4=[S(0)]+S(2)] mod 4=(3+0) mod 4=3
5. O_4=S(t)=S(3)=2=$10_{(2)}$

Iteración 5 (i=0, j=2, S=[3,1,0,2])
1. i=(i+1) mod 4=(0+1) mod 4=1
2. j=[j+S(i)] mod 4=[2+S(1)] mod 4=(2+1) mod 4=3
3. Intercambiar S(1) con S(3) -> S=[3,2,0,1]
4. t=[S(i)+S(j)] mod 4=[S(1)]+S(3)] mod 4=(2+1) mod 4=3
5. O_5=S(t)=S(3)=1=$01_{(2)}$

Iteración 6 (i=1, j=3, S=[3,2,0,1])
1. i=(i+1) mod 4=(1+1) mod 4=2
2. j=[j+S(i)] mod 4=[3+S(2)] mod 4=(3+0) mod 4=3
3. Intercambiar S(2) con S(3) -> S=[3,2,1,0]
4. t=[S(i)+S(j)] mod 4=[S(2)]+S(3)] mod 4=(1+0) mod 4=1
5. O_6=S(t)=S(1)=2=$10_{(2)}$

Iteración 7 (i=2, j=3, S=[3,2,1,0])
1. i=(i+1) mod 4=(2+1) mod 4=3

2. j=[j+S(i)] mod 4=[3+S(3)] mod 4=(3+0) mod 4=3
3. Intercambiar S(3) con S(3) -> S=[3,2,1,0]
4. t=[S(i)+S(j)] mod 4=[S(3)]+S(3)] mod 4=(0+0) mod 4=0
5. O_7=S(t)=S(0)=3=$11_{(2)}$

Iteración 8 (i=3, j=3, S=[3,2,1,0])
1. i=(i+1) mod 4=(3+1) mod 4=0
2. j=[j+S(i)] mod 4=[3+S(0)] mod 4=(3+3) mod 4=2
3. Intercambiar S(0) con S(2) -> S=[1,2,3,0]
4. t=[S(i)+S(j)] mod 4=[S(0)]+S(2)] mod 4=(1+3) mod 4=0
5. O_8=S(t)=S(0)=1=$01_{(2)}$

Iteración 9 (i=0, j=2, S=[1,2,3,0])
1. i=(i+1) mod 4=(0+1) mod 4=1
2. j=[j+S(i)] mod 4=[2+S(1)] mod 4=(2+2) mod 4=0
3. Intercambiar S(1) con S(0) -> S=[2,1,3,0]
4. t=[S(i)+S(j)] mod 4=[S(1)]+S(0)] mod 4=(1+2) mod 4=3
5. O_9=S(t)=S(3)=0=$00_{(2)}$

Iteración 10 (i=1, j=0, S=[2,1,3,0])
1. i=(i+1) mod 4=(1+1) mod 4=2
2. j=[j+S(i)] mod 4=[0+S(2)] mod 4=(0+3) mod 4=3
3. Intercambiar S(2) con S(3) -> S=[2,1,0,3]
4. t=[S(i)+S(j)] mod 4=[S(2)]+S(3)] mod 4=(0+3) mod 4=3
5. O_{10}=S(t)=S(3)=3=$11_{(2)}$

Iteración 11 (i=2, j=3, S=[2,1,0,3])
1. i=(i+1) mod 4=(2+1) mod 4=3
2. j=[j+S(i)] mod 4=[3+S(3)] mod 4=(3+3) mod 4=2
3. Intercambiar S(3) con S(2) -> S=[2,1,3,0]
4. t=[S(i)+S(j)] mod 4=[S(3)]+S(2)] mod 4=(0+3) mod 4=3
5. O_{11}=S(t)=S(3)=0=$00_{(2)}$

Iteración 12 (i=3, j=2, S=[2,1,3,0])
1. i=(i+1) mod 4=(3+1) mod 4=0
2. j=[j+S(i)] mod 4=[2+S(0)] mod 4=(2+2) mod 4=0
3. Intercambiar S(0) con S(0) -> S=[2,1,3,0]
4. t=[S(i)+S(j)] mod 4=[S(0)]+S(0)] mod 4=(2+2) mod 4=0
5. O_{12}=S(t)=S(0)=2=$10_{(2)}$

La secuencia de salida en 9_4 es |1,1|1,2| |1,2|3,1| |0,3|0,2|. Esto es
k_1= |0101|0110| |0110|1101| |0011|0010|$_{(2)}$ = 56 6D 32$_{(HEX)}$

Para descifrar c = |^E|,|~| = 05 44 126$_{(ASCII)}$ = 05 2C 7E$_{(HEX)}$ aplicamos Vernam
c = 05 2C 7E$_{(HEX)}$ = |0000|0101| |0010|1100| |0111|1110|$_{(2)}$

k_1 = 56 6D 32$_{(HEX)}$ = |0101|0110| |0110|1101| |0011|0010|$_{(2)}$
m = 53 41 4C$_{(HEX)}$ = |0101|0011| |0100|0001| |0100|1100|$_{(2)}$ = 83 65 76$_{(ASCII)}$ = SAL

3.3) Descifra el criptograma c = Ë = 203$_{(ASCII)}$ sabiendo que se ha utilizado el método Vernam con la secuencia cifrante de 8 bits obtenida mediante el algoritmo RC4 con 4 bits de salida por iteración.
La clave para el algoritmo viene dada por la cadena de 64 bits obtenida a partir de la palabra ALIMENTO codificada en ASCII.
El texto en claro corresponde a una vocal.
Ten en cuenta la siguiente tabla:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78
HEX	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E

	O	P	Q	R	S	T	U	V	W	X	Y	Z	Ë
ASCII	79	80	81	82	83	84	85	86	87	88	89	90	203
HEX	4F	50	51	52	53	54	55	56	57	58	59	05	CB

Solución:

En este caso trabajaremos en 9_{16}= {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}.

Para obtener la semilla k, consideramos la cadena de 64 bits de la clave dividida en bloques de 4 bits expresados en su forma decimal, esto es

ALIMENTO → 65 76 73 77 69 78 84 79$_{(ASCII)}$ → 41 4C 49 4D 45 4E 54 4F$_{(HEX)}$ →
→ |0100|0001| |0100|1100|···|0100|1111|$_{(2)}$ → 4,1,4,12,4,9,4,13,4,5,4,14,5,4,4,15

La semilla para RC4 es, por tanto, k=[4,1,4,12,4,9,4,13,4,5,4,14,5,4,4,15].

El algoritmo se utiliza con una salida de 4 bits por cada iteración del siguiente modo:

<u>Key Scheduling Algorithm (KSA)</u>

Para calcular los valores iniciales de la S-Caja, se hace lo siguiente:
1. S(i) = i $\forall$i{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}
2. Rellenar el array K(0) a K(15) repitiendo la clave tantas veces como sea necesario.
3. j = 0
4. Para i = 0 hasta 15 hacer:
   j = [j + S(i) + K(i)] mod 16
   Intercambiar S(i) y S(j) .

<u>Pseudo-Random Generation Algorithm-PRGA</u>

Se inicializan los índices i=0 y j=0.
En la iteración r, cada bloque de 4 bits, O_r, de la secuencia cifrante se calcula como sigue:
1. i = (i + 1) mod 16
2. j = [j + S(i)] mod 16
3. Intercambiar los valores de S(i) y S(j)
4. t = [S(i) + S(j)] mod 16
5. $O_r = S(t)_{(2)}$
6. Mientras se necesite secuencia cifrante volver a 1

Como por cada iteración obtenemos 4 bits y el criptograma tiene 8, necesitamos iterar 2 veces en el PRGA.

<u>Key Scheduling Algorithm (KSA)</u>

1. S=[S(0),S(1),S(2),S(3),S(4),S(5),S(6),S(7),S(8),S(9),S(10),S(11),S(12),S(13),S(14),S(15)]= =[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]
   Semilla =[4,1,4,12,4,9,4,13,4,5,4,14,5,4,4,15]
2. K=[K(0),K(1),K(2),K(3),K(4),K(5),K(6),K(7),K(8),K(9),K(10),K(11),K(12),K(13),K(14),K(15)]= = [4,1,4,12,4,9,4,13,4,5,4,14,5,4,4,15]
3. j= 0
4. i=0 (j=0, S=[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15])
   j=[j+S(i)+K(i)] mod 16=[0+S(0)+K(0)] mod 16=(0+0+4) mod 16=4
   Intercambiar S(0) con S(4)
   S=[4,1,2,3,0,5,6,7,8,9,10,11,12,13,14,15]
4. i=1 (j=4, S=[4,1,2,3,0,5,6,7,8,9,10,11,12,13,14,15])
   j=[j+S(i)+K(i)] mod 16=[4+S(1)+K(1)] mod 16=(4+1+1) mod 16=6
   Intercambiar S(1) con S(6)
   S=[4,6,2,3,0,5,1,7,8,9,10,11,12,13,14,15]
4. i=2 (j=6, S=[4,6,2,3,0,5,1,7,8,9,10,11,12,13,14,15])
   j=[j+S(i)+K(i)] mod 16=[6+S(2)+K(2)] mod 16=(6+2+4) mod 16=12
   Intercambiar S(2) con S(12)
   S=[4,6,12,3,0,5,1,7,8,9,10,11,2,13,14,15]
4. i=3 (j=12, S=[4,6,12,3,0,5,1,7,8,9,10,11,2,13,14,15])
   j=[j+S(i)+K(i)] mod 16=[12+S(3)+K(3)] mod 16=(12+3+12) mod 16=11
   Intercambiar S(3) con S(11)
   S=[4,6,12,11,0,5,1,7,8,9,10,3,2,13,14,15]
4. i=4 (j=11, S=[4,6,12,11,0,5,1,7,8,9,10,3,2,13,14,15])
   j=[j+S(i)+K(i)] mod 16=[11+S(4)+K(4)] mod 16=(11+0+4) mod 16=15
   Intercambiar S(4) con S(15)
   S=[4,6,12,11,15,5,1,7,8,9,10,3,2,13,14,0]
4. i=5 (j=15, S=[4,6,12,11,15,5,1,7,8,9,10,3,2,13,14,0])
   j=[j+S(i)+K(i)] mod 16=[15+S(5)+K(5)] mod 16=(15+5+9) mod 16=13
   Intercambiar S(5) con S(13)
   S=[4,6,12,11,15,13,1,7,8,9,10,3,2,5,14,0]
4. i=6 (j=13, S=[4,6,12,11,15,13,1,7,8,9,10,3,2,5,14,0])
   j=[j+S(i)+K(i)] mod 16=[13+S(6)+K(6)] mod 16=(13+1+4) mod 16=2

Intercambiar S(6) con S(2)
S=[4,6,1,11,15,13,12,7,8,9,10,3,2,5,14,0]
4. i=7 (j=2, S=[4,6,1,11,15,13,12,7,8,9,10,3,2,5,14,0])
j=[j+S(i)+K(i)] mod 16=[2+S(7)+K(7)] mod 16=(2+7+13) mod 16=6
Intercambiar S(7) con S(6)
S=[4,6,1,11,15,13,7,12,8,9,10,3,2,5,14,0]
4. i=8 (j=6, S=[4,6,1,11,15,13,7,12,8,9,10,3,2,5,14,0])
j=[j+S(i)+K(i)] mod 16=[6+S(8)+K(8)] mod 16=(6+8+4) mod 16=2
Intercambiar S(8) con S(2)
S=[4,6,8,11,15,13,7,12,1,9,10,3,2,5,14,0]
4. i=9 (j=2, S=[4,6,8,11,15,13,7,12,1,9,10,3,2,5,14,0])
j=[j+S(i)+K(i)] mod 16=[2+S(9)+K(9)] mod 16=(2+9+5) mod 16=0
Intercambiar S(9) con S(0)
S=[9,6,8,11,15,13,7,12,1,4,10,3,2,5,14,0]
4. i=10 (j=0, S=[9,6,8,11,15,13,7,12,1,4,10,3,2,5,14,0])
j=[j+S(i)+K(i)] mod 16=[0+S(10)+K(10)] mod 16=(0+10+4) mod 16=14
Intercambiar S(10) con S(14)
S=[9,6,8,11,15,13,7,12,1,4,14,3,2,5,10,0]
4. i=11 (j=14, S=[9,6,8,11,15,13,7,12,1,4,14,3,2,5,10,0])
j=[j+S(i)+K(i)] mod 16=[14+S(11)+K(11)] mod 16=(14+3+14) mod 16=15
Intercambiar S(11) con S(15)
S=[9,6,8,11,15,13,7,12,1,4,14,0,2,5,10,3]
4. i=12 (j=15, S=[9,6,8,11,15,13,7,12,1,4,14,0,2,5,10,3])
j=[j+S(i)+K(i)] mod 16=[15+S(12)+K(12)] mod 16=(15+2+5) mod 16=6
Intercambiar S(12) con S(6)
S=[9,6,8,11,15,13,2,12,1,4,14,0,7,5,10,3]
4. i=13 (j=6, S=[9,6,8,11,15,13,2,12,1,4,14,0,7,5,10,3])
j=[j+S(i)+K(i)] mod 16=[6+S(13)+K(13)] mod 16=(6+5+4) mod 16=15
Intercambiar S(13) con S(15)
S=[9,6,8,11,15,13,2,12,1,4,14,0,7,3,10,5]
4. i=14 (j=15, S=[9,6,8,11,15,13,2,12,1,4,14,0,7,3,10,5])
j=[j+S(i)+K(i)] mod 16=[15+S(14)+K(14)] mod 16=(15+10+4) mod 16=13
Intercambiar S(14) con S(13)
S=[9,6,8,11,15,13,2,12,1,4,14,0,7,10,3,5]
4. i=15 (j=13, S=[9,6,8,11,15,13,2,12,1,4,14,0,7,10,3,5])
j=[j+S(i)+K(i)] mod 16=[13+S(15)+K(15)] mod 16=(13+5+15) mod 16=1
Intercambiar S(15) con S(1)
S=[9,5,8,11,15,13,2,12,1,4,14,0,7,10,3,6]

Pseudo-Random Generation Algorithm (PRGA)

S=[S(0),S(1),S(2),S(3),S(4),S(5),S(6),S(7),S(8),S(9),S(10),S(11),S(12),S(13),S(14),S(15)]=
[9,5,8,11,15,13,2,12,1,4,14,0,7,10,3,6]
i=0,j=0

Iteración 1 (i=0, j=0, S=[9,5,8,11,15,13,2,12,1,4,14,0,7,10,3,6])
1. i=(i+1) mod 16=(0+1) mod 16=1

2. j=[j+S(i)] mod 16=[0+S(1)] mod 16=(0+5) mod 16=5
3. Intercambiar S(1) con S(5) -> S=[9,13,8,11,15,5,2,12,1,4,14,0,7,10,3,6]
4. t=[S(i)+S(j)] mod 16=[S(1)]+S(5)] mod 16=(13+5) mod 16=2
5. O1=S(t)=S(2)=8=$1000_{(2)}$

Iteración 2 (i=1, j=5, S=[9,13,8,11,15,5,2,12,1,4,14,0,7,10,3,6])
1. i=(i+1) mod 16=(1+1) mod 16=2
2. j=[j+S(i)] mod 16=[5+S(2)] mod 16=(5+8) mod 16=13
3. Intercambiar S(2) con S(13) -> S=[9,13,10,11,15,5,2,12,1,4,14,0,7,8,3,6]
4. t=[S(i)+S(j)] mod 16=[S(2)]+S(13)] mod 16=(10+8) mod 16=2
5. O2=S(t)=S(2)=10=$1010_{(2)}$

La secuencia de salida en 9_{16} es 8,10; esto es k_1= $|1000|1010|_{(2)}$ = $8A_{(HEX)}$.

Para descifrar c = Ë = $203_{(ASCII)}$ = $CB_{(HEX)}$ aplicamos Vernam
c = $CB_{(HEX)}$ = $|1100|1011|_{(2)}$
k_1 = $8A_{(HEX)}$ = $|1000|1010|_{(2)}$
m = $41_{(HEX)}$ = $|0100|0001|_{(2)}$ = $65_{(ASCII)}$ = A

3.4) Describe, brevemente, el esquema fundamental de un cifrador en flujo (qué hace el emisor del mensaje m, que hace el receptor del criptograma c, …)

Solución:

Emisor y receptor comparten una clave corta y secreta, *k*.
E1 emisor, haciendo uso de un algoritmo determinista, genera a partir de *k* una secuencia binaria *S* cuyos elementos se suman módulo 2 con los correspondientes bits de texto claro *m*, dando lugar a los bits del criptograma *c* que envía al receptor a través de un canal público.
El receptor, con la misma clave *k* y el mismo algoritmo determinista, genera la misma secuencia binaria *S*, que se suma módulo 2 con la secuencia cifrada *c*, dando lugar a los bits del texto en claro *m*.

3.5) Todo registro de desplazamiento realimentado linealmente con n celdas tiene asociado un polinomio de realimentación de grado *n*. En el caso de que este polinomio sea primitivo, explica qué tipo de secuencia se obtendría.

Solución:

Las secuencias binarias que se obtienen no dependen del estado inicial del registro y tienen periodo máximo 2^n-1 (se las conoce como m-secuencias).

3.6) Explica brevemente las características generales del algoritmo de cifrado A5.

Solución:

El algoritmo A5 es un cifrador en flujo que genera la secuencia binaria cifrante utilizada para cifrar el enlace entre el teléfono móvil y la estación base en el sistema de telefonía móvil GSM (*Global Systems for Mobile communications*) o telefonía 2G.
Utiliza 3 LFSR con 19, 22 y 23 celdas que generan un periodo muy pequeño por lo que no es seguro. La longitud de clave es, por tanto, de 64 bits.

3.7) Explica brevemente las características generales del algoritmo de cifrado E0.

Solución:

El algoritmo E0 es un cifrador en flujo que genera la secuencia binaria cifrante utilizada para cifrar la información transmitida mediante tecnología Bluetooth.
Consta de 4 LFSR con 25, 31, 33 y 39 celdas por lo que la longitud de clave es de 128 bits.

Tema 4
Cifrado en bloque con clave secreta

4.1) Supongamos que las claves que utilizamos para cifrar con AES128 están constituidas por sólo diecisési letras mayúsculas del alfabeto castellano en código ASCII.
a) ¿Cuántas horas tardaremos en obtener la clave utilizada por búsqueda exhaustiva si suponemos que habrá que probar aproximadamente la mitad de todas las claves posibles y que el ordenador que utilizamos es capaz de comprobar la bondad de una clave en una millonésima de segundo?
b) ¿Y si la clave puede tener tanto letras mayúsculas como minúsculas?
c) ¿Y si además de letras puede contener números?

Solución:

El tamaño de la clave es de 128 bits, lo que equivale a dieciséis símbolos ASCII de ocho bits.
a) El alfabeto de claves es

ABCDEFGHYJKLMNÑOPQRSTUVWXYZ

de 27 letras.
En total hay PR_{27}^{16} claves distintas, esto es

$$27^{16} \cong 7'98\ 10^{22}$$

Si suponemos que hay que probar aproximadamente la mitad y que el ordenador que utilizamos es capaz de comprobar la bondad de una clave en una millonésima de segundo, el tiempo requerido es

$$\text{Tiempo} = \frac{7'98}{2}\frac{10^{22}}{10^{6}} \cong 3'99\ \ 10^{16}\ \text{seg.} \cong 1.264.688.659\ \ \text{años}$$

b) Ahora el espacio de claves posibles tiene

$$54^{16} \cong 5'23\ \ 10^{27}$$

elementos
Luego

$$\text{Tiempo} = \frac{5'23\ 10^{27}}{2\ \ 10^{6}} \cong 2'61\ \ 10^{21}\ \text{seg.} \cong 8'29\ \ 10^{13}\ \text{años}$$

c) El número total de claves es

$$64^{16} = 3'96\ \ 10^{28}$$

y

$$\text{Tiempo} = \frac{3'96\ 10^{28}}{2\ \ 10^{6}} \cong 3'96\ \ 10^{22}\ \text{seg.} \cong 1'26\ \ 10^{15}\ \text{años}$$

4.2) En los algoritmos de cifrado en bloque, por lo general, se utiliza un algoritmo de expansión de clave. Explica, brevemente, cual es la finalidad de esta expansión de clave.

Solución:

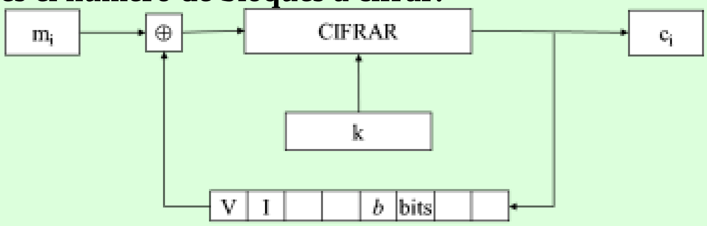
El algoritmo de expansión de clave tiene por objeto convertir la clave de cifrado en un conjunto de subclaves que pueden estar constituidas por varios cientos de bits en total. Utilizándose, por lo general, una subclave distinta en cada ronda del algoritmo de cifrado en bloque.
Conviene que sea unidireccional y que el conocimiento de una o varias subclaves intermedias no permita deducir las subclaves anteriores o siguientes; además, se ha de exigir que las subclaves producidas no constituyan un pequeño subconjunto repetido de todas las posibles.

4.3) Explica, brevemente, las características principales de AES: tipo de cifrado, tamaños de bloque y clave.

Solución:

AES es un algoritmo de cifrado en bloque con clave secreta, con un tamaño de bloque fijo de 128 bits y tres tamaños de clave elegibles de 128, 192 y 256 bits.

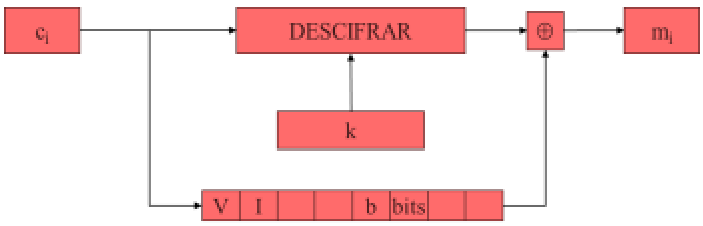
4.4) **Para un cifrador en bloque de *b* bits de tamaño de bloque, en el modo de cifrado CBC, para empezar se genera un vector inicial VI aleatorio de *b* bits con el que se carga el registro.**
Cada bloque m_i de *b* bits del texto en claro se cifra con la misma clave k y el bloque de salida c_i se realimenta hacia la entrada mediante el registro de *b* bits.
Para cifrar se aplica la recurrencia
$c_1 = E_k(m_1 \oplus VI)$; $c_i = E_k(m_i \oplus c_{i-1})$, para i = 2,3,···,n;
donde n es el número de bloques a cifrar.



Explica, brevemente, cómo se descifra escribiendo las ecuaciones de recurrencia.

Solución:

Para descifrar, cada bloque c_i de *b* bits del criptograma se descifra con la misma clave k y, al tiempo, alimenta el registro de *b* bits que se suma módulo 2 con la salida $D(c_i)$.
Se tiene
$D_k(c_1) = D_k[E_k(m_1 \oplus VI)] = m_1 \oplus VI$, luego **$m_1 = D_k(c_1) \oplus VI$**.
$D_k(c_i) = D_k[E_k(m_i \oplus c_{i-1})] = m_i \oplus c_{i-1}$, luego **$m_i = D_k(c_i) \oplus c_{i-1}$** para i = 2,3,···,n.



4.5) ¿En el algoritmo AES, cuál es el resultado de aplicar la función *DesplazarFila (ShiftRows)* a la matriz de estado

C2	**CB**	**C9**	**50**
89	**02**	**F4**	**69**
6E	**63**	**64**	**26**
27	**23**	**9A**	**FB**

Solución:

Esta transformación consiste en desplazar a la izquierda cíclicamente las filas de la matriz de estado.
Cada la fila f_i se desplaza un número de posiciones c_i diferente.
Mientras que c_0 siempre es igual a cero (esta fila siempre permanece inalterada), el resto de valores se refleja en la tabla

c_1	c_2	c_3
1	2	3

Tendremos, por tanto, la siguiente matriz de estado

C2	CB	C9	50
02	F4	69	89
64	26	6E	63
FB	27	23	9A

4.6) Explica, brevemente, las diferencias fundamentales entre cifradores en flujo y cifradores en bloque con clave secreta. Indica en qué tipo de tratamiento de la información los utilizarías y qué algoritmos.

Solución:

La diferencia fundamental es que los cifradores en bloque dividen la información en bloques de un determinado tamaño y aplican las mismas operaciones a cada bloque mientras que los cifradores en flujo, por lo general, dividen la información en bloques de un solo carácter (bit).
Lo habitual es que los cifradores en flujo sean más rápidos que los cifradores en bloque por lo que son recomendables cuando sea necesaria mayor eficiencia. Los algoritmos más utilizados son RC4 en flujo y AES en bloque.

4.7) Supongamos que las claves que utilizamos para cifrar con el DES están constituidas por sólo siete letras mayúsculas del alfabeto castellano en código ASCII.
a) ¿Cuántas horas tardaremos en obtener la clave utilizada por búsqueda exhaustiva si suponemos que habrá que probar aproximadamente la mitad de todas las claves posibles y que el ordenador que utilizamos es capaz de comprobar la bondad de una clave en una millonésima de segundo?
b) ¿Y si la clave puede tener tanto letras mayúsculas como minúsculas?
c) ¿Y si además de letras puede contener números?

Solución:

El tamaño de las clave es de 56 bits, lo que equivale a siete símbolos ASCII de ocho bits.

a) El alfabeto de claves es

ABCDEFGHYJKLMNÑOPQRSTUVWXYZ

de 27 letras.

En total hay PR_{27}^{7} claves distintas, esto es

$$27^7 = 1'046\ \ 10^{10}$$

Si suponemos que hay que probar aproximadamente la mitad y que el ordenador que utilizamos es capaz de comprobar la bondad de una clave en una millonésima de segundo, el tiempo requerido es

$$T = \frac{1'046\ \ 10^{10}}{2\ \ \ 10^{6}} = 5'23\ 10^{3}\,\text{s.} =$$

$$= 1'453 \text{ h.} = 1\text{h. } 27\text{m. } 10'18\text{s.}$$

b) Ahora el espacio de claves posibles tiene

$$54^7 = 1'339\ \ 10^{12}$$

elementos

Luego

$$T = \frac{1'339\ \ 10^{12}}{2\ \ \ 10^{6}} = 6'695\ \ 10^{5}\,\text{s.} =$$

$$= 185'96\ \text{ h.} = 7 \text{ dias } 17\text{h. } 57\text{m. } 42'48\text{s.}$$

c) El número total de claves es

$$64^7 = 4'389\ \ 10^{12}$$

y

$$T = \frac{4'398\ \ 10^{12}}{2\ \ \ 10^{6}} = 2'199\ \ 10^{6}\ \text{s.} =$$

$$= 610'84\ \text{ h.} = 25 \text{ dias } 10\text{h. } 50\text{m. } 23'25\text{ s.}$$

Tema 5
Cifrado con clave pública

5.1) Antonio y Blanca necesitan compartir una clave de siete bits haciendo uso del protocolo Diffie-Hellman. Acuerdan como primo p = 101 y como generador de $\mathbb{Z}_{101}$ el valor α=11. Si Antonio elige como clave privada el valor a=17 y Blanca el valor b=20, ¿qué clave comparten?

Solución:

Antonio calcula α^a mod p = 11^{17} mod 101 = 89 y se lo envía a Blanca.

17=**10001**$_{(2)}$

11 mod 101 = = **11** **1**
11^2 mod 101 = 11^2 mod 101 = 121 mod 101 = 20 **0**
11^4 mod 101 = 20^2 mod 101 = 400 mod 101 = 97 **0**
11^8 mod 101 = 97^2 mod 101 = 9409 mod 101= 16 **0**
11^{16} mod 101 = 16^2 mod 101 = 256 mod 101 = **54** **1**

11·**54** mod 101 = 89

Blanca calcula α^b mod p = 11^{20} mod 101 = 87 y se lo envía a Antonio.

20=**101000**$_{(2)}$

11 mod 101 = = 11 **0**
11^2 mod 101 = 11^2 mod 101 = 121 mod 101 = 20 **0**
11^4 mod 101 = 20^2 mod 101 = 400 mod 101 = **97** **1**
11^8 mod 101 = 97^2 mod 101 = 9409 mod 101 = 16 **0**
11^{16} mod 101 = 16^2 mod 101 = 256 mod 101 = **54** **1**

97·**54** mod 101 = 87

Antonio calcula 87^a mod 101 = 87^{17} mod 101 = 95 = $1011111_{(2)}$

17=$\mathbf{10001_{(2)}}$

87 mod 101 = = **87** **1**
87^2 mod 101 = 87^2 mod 101 = 7569 mod 101 = 95 **0**
87^4 mod 101 = 95^2 mod 101 = 9025 mod 101 = 36 **0**
87^8 mod 101 = 36^2 mod 101 = 1296 mod 101 = 84 **0**
87^{16} mod 101 = 84^2 mod 101 = 7056 mod 101 = **87** **1**

87·**87** mod 101 = 95

Blanca calcula 89^b mod 101 = 89^{20} mod 101 = 95 = $1011111_{(2)}$

20=$\mathbf{101000_{(2)}}$

89 mod 101 = = 89 **0**
89^2 mod 101 = 89^2 mod 101 = 7921 mod 101 = 43 **0**
89^4 mod 101 = 43^2 mod 101 = 1849 mod 101 = **31** **1**
89^8 mod 101 = 31^2 mod 101 = 961 mod 101 = 52 **0**
89^{16} mod 101 = 52^2 mod 101 = 2704 mod 101 = **78** **1**

31·**78** mod 101 = 95 = $1011111_{(2)}$

Luego la clave de siete bits que comparten es 1011111.

5.2) Alice y Bob desean intercambiar una clave de sesión mediante el protocolo Diffie-Hellman. Para ello acuerdan un número primo p=503 y un generador α=399 de $\mathbb{Z}_{503}$. Alice genera aleatoriamente un número privado a=257 y Bob otro número privado b=320.
a) Comprueba que el generador se ha elegido correctamente.
b) ¿Qué valor envía Alice a Bob?
c) ¿Qué valor envía Bob a Alice?
d) ¿Qué clave comparten?

Solución:

Recordemos que el número de generadores del grupo cíclico $\mathbb{Z}_{503}$ es $\Phi(\Phi(503))=\Phi(502)=\Phi(2\cdot251)=250$.

a) Un número $\alpha\in\mathbb{Z}_{503}$ es generador de $\mathbb{Z}_{503}$ si y sólo si para cada divisor primo, q, de $\Phi(503)$ se cumple $\alpha^{\Phi(503)/q}$ mod 503 $\neq$1.

Los divisores primos de $\Phi(503)$=502 son 2 y 251.

Se cumple

- $\alpha^{\Phi(503)/2} \bmod 503 = 399^{502/2} \bmod 503 = 399^{251} \bmod 503 = 502 \neq 1$,
- $\alpha^{\Phi(503)/251} \bmod 503 = 399^{502/251} \bmod 503 = 399^{2} \bmod 503 = 253 \neq 1$,

luego $\alpha=399$ es un generador de 9_{503}.

Hemos realizado los siguientes cálculos:

$251=$ **$11111011_{(2)}$**

$399 \bmod 503 =$ $=$ **399 1**

$399^{2} \bmod 503 = 399^{2} \bmod 503 = 159201 \bmod 503 =$ **253 1**

$399^{4} \bmod 503 = 253^{2} \bmod 503 = 64009 \bmod 503 =$ 128 **0**

$399^{8} \bmod 503 = 128^{2} \bmod 503 = 16384 \bmod 503 =$ **288 1**

$399^{16} \bmod 503 = 288^{2} \bmod 503 = 82944 \bmod 503 =$ **452 1**

$399^{32} \bmod 503 = 452^{2} \bmod 503 = 204304 \bmod 503 =$ **86 1**

$399^{64} \bmod 503 = 86^{2} \bmod 503 = 7396 \bmod 503 =$ **354 1**

$399^{128} \bmod 503 = 354^{2} \bmod 503 = 125316 \bmod 503 =$ **69 1**

399·**253** mod 503 = 347

347·**288** mod 503 = 342

342·**452** mod 503 = 163

163· **86** mod 503 = 437

437·**354** mod 503 = 277

277· **69** mod 503 = 502

b) Alice calcula $\alpha^{a} \bmod 503 = 399^{257} \bmod 503 = 311$ y se lo envía a Bob.

$257=$ **$100000001_{(2)}$**

$399 \bmod 503 =$ $=$ **399 1**

$399^{2} \bmod 503 = 399^{2} \bmod 503 = 159201 \bmod 503 = 253$ **0**

$399^{4} \bmod 503 = 253^{2} \bmod 503 = 64009 \bmod 503 = 128$ **0**

$399^{8} \bmod 503 = 128^{2} \bmod 503 = 16384 \bmod 503 = 288$ **0**

$399^{16} \bmod 503 = 288^{2} \bmod 503 = 82944 \bmod 503 = 452$ **0**

$399^{32} \bmod 503 = 452^{2} \bmod 503 = 204304 \bmod 503 = 86$ **0**

$399^{64} \bmod 503 = 86^{2} \bmod 503 = 7396 \bmod 503 = 354$ **0**

$399^{128} \bmod 503 = 354^{2} \bmod 503 = 125316 \bmod 503 = 69$ **0**

$399^{256} \bmod 503 = 69^{2} \bmod 503 = 4761 \bmod 503 =$ **234 1**

399·**234** mod 503 = 311

c) Bob calcula $\alpha^{b} \bmod 503 = 399^{320} \bmod 503 = 344$ y se lo envía a Alice.

$320=$ **$101000000_{(2)}$**

$399 \bmod 503 =$ $= 399$ **0**

$399^{2} \bmod 503 = 399^{2} \bmod 503 = 159201 \bmod 503 = 253$ **0**

$399^{4} \bmod 503 = 253^{2} \bmod 503 = 64009 \bmod 503 = 128$ **0**

399^{8} mod 503 = 128^{2} mod 503 = 6384 mod 503 = 288 **0**
399^{16} mod 503 = 288^{2} mod 503 = 82944 mod 503 = 452 **0**
399^{32} mod 503 = 452^{2} mod 503 = 204304 mod 503 = 86 **0**
399^{64} mod 503 = 86^{2} mod 503 = 7396 mod 503 = **354 1**
399^{128} mod 503 = 354^{2} mod 503 = 125316 mod 503 = 69 **0**
399^{256} mod 503 = 69^{2} mod 503 = 4761 mod 503 = **234 1**

354·**234** mod 503 = 344

d) Bob ha recibido 311 y calcula 311^{b} mod 503 = 311^{320} mod 503 = 184. Alice ha recibido 344 y calcula 344^{a} mod 503 = 344^{257} mod 503 = 184 luego la clave compartida es 184= $010111000_{(2)}$

Bob ha realizado los siguientes cálculos:
320=**101000000** $_{(2)}$

311 mod 503 = = 311 **0**
311^{2} mod 503 = 311^{2} mod 503 = 96721 mod 503 = 145 **0**
311^{4} mod 503 = 145^{2} mod 503 = 21025 mod 503 = 402 **0**
311^{8} mod 503 = 402^{2} mod 503 = 161604 mod 503 = 141 **0**
311^{16} mod 503 = 141^{2} mod 503 = 19881 mod 503 = 264 **0**
311^{32} mod 503 = 264^{2} mod 503 = 69696 mod 503 = 282 **0**
311^{64} mod 503 = 282^{2} mod 503 = 79524 mod 503 = **50 1**
311^{128} mod 503 = 50^{2} mod 503 = 2500 mod 503 = 488 **0**
311^{256} mod 503 = 488^{2} mod 503 = 238144 mod 503 = **225 1**

50·**225** mod 503 = 184

Alice ha realizado los siguientes cálculos:
257=**100000001**$_{(2)}$

344 mod 503 = = **344 1**
344^{2} mod 503 = 344^{2} mod 503 = 118336 mod 503 = 131 **0**
344^{4} mod 503 = 131^{2} mod 503 = 17161 mod 503 = 59 **0**
344^{8} mod 503 = 59^{2} mod 503 = 3481 mod 503 = 463 **0**
344^{16} mod 503 = 463^{2} mod 503 = 214369 mod 503 = 91 **0**
344^{32} mod 503 = 91^{2} mod 503 = 8281 mod 503 = 233 **0**
344^{64} mod 503 = 233^{2} mod 503 = 54289 mod 503 =468 **0**
344^{128} mod 503 = 468^{2} mod 503 = 219024 mod 503 = 219 **0**
344^{256} mod 503 = 219^{2} mod 503 = 47961 mod 503 = **176 1**

344·**176** mod 503 = 184

5.3) Sean p=13, q=17 y A={AB...NÑO...YZ} el alfabeto de textos en claro al que asignamos los números {2,3,....,27,28}.
a) Cifra la palabra CRIPTOGRAFIA utilizando clave pública e=11.
b) Descifra la secuencia numérica obtenida para recuperar la palabra original.

Solución:

En este caso $n = pq = 221$ y $\phi(n) = 12\ \ 16 = 192$

a) Si utilizamos e=11, la clave de cifrado es

$$k=(221,11)$$

El algoritmo de cifrado es

$$c = E_k(x) = x^{11} \bmod 221$$

Asignemos al texto en claro los correspondientes números.

m = CRIPTOGRAFIA = 04 20 10 18 22 17 08 20 02 07 10 02

Tenemos

$$\begin{aligned}
04^{11} \bmod 221 &= 4^{8+2+1} \bmod 221 = \\
&= \left(\left(4^2\right)^2\right)^2 4^2\ 4 \bmod 221 = \\
&= \left(16^2\right)^2 16\ 4 \bmod 221 = \\
&= (256)^2\ 16\ 4 \bmod 221 = \\
&= (35)^2 16\ 4 \bmod 221 = \\
&= 1225\ 16\ 4 \bmod 221 = \\
&= 120\ 16\ 4 \bmod 221 = \\
&= 166
\end{aligned}$$

O también

$4 \bmod 221$	=			=	**4**	**1**
$4^2 \bmod 221$	=	$4^2 \bmod 221$	= $16 \bmod 221$	=	**16**	**1**
$4^4 \bmod 221$	=	$16^2 \bmod 221$	= $256 \bmod 221$	=	35	**0**
$4^8 \bmod 221$	=	$35^2 \bmod 221$	= $1225 \bmod 221$	=	**120**	**1**

4 . **16** mod 221 = 64

64 . **120** mod 221 = 166

Análogamente

R	$20^{11} \bmod 221$	= 41
I	$10^{11} \bmod 221$	= 173

P	18^{11}	mod	221	=	86
T	22^{11}	mod	221	=	198
O	17^{11}	mod	221	=	153
G	08^{11}	mod	221	=	70
R	20^{11}	mod	221	=	41
A	02^{11}	mod	221	=	59
F	07^{11}	mod	221	=	184
I	10^{11}	mod	221	=	173
A	02^{11}	mod	221	=	59

Luego

c = 166 041 173 086 198 153 070 041 059 184 173 059

b) Necesitamos la clave de descifrado.

Como

$$\text{mcd}(e,n) = 1$$

buscamos

$$d = e^{-1} \bmod \phi(n)$$

Para d = 35

$$d\,e \bmod 192 = 385 \bmod 192 = 1$$

$$\boxed{\begin{array}{l} 192=17\cdot 11+5 \rightarrow 5=192-17\cdot 11 \bmod 192=-17\cdot 11 \bmod 192 \\ \;\; 11=\;2\cdot 5\;\;+1 \rightarrow 1=\;11-\;2\cdot 5\;\;\bmod 192=11-2(-17)11 \bmod 192 = 35\cdot 11\;\;\bmod 192 \end{array}}$$

Luego la clave es

$$k = (221,35)$$

y

$$D_k(x) = x^{35} \bmod 221$$

Tenemos entonces

$$\begin{aligned} 166^{35} \bmod 221 &= 166^{32}\, 166^{2}\, 166 \bmod 221 = \\ &= (166^{2})^{16}\, 166^{2}\, 166 \bmod 221 = \\ &= (152^{2})^{8}\, 152\; 166 \bmod 221 = \\ &= (120^{2})^{4}\, 152\; 166 \bmod 221 = \\ &= (35^{2})^{2}\;\; 152\; 166 \bmod 221 = \\ &= (120^{2})\;\; 152\; 166 \bmod 221 = \\ &= 35\; 152\; 166 \bmod 221 = \\ &= 35\; 38 \bmod 221 = \\ &= 4 = C \end{aligned}$$

O también

166	mod	221	=								=	**166**	**1**
166^{2}	mod	221	=	166^{2}	mod	221	=	27556	mod	221	=	**152**	**1**
166^{4}	mod	221	=	152^{2}	mod	221	=	23104	mod	221	=	120	**0**
166^{8}	mod	221	=	120^{2}	mod	221	=	14400	mod	221	=	35	**0**
166^{16}	mod	221	=	35^{2}	mod	221	=	1225	mod	221	=	120	**0**

$166^{32} \bmod 221 = 120^2 \bmod 221 = 14400 \bmod 221 =$ **35 1**

166 . **152** mod 221 = 38
38 . **35** mod 221 = 4

Análogamente, se comprueba para los demás que

$$041^{35} \bmod 221 = 20 = R$$

etcétera.

5.4) Consideremos un sistema de cifrado RSA en el que n=55 y e=7.
a) Cifra el número 10.
b) Factoriza n para obtener p y q y de esa manera descifrar el criptograma c=35.

Solución:

a) La clave es $k = (55,7)$ y $c = E_k(10) = 10^7 \bmod 55 = 10$

b) En este caso

$$n = 55 = 5\ 11 = p\ q$$

luego

$$\phi(n) = 4\ 10 = 40$$

Calculemos

$$d = e^{-1} \bmod 40 = 23$$

$40 = 5 \cdot 7 + 5 \rightarrow\ 5 = 40 - 5 \cdot 7 \bmod 40 = - 5 \cdot 7 \bmod 40;$
$7 = 1 \cdot 5 + 2 \rightarrow\ 2 = 7 - 1 \cdot 5 \bmod 40 = 7 - 1 \cdot (- 5 \cdot 7) \bmod 40 = 6 \cdot 7 \bmod 40;$
$5 = 2 \cdot 2 + 1 \rightarrow\ 1 = 5 - 2 \cdot 2 \bmod 40 = - 5 \cdot 7 - 2 \cdot (6 \cdot 7) \bmod 40 = -17 \cdot 7 \bmod 40$
$= (-17 + 40) \cdot 7 \bmod 40 = 23 \cdot 7 \bmod 40;$

Por tanto

$m = D_k(c) = D_k(35) =$
$= 35^{23} \bmod 55 =$
$= 35^{16+4+2+1} \bmod 55 =$
$= (35^2)^8 (35^2)^2\ 35^2\ 35 \bmod 55 =$
$= (15^2)^4\ 15^2\ 15\ 35 \bmod 55 =$
$= 5^4\ 5\ 15\ 35 \bmod 55 =$
$= 20\ 5\ 15\ 35 \bmod 55 =$
$= 20\ 5\ 30 \bmod 55 =$
$= 20\ 40 \bmod 55 =$
$= 30$

O también
$m = D_k(c) = D_k(35) = 35^{23} \bmod 55 = 30$

$35^{23} \bmod 55$

35	mod	55	=								=	**35**	**1**
35^2	mod	55	=	35^2	mod	55	=	1225	mod	55	=	**15**	**1**
35^4	mod	55	=	15^2	mod	55	=	225	mod	55	=	**5**	**1**
35^8	mod	55	=	5^2	mod	55	=	25	mod	55	=	25	**0**
35^{16}	mod	55	=	25^2	mod	55	=	625	mod	55	=	**20**	**1**

35	.	**15**	mod	55	=	30
30	.	**5**	mod	55	=	40
40	.	**20**	mod	55	=	30

5.5) En un criptosistema RSA en el que p=29 y q=31 descifra el número 126, sabiendo que la clave pública utilizada es e=17.

Solución:

En este problema el valor de n es

$$n = 29\ 31 = 899$$

por lo que

$$\phi(n) = 28\ 30 = 840$$

Tenemos

$$e=17$$

con lo que la clave de cifrado

$$k = (899,17)$$

Notemos que

$$\text{mcd}\,[e, \phi(n)] = \text{mcd}(17,840) = 1$$

Necesitamos

$$d = e^{-1} \bmod \phi(n)$$

Como

$$593\ 17 \bmod 840 = 10081 \bmod 840 = (12\ 840 + 1) \bmod 840 = 1$$

podemos afirmar que

$$d = 593$$

$840 = 49 \cdot 17 + 7 \rightarrow$	$7 = 840 + (-49)\ 17 \bmod 840 =$			$(-49)\ 17 \bmod 840 =$	$791 \cdot 17 \bmod 840$
$17 = 2 \cdot 7 + 3 \rightarrow$	$3 = 17 + (-2)\ 7 \bmod 840 =$	$1 \cdot 1 \cdot 17 + (-2)\ 791 \cdot 17 \bmod 840 =$		$(-1581)\ 17 \bmod 840 =$	$99 \cdot 17 \bmod 840$
$7 = 2 \cdot 3 + 1 \rightarrow$	$1 = 7 + (-2)\ 3 \bmod 840 =$	$1 \cdot 791 \cdot 17 + (-2)\ 99 \cdot 17 \bmod 840 =$		$(593)\ 17 \bmod 840 =$	$593 \cdot 17 \bmod 840$

La clave de descifrado es

$$k = (899,593)$$

y

$$D_k(x) = x^{593} \bmod 899$$

Descifremos 126.

$$126^{593} \bmod 899 = 126^{512+64+16+1} \bmod 899 =$$

$$= \left(126^2\right)^{256} \left(126^2\right)^{32} \left(126^2\right)^{8}\, 126 \bmod 899 =$$

$$= \left(593^2\right)^{128} \left(593^2\right)^{16} \left(593^2\right)^{4}\, 126 \bmod 899 =$$

$$= \left(140^2\right)^{64} \left(140^2\right)^{8} \left(140^2\right)^{2}\, 126 \bmod 899 =$$

$$= \left(\left(721\right)^2\right)^{32} \left(721^2\right)^{4}\, 721^2\, 126 \bmod 899 =$$

$$= \left(219^2\right)^{16} \left(219^2\right)^{2}\, 219\; 126 \bmod 899 =$$

$$= (314^2)^8\, 314^2\, 219\; 126 \bmod 899 =$$

$$= \left(605^2\right)^{4}\, 605\; 219\; 126 \bmod 899 =$$

$$= \left(132\right)^{4}\, 605\; 219\; 126 \bmod 899 =$$

$$= 779\; 605\; 219\; 126 \bmod 899 =$$

$$= 779\; 605\; 624 \bmod 899 =$$

$$= 779\; 839 \bmod 899 =$$

$$= 8$$

O también, dado que 593 = **1001010001**$_{(2)}$

$126 \bmod 899 =$ = **126 1**
$126^2 \bmod 899 = 126^2 \bmod 899 = 15876 \bmod 899$ = 593 **0**
$126^4 \bmod 899 = 593^2 \bmod 899 = 351649 \bmod 899$ = 140 **0**
$126^8 \bmod 899 = 140^2 \bmod 899 = 19600 \bmod 899$ = 721 **0**
$126^{16} \bmod 899 = 721^2 \bmod 899 = 519841 \bmod 899$ = **219 1**
$126^{32} \bmod 899 = 219^2 \bmod 899 = 47961 \bmod 899$ = 314 **0**
$126^{64} \bmod 899 = 314^2 \bmod 899 = 98596 \bmod 899$ = **605 1**
$126^{128} \bmod 899 = 605^2 \bmod 899 = 366025 \bmod 899$ = 132 **0**
$126^{256} \bmod 899 = 132^2 \bmod 899 = 17424 \bmod 899$ = 343 **0**
$126^{512} \bmod 899 = 343^2 \bmod 899 = 117649 \bmod 899$ = **779 1**

126 · **219** mod 899 = 624
624 · **605** mod 899 = 839
839 · **779** mod 899 = 8

Si suponemos que se realiza la asignación numérica

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*
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

se trata de la letra G.

5.6) Cifra la palabra CRIPTOGRAFIA utilizando un criptosistema RSA cuya clave pública viene dada por los valores n = 943 (p = 41, q = 23) y e = 7, de manera que el agrupamiento de caracteres haga que el criptograma se pueda codificar con el mismo alfabeto que el texto en claro.
El alfabeto que se debe emplear es {A,B,...,N,Ñ,O,...,Z,_} con asignación numérica {0,1,...,27}.

Solución:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	27

La asignación numérica de m = CRIPTOGRAFIA es la que sigue

m = 02 18 08 16 20 15 06 18 00 05 08 00

La función de cifrado viene dada por la expresión $c_i = E_k(m_i) = m_i^{\,7} \bmod 943$.
Cifraremos m agrupando en bloques de 2 caracteres, ya que $28^2 \leq 943 < 28^3$, esto es m = CR IP TO GR AF IA.

m_1 = CR = $(02)(18)_{(28)} = 02 \cdot 28 + 18 = 74$
m_2 = IP = $(08)(16)_{(28)} = 08 \cdot 28 + 16 = 240$
m_3 = TO = $(20)(15)_{(28)} = 20 \cdot 28 + 15 = 575$
m_4 = GR = $(06)(18)_{(28)} = 06 \cdot 28 + 18 = 186$
m_5 = AF = $(00)(05)_{(28)} = 00 \cdot 28 + 05 = 5$
m_6 = IA = $(08)(00)_{(28)} = 08 \cdot 28 + 00 = 224$

El valor más grande de c_i que se puede obtener es 942, que se puede expresar en base 28 como $942 = 1 \cdot 28^2 + 5 \cdot 28 + 18 = (01)(05)(18)_{(28)}$ = BFR; y por tanto codificar con tres caracteres del alfabeto de texto en claro.

$c_1 = E_k(m_1) = 74^7 \bmod 943 = 74^4 \cdot 74^2 \cdot 74 \bmod 943 = 119 \cdot 761 \cdot 74 \bmod 943$
$= 408 = 0 \cdot 28^2 + 14 \cdot 28 + 16 = (00)\,(14)\,(16)_{(28)}$ = AÑP
$c_2 = E_k(m_2) = 240^7 \bmod 943 = 750 = 0 \cdot 28^2 + 26 \cdot 28 + 22 = (0)\,(26)\,(22)_{(28)}$ = AZV
$c_3 = E_k(m_3) = 575^7 \bmod 943 = 575 = 0 \cdot 28^2 + 20 \cdot 28 + 15 = (0)\,(20)\,(15)_{(28)}$ = ATO
$c_4 = E_k(m_4) = 186^7 \bmod 943 = 749 = 0 \cdot 28^2 + 26 \cdot 28 + 21 = (0)\,(26)\,(21)_{(28)}$ = AZU
$c_5 = E_k(m_5) = 5^7 \bmod 943 = 799 = 1 \cdot 28^2 + 0 \cdot 28 + 15 = (1)\,(0)\,(15)_{(28)}$ = BAO
$c_6 = E_k(m_6) = 224^7 \bmod 943 = 112 = 0 \cdot 28^2 + 4 \cdot 28 + 0 = (0)\,(4)\,(0)_{(28)}$ = AEA

Tenemos

$c = E_k(m)$ = AÑP AZV ATO AZU BAO AEA

5.7) Cifra la palabra CRIPTOGRAFIA utilizando un criptosistema RSA cuya clave pública viene dada por los valores n = 221 (p = 13, q = 17) y e = 11, de manera que el agrupamiento de caracteres haga que el criptograma se pueda codificar con el mismo alfabeto que el texto en claro.
El alfabeto que se debe emplear es {A,B,...,N,Ñ,O,...,Z,_} con asignación numérica {0,1,...,27}.
Descifra el criptograma obtenido para recuperar el mensaje original.

Solución:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
14	15	16	17	18	19	20	21	22	23	24	25	26	27

La asignación numérica de m = CRIPTOGRAFIA es la que sigue:

m = 02 18 08 16 20 15 06 18 00 05 08 00

La función de cifrado viene dada por la expresión siguiente:
$c_i = E_k(m_i) = m_i^{11} \bmod 221$

Cifraremos m agrupando en bloques de 1 caracteres ya que
$28^1 \leq n=221 < 28^2=784$

Si dividimos m en grupos de 1 caracteres obtenemos que:
m= C R I P T O G R A F I A

m_1 = C = $(02)_{(28)}$ = 2
m_2 = R = $(18)_{(28)}$ = 18
m_3 = I = $(08)_{(28)}$ = 8
m_4 = P = $(16)_{(28)}$ = 16
m_5 = T = $(20)_{(28)}$ = 20
m_6 = O = $(15)_{(28)}$ = 15
m_7 = G = $(06)_{(28)}$ = 6
m_8 = R = $(18)_{(28)}$ = 18
m_9 = A = $(00)_{(28)}$ = 0
m_{10} = F = $(05)_{(28)}$ = 5
m_{11} = I = $(08)_{(28)}$ = 8
m_{12} = A = $(00)_{(28)}$ = 0

El valor más grande de c_i que se puede obtener es 220, que se puede expresar en base 28 como: 220 = $(7)(24)_{(28)}$ = HX
Por tanto codificaremos con 2 caracteres del alfabeto del texto en claro.

El cifrado de cada uno de los bloques es:
$c_1 = E_k(2) \;=\; 2^{11}$ mod 221 = 59 = $(2)(3)_{(28)}$ = CD
$c_2 = E_k(18) = 18^{11}$ mod 221 = 86 = $(3)(2)_{(28)}$ = DC

Análogamente
c_3 = 70 = CÑ
c_4 = 152 = FM
c_5 = 41 = BN
c_6 = 111 = D_
c_7 = 141 = FB
c_8 = 86 = DC
c_9 = 0 = AA
c_{10} = 164 = FX
c_{11} = 70 = CÑ
c_{12} = 0 = AA

El criptograma obtenido es

$$c = E_k(m) = \text{CDDCCÑFMBND\_FBDCAAFXCÑAA}$$

DESCIFRADO

La asignación numérica de c = CDDCCÑFMBND FBDCAAFXCÑAA es la que sigue
c = 02 03 03 02 02 14 05 12 01 13 03 27 05 01 03 02 00 00 05 24 02 14 00 00

La función de descifrado viene dada por la expresión

$$m_i = D_k\,(c_i) = c_i^{\,d} \bmod n = c_i^{35} \bmod 221$$

Sabemos que el texto en claro, m, ha sido agrupado en bloques de 1 carácter ya que

$$28^1 \leq n=221 < 28^2=784.$$

El valor más grande de c_i que se puede obtener es 220, que se puede expresar en base 28 como: 220 = $(7)(24)_{(28)}$ = HX, por tanto, dividiremos c en bloques de 2 caracteres.

c=CD DC CÑ FM BN D FB DC AA FX CÑ AA
c_1 = CD = $(02)(03)_{(28)}$ = 59
c_2 = DC = $(03)(02)_{(28)}$ = 86
c_3 = CÑ = $(02)(14)_{(28)}$ = 70
c_4 = FM = $(05)(12)_{(28)}$ = 152
c_5 = BN = $(01)(13)_{(28)}$ = 41
c_6 = D = $(03)(27)_{(28)}$ = 111
c_7 = FB = $(05)(01)_{(28)}$ = 141
c_8 = DC = $(03)(02)_{(28)}$ = 86
c_9 = AA = $(00)(00)_{(28)}$ = 0
c_{10} = FX = $(05)(24)_{(28)}$ = 164
c_{11} = CÑ = $(02)(14)_{(28)}$ = 70
c_{12} = AA = $(00)(00)_{(28)}$ = 0

Aplicando la función de descifrado a cada grupo obtendremos el texto en claro
$m_1 = D_k(59) = 59^{35} \bmod 221 = 2 = (2)_{(28)} = C$
$m_2 = D_k(86) = 86^{35} \bmod 221 = 18 = (18)_{(28)} = R$
Análogamente
$m_3 = 8 = I$
$m_4 = 16 = P$
$m_5 = 20 = T$
$m_6 = 15 = O$
$m_7 = 6 = G$
$m_8 = 18 = R$
$m_9 = 0 = A$
$m_{10} = 5 = F$
$m_{11} = 8 = I$
$m_{12} = 0 = A$

El mensaje descifrado obtenido es m = CRIPTOGRAFIA.

5.8) Supongamos que en una red de comunicación se utiliza RSA con agrupación óptima de letras y alfabeto

_	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	?
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**	**26**	**27**	**28**

Un usuario, con clave pública (n=1501, e=37), recibe el mensaje
c = AL?_KKAFR_V__KL_CTANI_S?
¿A qué texto en claro corresponde?

Solución:

En primer lugar debemos obtener la función de descifrado, $m_i = D_k(c_i) = c_i^d \bmod n$, donde $d = e^{-1} \bmod \Phi(n)$.

El valor de n se puede descomponer como producto de los primos p = 79 y q = 19, por lo que $\Phi(n) = 78 \cdot 18 = 1404$.

Procedemos ahora a calcular $d = 37^{-1} \bmod 1404$

$1404 = 37 \cdot 37 + 35 \rightarrow 35 = 1404 - 37 \cdot 37 \bmod 1404 = -37 \cdot 37 \bmod 1404;$
$37 = 1 \cdot 35 + 2 \rightarrow 2 = 37 - 1 \cdot 35 \bmod 1404 = 37 - (-37) \cdot 37 \bmod 1404 = 38 \cdot 37 \bmod 1404;$
$35 = 17 \cdot 2 + 1 \rightarrow 1 = 35 - 17 \cdot 2 \bmod 1404 = -37 \cdot 37 - 17 \cdot 38 \cdot 37 \bmod 1404$
$= -683 \cdot 37 \bmod 1404 = 721 \cdot 37 \bmod 1404 \rightarrow 37^{-1} \bmod 1404 = 721.$

El valor de n está comprendido entre 841 y 24389, esto es: $29^2 \le n < 29^3$, por lo que el mensaje en claro ha sido cifrado agrupando los caracteres de dos en dos; además, como n-1 = 1500 = $(1)(22)(21)_{(29)}$ = AUT, el criptograma debe agruparse de tres en tres caracteres, para descifrar.

c = AL? _KK AFR _V_ _KL _CT ANI _S? = c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8

Los grupos están codificados en base 29 con el alfabeto, de ahí que

c_1 = AL? = $(1)(12)(28)_{(29)} = 1 \cdot 29^2 + 12 \cdot 29 + 28 = 1217$;
c_2 = _KK = $(0)(11)(11)_{(29)} = 0 \cdot 29^2 + 11 \cdot 29 + 11 = 330$;
c_3 = AFR = $(1)(6)(19)_{(29)} = 0 \cdot 29^2 + 6 \cdot 29 + 19 = 193$;
c_4 = _V_ = $(0)(23)(0)_{(29)} = 0 \cdot 29^2 + 23 \cdot 29 + 0 = 667$;
c_5 = _KL = $(0)(11)(12)_{(29)} = 0 \cdot 29^2 + 11 \cdot 29 + 12 = 331$;
c_6 = _CT = $(0)(3)(21)_{(29)} = 0 \cdot 29^2 + 3 \cdot 29 + 21 = 108$;
c_7 = ANI = $(1)(14)(9)_{(29)} = 1 \cdot 29^2 + 14 \cdot 29 + 9 = 1256$;
c_8 = _S? = $(0)(20)(28)_{(29)} = 0 \cdot 29^2 + 20 \cdot 29 + 28 = 608$.

Aplicando la función de descifrado, obtendremos el texto en claro, codificado.

$$
\begin{aligned}
m_1 = D_k(c_1) &= D_k(1217) = 1217^{721} \bmod 1501 = (1217^2)^{360} \cdot 1217 \bmod 1501\\
&= (1103)^{360} \cdot 1217 \bmod 1501 = (1103^2)^{180} \cdot 1217 \bmod 1501\\
&= (799)^{180} \cdot 1217 \bmod 1501 = (799^2)^{90} \cdot 1217 \bmod 1501\\
&= (476)^{90} \cdot 1217 \bmod 1501 = (476^3)^{30} \cdot 1217 \bmod 1501\\
&= (324)^{30} \cdot 1217 \bmod 1501 = (324^4)^{7} \cdot 324^2 \cdot 1217 \bmod 1501\\
&= (1331)^{7} \cdot 1179 \bmod 1501 = (1331^2)^{3} \cdot 1331 \cdot 1179 \bmod 1501\\
&= (381)^{3} \cdot 704 \bmod 1501 = 495 \cdot 704 \bmod 1501\\
&= 248 = 8 \cdot 29 + 16 = (8)(16)_{(29)} = \text{HO};
\end{aligned}
$$

El cálculo de 1217^{721} mod 1501 también se puede realizar del siguiente modo:

1217	mod	1501	=								=	**1217**	**1**
1217^2	mod	1501	=	1217^2	mod	1501	=	1481089	mod	1501	=	1103	**0**
1217^4	mod	1501	=	1103^2	mod	1501	=	1216609	mod	1501	=	799	**0**
1217^8	mod	1501	=	799^2	mod	1501	=	638401	mod	1501	=	476	**0**
1217^{16}	mod	1501	=	476^2	mod	1501	=	226576	mod	1501	=	**1426**	**1**
1217^{32}	mod	1501	=	1426^2	mod	1501	=	2033476	mod	1501	=	1122	**0**
1217^{64}	mod	1501	=	1122^2	mod	1501	=	1258884	mod	1501	=	**1046**	**1**
1217^{128}	mod	1501	=	1046^2	mod	1501	=	1094116	mod	1501	=	**1388**	**1**
1217^{256}	mod	1501	=	1388^2	mod	1501	=	1926544	mod	1501	=	761	**0**
1217^{512}	mod	1501	=	761^2	mod	1501	=	579121	mod	1501	=	**1236**	**1**

1217	.	**1426**	mod	1501	=	286
286	.	**1046**	mod	1501	=	457
457	.	**1388**	mod	1501	=	894

894 . **1236** mod 1501 = 248

$m_2 = D_k(c_2) = D_k(330) = 330^{721}$ mod 1501 = 349 = $(12)(1)_{(29)}$ = LA;
$m_3 = D_k(c_3) = D_k(193) = 193^{721}$ mod 1501 = 3 = $(0)(3)_{(29)}$ = _C;
$m_4 = D_k(c_4) = D_k(667) = 667^{721}$ mod 1501 = 477 = $(16)(13)_{(29)}$ = OM;
$m_5 = D_k(c_5) = D_k(331) = 331^{721}$ mod 1501 = 464 = $(16)(00)_{(29)}$ = O_;
$m_6 = D_k(c_6) = D_k(108) = 108^{721}$ mod 1501 = 165 = $(5)(20)_{(29)}$ = ES;
$m_7 = D_k(c_7) = D_k(1256) = 1256^{721}$ mod 1501 = 610 = $(21)(01)_{(29)}$ = TA;
$m_8 = D_k(c_8) = D_k(608) = 608^{721}$ mod 1501= 608 = $(20)(28)_{(29)}$ = S?.

El mensaje original es

m = HOLA COMO ESTAS?

5.9) Alicia, Benito y Carlos son tres amigos que utilizan para comunicarse RSA con alfabeto de cifrado

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
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

y clave pública de cada uno de ellos:
Alicia (n_A = 33, e_A = 7), Benito (n_B = 34, e_B = 5), Carlos (n_C = 35, e_C = 11).
Alicia recibe el mensaje cifrado c = 22 30 29 20 08 con firma digital s=18.
El remitente del mensaje ha firmado digitalmente la suma de los elementos del texto en claro módulo n_A.

a) **¿Qué mensaje en claro ha recibido Alicia?**

b) **¿Puede saber cual de los dos amigos se lo ha enviado y estar segura de que no ha sido el otro?**

Solución:

a) En primer lugar, vamos a obtener la clave de descifrado de Alicia.

Como $n_A = 33 = 3 \cdot 11$, se tiene que $\Phi(n_A) = 2 \cdot 10 = 20$.

Por definición, $d_A = e_A^{-1} \bmod 20 = 7^{-1} \bmod 20 = 3$.

La función de descifrado para Alicia viene dada por $D_{K_A}(c) = c^3 \bmod 33$

$D_{K_A}(22) = 22^3 \bmod 33 = 22 \rightarrow$ T
$D_{K_A}(30) = 30^3 \bmod 33 = 06 \rightarrow$ E
$D_{K_A}(29) = 29^3 \bmod 33 = 02 \rightarrow$ A
$D_{K_A}(20) = 20^3 \bmod 33 = 14 \rightarrow$ M
$D_{K_A}(08) = 08^3 \bmod 33 = 17 \rightarrow$ O

Luego el mensaje en claro es m = TEAMO

Llamemos t = (22+06+02+14+17) mod n_A = 61 mod 33 = 28

b) Para saber cuál de los dos amigos le ha enviado el mensaje, Alicia comprueba la firma digital de t, para ello, obtiene en primer lugar la rúbrica

$$D_{K_A}(s) = 18^3 \bmod 33 = 24 = r$$

y a continuación cifrará la rúbrica con la clave pública de Benito, $E_{K_B}(r)$, y la de Carlos, $E_{K_B}(r)$, para comparar el resultado con el mensaje original, t

$$E_{K_B}(r) = 24^{05} \bmod 34 = 28 = t$$
$$E_{K_C}(r) = 24^{11} \bmod 35 = 19 \neq t$$

luego el mensaje es de Benito.

5.10) En una red, Alicia desea enviar a Belén un mensaje m y firmarlo digitalmente. Para ello se utiliza un algoritmo de clave pública en el que las funciones de cifrado y descifrado de Alicia son E_{k_A} y D_{k_A} y las de Belén son E_{k_B} y D_{k_B}. El proceso seguido consiste en que Alicia cifra el mensaje $c = E_{k_B}(m)$, obtiene la firma digital $s = E_{k_B}\left[D_{k_A}(m)\right]$ y envía los valores de c y s a Belén. ¿Qué proceso tiene que realizar Belén para descifrar c y comprobar que el mensaje es auténtico?

Solución:

Para descifrar el criptograma, Belén realiza la operación $D_{k_B}(c) = D_{k_B}\left[E_{k_B}(m)\right] = m$.

Para verificar su autenticidad, Belén comprueba que $E_{k_A}\left[D_{k_B}(s)\right] = m$, esto es,

$$E_{k_A}\left[D_{k_B}(s)\right] = E_{k_A}\left[D_{k_B}\left[E_{k_B}\left[D_{k_A}(m)\right]\right]\right] = E_{k_A}\left[D_{k_A}(m)\right] = m.$$

5.11) Explica, brevemente, por qué no se utiliza la criptografía de clave pública para el cifrado general de la información. ¿Qué alternativa se utiliza?

Solución:

Comúnmente, el cifrado con clave pública involucra cálculos con un coste computacional alto es por ello que para el cifrado general de la información se utiliza el cifrado con clave secreta o simétrico.

5.12) Explica, brevemente, por qué crees que en todos certificados con algoritmo RSA la clave pública e = 65537.

Solución:

La función de cifrado de RSA es $E_k(m) = m^e \bmod n$ por lo que en el proceso de cifrado se tiene que calcular $m^e \bmod n$. Para ello, se descompone e como suma de potencias de 2 y se aplican las propiedades de las potencias. El número 65537 = $010001_{(16)}$ = $1\ 0000\ 0000\ 0000\ 0001_{(2)}$ hace que en el producto final solo haya que multiplicar dos potencias de 2 que son 2^{65536} y 2^1.

5.13) Si se desea utilizar un algoritmo para cifrar una videoconferencia (audio y video); explica, brevemente, qué tipo de algoritmo de entre los siguientes resultaría inadecuado: cifrado en flujo, cifrado en bloque simétrico, cifrado asimétrico.

Solución:

El cifrado asimétrico ya que es mucho más lento que los otros dado que involucra operaciones con un mayor coste computacional.

5.14) Explica, brevemente, cuál es la principal ventaja de los criptosistemas de clave pública frente a los de clave secreta y el principal inconveniente.

Solución:

La principal ventaja de los criptosistemas de clave pública frente a los de clave secreta es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y no es necesario po-ner en peligro la clave privada enviándola por medios potencialmente inseguros, ya que ésta debe permanecer siempre oculta y en poder, únicamente, de su propietario.

El inconveniente que presentan estos criptosistemas frente a los de clave secreta es que son mucho más lentos, por lo que, generalmente, se usan para el envío seguro de la clave de cifrado del criptosistema de clave secreta utilizado para el cifrado de la información.
En muchas ocasiones, se implementan sistemas criptográficos mixtos, en los que se usa la clave pública del receptor para cifrar una clave simétrica que se usará en el proceso de comunicación cifrada. De esta forma se aprovechan las ventajas de ambos sistemas, usando el sistema asimétrico para el envío de la clave sensible y el simétrico, con mayor velocidad de proceso, para el envío masivo de datos.

5.15) Explica, brevemente, qué papel desempeñan las funciones hash en la firma digital.

Solución:

Los cifradores de clave pública, por lo general, son bastante costosos computacionalmente, por lo que los protocolos de firma digital, también suelen ser costosos computacionalmente y, en ocasiones, la longitud de la firma suele ser similar o mayor que el propio mensaje que se firma. Es por ello que, en lugar de firmar digitalmente el mensaje completo, se firma digitalmente un resumen o hash de dicho mensaje, representado por sólo una centena de bits.

5.16) Explica, brevemente, en qué consisten las características siguientes que debe cumplir una función hash para que se considere segura: unidireccionalidad, colisión fuerte.

Solución:

Por unidireccionalidad se entiende que, conocido un resumen h(m), debe ser computacionalmente imposible encontrar m a partir de dicho resumen.

Por colisión fuerte se entiende que será computacionalmente difícil encontrar un par de mensajes (m, m') de forma que h(m) = h(m').

Tema 6
Infraestructuras de clave pública

6.1) Una autoridad certificadora (AC) tiene clave pública RSA e_{AC}= 19, siendo n_{AC}= 23·31 = 713. Un usuario, A, tiene clave pública RSA e_A= 3, siendo n_A= 11·23 = 253.
¿Qué protocolo aplica AC para certificar la clave pública del usuario A? Efectúa los cálculos pertinentes para obtener el certificado de A, c_A.

Solución:

Para certificar la clave pública de A, la Autoridad Certificadora aplica el protocolo $c_A=D_{K_{AC}}(e_A)$.

Para obtener el certificado c_A debemos calcular, por tanto,

$$c_A=D_{K_{AC}}(e_A)=D_{K_{AC}}(3)=3^{d_{AC}} \bmod n_{AC}=3^{d_{AC}} \bmod 713.$$

El valor de n_{AC}=23·31=713 por lo que $\Phi(n_{AC})$=22·30=660

Necesitamos conocer la clave privada de AC,

$$d_{AC}=e_{AC}^{-1} \bmod \Phi(n_{AC})=19^{-1} \bmod 660=139$$

660 = 34 · 19 + 14 →	14 = 660 + (-34) 19 mod 660 =		(-34) 19 mod 660 = 626 · 19 mod 660
19 = 1 · 14 + 5 →	5 = 19 + (-1) 14 mod 660 =	1 · 1 · 19 + (-1) 626 · 19 mod 660 =	(-625) 19 mod 660 = 35 · 19 mod 660
14 = 2 · 5 + 4 →	4 = 14 + (-2) 5 mod 660 =	1 · 626 · 19 + (-2) 35 · 19 mod 660 =	(556) 19 mod 660 = 556 · 19 mod 660
5 = 1 · 4 + 1 →	1 = 5 + (-1) 4 mod 660 =	1 · 35 · 19 + (-1) 556 · 19 mod 660 =	(-521) 19 mod 660 = 139 · 19 mod 660

En consecuencia, $c_A=D_{K_{AC}}(e_A)=D_{K_{AC}}(3)=3^{139} \bmod 713=$**508**.

3 mod 713 = = **3 1**
3^2 mod 713 = 3^2 mod 713 = 9 mod 713 = **9 1**

3^4 mod 713 = 9^2 mod 713 = 81 mod 713 = 81 **0**
3^8 mod 713 = 81^2 mod 713 = 6561 mod 713 = **144 1**
3^{16} mod 713 = 144^2 mod 713 = 20736 mod 713 = 59 **0**
3^{32} mod 713 = 59^2 mod 713 = 3481 mod 713 = 629 **0**
3^{64} mod 713 = 629^2 mod 713 = 395641 mod 713 = 639 **0**
3^{128} mod 713 = 639^2 mod 713 = 408321 mod 713 = **485 1**

3 . **9** mod 713 = 27
27 . **144** mod 713 = 323
323 . **485** mod 713 = **508**

6.2) Consideremos la autoridad certificadora, AC, del ejercicio anterior (RSA, e_{AC}= 19, n_{AC}=23·31=713), el usuario A (RSA, e_A=3, n_A=11·23=253) de ese ejercicio y un usuario B con clave pública RSA, e_B= 5, n_B= 13·19 = 247 y un certificado expedido por AC, c_B=408.

a) El usuario A envía a B su clave pública e_A, n_A y su certificado c_A. ¿Qué protocolo aplica B para comprobar que la clave es auténtica? Realiza los cálculos.

b) El usuario B cifra el mensaje m=12 para A y le envía el criptograma c obtenido y A lo descifra para obtener m. Calcula c y realiza el descifrado que hace A de c para obtener m.

c) El usuario B firma digitalmente el mensaje m y le envía la firma digital, s, al usuario A. Calcula s.

d) El usuario A verifica que la clave pública de B es de ese usuario y aplica el protocolo de firma digital para comprobar que el mensaje recibido del usuario B es auténtico. Haz los cálculos para ambas verificaciones.

Solución:

a) El usuario B debe aplicar $E_{AC}(c_A)$ y comprobar que el resultado coincide con la clave pública de A, e_A.
Se tiene

$$E_{AC}(c_A) = E_{AC}(508) = 508^{19} \text{ mod } 713 = 3 = e_A.$$

508 mod 713 = = **508 1**
508^2 mod 713 = 508^2 mod 713 = 258064 mod 713 = **671 1**
508^4 mod 713 = 671^2 mod 713 = 450241 mod 713 = 338 **0**
508^8 mod 713 = 338^2 mod 713 = 114244 mod 713 = 164 **0**
508^{16} mod 713 = 164^2 mod 713 = 26896 mod 713 = **515 1**

508 . **671** mod 713 = 54
54 . **515** mod 713 = 3

b) El usuario B hace el siguiente cálculo para obtener c

$$c = E_{K_A}(m) = E_{K_A}(12) = 12^3 \bmod 253 = 1728 \bmod 253 = 210.$$

El usuario A hace el siguiente cálculo para obtener m

$$m = D_{K_A}(c) = D_{K_A}(210) = 210^{dA} \bmod 253 = 210^{147} \bmod 253 = 12.$$

$210 \bmod 253 = \quad = \mathbf{210}\ \mathbf{1}$
$210^2 \bmod 253 = 210^2 \bmod 253 = 44100 \bmod 253 = \mathbf{78}\ \mathbf{1}$
$210^4 \bmod 253 = 78^2 \bmod 253 = 6084 \bmod 253 = 12\ \mathbf{0}$
$210^8 \bmod 253 = 12^2 \bmod 253 = 144 \bmod 253 = 144\ \mathbf{0}$
$210^{16} \bmod 253 = 144^2 \bmod 253 = 20736 \bmod 253 = \mathbf{243}\ \mathbf{1}$
$210^{32} \bmod 253 = 243^2 \bmod 253 = 59049 \bmod 253 = 100\ \mathbf{0}$
$210^{64} \bmod 253 = 100^2 \bmod 253 = 10000 \bmod 253 = 133\ \mathbf{0}$
$210^{128} \bmod 253 = 133^2 \bmod 253 = 17689 \bmod 253 = \mathbf{232}\ \mathbf{1}$

210. **78** mod 253 = 188
188.**243** mod 253 = 144
144.**232** mod 253 = 12

Siendo $d_A = e_A^{-1} \bmod \Phi(n_A) = 3^{-1} \bmod 220 = 147$

220 = 73· 3+**1**→ **1**=220+(-73) 3 mod 220=(-73) 3 mod 220 = **147** 3 mod 220

c) Necesitamos conocer la clave privada del usuario B, d_B,

$$d_B = e_B^{-1} \bmod \Phi(n_B) = 5^{-1} \bmod 216 = 173$$

216=43·5+**1**→ **1**=216+(-43) 5 mod 216 = (-43) 5 mod 216 = **173** 5 mod 216

El usuario B cálcula en primer lugar la rúbrica,

$$r = D_{K_B}(m) = D_{K_B}(12) = 12^{173} \bmod 247 = 103$$

$12 \bmod 247 = \quad = \mathbf{12}\ \mathbf{1}$
$12^2 \bmod 247 = 12^2 \bmod 247 = 144 \bmod 247 = 144\ \mathbf{0}$
$12^4 \bmod 247 = 144^2 \bmod 247 = 20736 \bmod 247 = \mathbf{235}\ \mathbf{1}$
$12^8 \bmod 247 = 235^2 \bmod 247 = 55225 \bmod 247 = \mathbf{144}\ \mathbf{1}$
$12^{16} \bmod 247 = 144^2 \bmod 247 = 20736 \bmod 247 = 235\ \mathbf{0}$
$12^{32} \bmod 247 = 235^2 \bmod 247 = 55225 \bmod 247 = \mathbf{144}\ \mathbf{1}$
$12^{64} \bmod 247 = 144^2 \bmod 247 = 20736 \bmod 247 = 235\ \mathbf{0}$
$12^{128} \bmod 247 = 235^2 \bmod 247 = 55225 \bmod 247 = \mathbf{144}\ \mathbf{1}$

12 . **235** mod 247 = 103
103 . **144** mod 247 = 12

12 . **144** mod 247 = 246
246 . **144** mod 247 = 103

Y a continuación la firma digital

$$s = E_{K_A}(r) = E_{K_A}(103) = 103^3 \bmod 253 = 20$$

103 mod 253 = = **103** **1**
103^2 mod 253 = 103^2 mod 253 = 10609 mod 253 = **236** **1**

103.**236** mod 253 = 20

d) El usuario A, en primer lugar, comprueba que la clave pública de B es de ese usuario. Para ello tiene que verificar que $E_{K_{AC}}(c_B) = e_B$

$$E_{K_{AC}}(c_B)=E_{K_{AC}}(408)= 408^{19} \bmod 713 = 5 = e_B$$

408 mod 713 = = **408** **1**
408^2 mod 713 = 408^2 mod 713 = 166464 mod 713 = **335** **1**
408^4 mod 713 = 335^2 mod 713 = 112225 mod 713 = 284 **0**
408^8 mod 713 = 284^2 mod 713 = 80656 mod 713 = 87 **0**
408^{16} mod 713 = 87^2 mod 713 = 7569 mod 713 = **439** **1**

408 . **335** mod 713 = 497
497 . **439** mod 713 = 5

Por tanto, la clave pública del usuario B es auténtica.

Para comprobar que el mensaje proviene del usuario B, tiene que aplicar el protocolo de firma digital a s y comprobar que $E_{K_B}[D_{K_A}(s)] = m$

$$D_{K_A}(s) = D_{K_A}(20) = 20^{147} \bmod 253 = 103 = r$$

20 mod 253 = = **20** **1**
20^2 mod 253 = 20^2 mod 253 = 400 mod 253 = **147** **1**
20^4 mod 253 = 147^2 mod 253 = 21609 mod 253 = 104 **0**
20^8 mod 253 = 104^2 mod 253 = 10816 mod 253 = 190 **0**
20^{16} mod 253 = 190^2 mod 253 = 36100 mod 253 = **174** **1**
20^{32} mod 253 = 174^2 mod 253 = 30276 mod 253 = 169 **0**
20^{64} mod 253 = 169^2 mod 253 = 28561 mod 253 = 225 **0**
20^{128} mod 253 = 225^2 mod 253 = 50625 mod 253 = **25** **1**

20.**147** mod 253 = 157
157.**174** mod 253 = 247

247.**25** mod 253 = 103

$$E_{K_B}(r) = E_{K_B}(103) = 103^5 \bmod 247 = 12 = m$$

103 mod 247 = = **103 1**
103^2 mod 247 = 103^2 mod 247 = 10609 mod 247 = 235 **0**
103^4 mod 247 = 235^2 mod 247 = 55225 mod 247 = **144 1**

103.**144** mod 247 = 12

En consecuencia, el mensaje es auténtico del usuario B.

6.3) Explica, brevemente, qué es un certificado digital.

Solución:

Un certificado digital es un documento electrónico que contiene datos identificativos de una persona o entidad (empresa, servidor web, etc.) y la clave pública de la misma, haciéndose responsable de la autenticidad de los datos que figuran en el certificado otra persona o entidad de confianza, denominada Autoridad Certificadora (AC).

El certificado digital vincula, pues, indisolublemente a una persona o entidad con una clave pública, y mediante el protocolo de firma digital se asegura que el certificado que recibimos es realmente de la persona o entidad que consta en el mismo.

Si el certificado es auténtico y confiamos en la AC, entonces, podemos confiar en que el sujeto identificado en el certificado digital posee la clave pública que se señala en dicho certificado.