uc3m | Universidad Carlos III de Madrid

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

"Esquemas de firma digital"

Ejercicios propuestos

Ejercicio 1 :

Sea un sistema RSA con p= 13 y q=19, donde se desea firmar digitalmente el mensaje M=10. Supóngase e= 11. Halle la firma digital de mensaje M y compruebe el resultado obtenido.

Solución:

Lo primero a hacer es comprobar que las condiciones se cumplen:

$$N=p\cdot q=13\cdot 19=247$$
$$\phi(N)=12\cdot 18=216$$
$$1<e<N \rightarrow 1<11<247 \text{ Cierto}$$
$$\text{Mcd } (e\ ,\ \phi(N)\ )=1 \rightarrow \text{Mcd } (11,\ 216)=1 \text{ Cierto}$$

p y q números primos grandes Falso, pero nos vale para el ejercicio

Una vez comprobadas las condiciones, podemos operar. Primero necesitamos calcular la clave privada para poder firmar:

$d\cdot e=1 \text{ mód } (\phi(N\ ))$

$11\cdot d=1 \text{ mód } (216)$

$216=19\cdot 11+7$	$7=216-19\cdot 11$
$11=1\cdot 7+4$	$4=11-1\cdot 7$
$7=1\cdot 4+3$	$3=7-1\cdot 4$
$4=1\cdot 3+1$	$1=4-1\cdot 3$

$1=4-1\cdot 3 \text{ mód } (216) = 4-(7-1\cdot 4) \text{ mód } (216) = 2\cdot 4-7\text{mód } (216) =$

$= 2\cdot(11-1\cdot 7)-7 \text{ mód } (216) = 2\cdot 11-3\cdot 7 \text{ mód } (216) = 2\cdot 11-3\cdot(216-19\cdot 11) \text{ mód } (216) =$

$= 59\cdot 11-3\cdot 216 \text{ mód } (216) = 59\cdot 11 \text{ mód } (216)$

Por lo tanto, d = 59

$\text{Firma}(M\ )=M^d \text{ mód } (N\ )=10^{59}\text{mód } (247)=(10^3)^{19}\cdot 10^2\text{mód } (247)=12^{19}\cdot 10^2\text{mód } (247)=$

$=4^{19}\cdot 3^{19}\cdot 10^2\text{mód } (247)=4^3\cdot(3^2)^4\cdot 3^{19}\cdot 10^2\text{mód } (247)=4^3\cdot 3^{27}\cdot 10^2\text{mód } (247)=$

$=4^3\cdot 3^2\cdot(-4)^5\cdot 10^2\text{mód } (247)=(-1)\cdot 4^8\cdot 3^2\cdot 10^2\text{mód } (247)=(-1)\cdot(9)^2\cdot 3^2\cdot 10^2\text{mód } (247)=$

$=(-1)\cdot 3^6\cdot 10^2\text{mód } (247)=(-1)\cdot 3\cdot(-4)\cdot 100\text{mód } (247)=4\cdot 53\text{mód } (247)=212\text{mód } (247)$

Comprobamos el resultado obtenido:

$F^e \text{ mód } (N\ )=212^{11}\text{mód } (247)$

$212\cdot 212=44944;\ 44944 \text{ mód } 247=237\text{mód } 247=(-10)\text{mód } 247$

$212^{11}\text{mód } (247)=(-10)^5\cdot 212\text{mód } (247)=(-1)\cdot 100\cdot 1000\cdot 212 \text{ mód } (247)=$

$=(-1)\cdot 100\cdot 12\cdot 212 \text{mód } (247)=(-1)\cdot 10\cdot 10\cdot 12\cdot 2\cdot 106 \text{mód } (247)=$
$=(-1)\cdot 10\cdot 240\cdot 106 \text{mód } (247)=(-1)\cdot 10\cdot(-7)\cdot 106 \text{ mód } (247)=10\cdot 7\cdot 53\cdot 2 \text{mód } (247)=$
$=10\cdot 2\cdot 371 \text{mód } (247)=10\cdot 2\cdot 124 \text{ mód } (247)=10\cdot 248 \text{mód } (247)=10$

Ejercicio 2:

2. Dos espías A y B se intercambian mensajes a través de correo electrónico. Desean mantener en secreto estos mensajes y estar seguros de su procedencia ya que A sospecha que un tal C quiere suplantar a B. Para ello firman digitalmente sus mensajes y los envían codificados con 27 elementos de forma que A=00, B=01,..., Z=26. Hacen uso del algoritmo RSA tanto para firmar como para cifrar sus comunicaciones.

Datos:

A: $N_A= 3 \cdot 13 =39$ $e_A=5$
B: $N_B=5 \cdot 11 = 55$ $e_B=9$

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

A y B tienen un plan acordado y sólo necesitan saber si la ciudad donde deben reunirse es PARIS o LISBOA. Para ello cifran las dos primeras letras de la ciudad y firman sólo la primera. Imagine que la ciudad en cuestión para A es París y para B Lisboa. Se pide:

a) Calcular los dos mensajes cifrados: C_A y C_B.

b) Firmar cada uno de los mensajes. $F_A(M_A)$ y $F_B(M_B)$.

c) Descifrar los criptogramas y comprobar la firma en cada caso.

d) A y B se dan cuenta de que no se han puesto de acuerdo. Indique un protocolo seguro en el que sólo se intercambie el mensaje PARIS.

Solución:

a) El mensaje de A a B es:
$M_A=[PA]=(16,0)$
$C_A = M_{A1}^{eB} \text{ (mód } N_B), M_{A2}^{\ eB} \text{ (mód } N_B) = 16^9, 0^9 \text{ mód } 55 =$
$= 2^{36},0 \text{ (mód } 55) = 9^6,0 \text{ (mód } 55) = 3^{12},0 \text{ (mód } 55) = (3^4)^3 \text{ (mód } 55)= 26^3, 0 \text{ (mód } 55) =$
$16\cdot 26, 0 \text{ (mód } 55) =$ [**31, 0**](mód 55)

El mensaje de B a A es:
$M_B=[LI]=(11,8)$
$C_B = M_{B1}^{eA}\text{(mód } N_A), M_{B2}^{eA}\text{(mód } N_A) = 11^5,8^5 \text{ (mód } 39) = (11^2)^2\cdot 11, (2^5)^3 \text{ (mód.}39) = 4^2\cdot 11, (-7)^3 \text{ (mód. } 39) = 4\cdot 5, 10\cdot(-7) \text{ (mód. } 39) =$ [**20, 8**](mód 39)

b) Para firmar los mensajes debemos calcular las claves privadas, y para ello necesitamos calcular el indicador ϕ (N):
$\phi (N_A)=2\cdot 12=24$
$\phi (N_B)=4\cdot 10=40$

$e_A \cdot d_A = 1(\text{mód } \phi\ (N_A))$; $d_A \cdot 5 = 1(\text{mód } 24) \rightarrow d_A = 5$
$e_B \cdot d_B = 1(\text{mód } \phi\ (N_B))$; $d_B \cdot 9 = 1(\text{mód } 40) \rightarrow d_B = 9$
$F_A(M_A) = P^{dA}(\text{mód } N_A) = 16^5(\text{mód } 39) = 7^4\ (\text{mód } 39) = 22(\text{mód } 39)$
$F_B(M_B) = L^{dB}\ (\text{mód } N_B) = 11^9(\text{mód } 55) = 11(\text{mód } 55)$

Nota informativa:
A envía el mensaje $(C_{1A}, C_{2A}, F_A) = (31,0,22)$
B envía el mensaje $(C_{1B}, C_{2B}, F_B) = (20,8,11)$

c) Descifrado del mensaje de A por parte de B:
$M_A = C_{1A}^{dB}(\text{mód } N_B)\ , C_{2A}^{dB}\ (\text{mód } N_B) = 31^9,\ 0^9 \text{ mód } (55) = 16\ ,0(\text{mód } 55) = PA$

Comprobación de la firma de A:
$F_A^{eA}\text{mód } (N_A) = 22^5\ (\text{mód } 39) = 16^2 \cdot 22(\text{mód } 39) = 22 \cdot 22(\text{mód } 39) = 16(\text{mód } 39) = P$

Descifrado del mensaje de B por parte de A:
$M_B = C_{1B}^{dA}(\text{mód } N_A)\ , C_{2B}^{dA}(\text{mód } N_A) = 20^5, 8^5\ (\text{mód } 39) = 11,8\ (\text{mód } 39) = LI$

Comprobación de la firma de B:
$F_B^{eB}\text{ mód } (N_B) = 11^9(\text{mód } 55) = 11(\text{mód } 55) = L$

d) Un ejemplo es el siguiente: A envía PARIS cifrado y firmado a B. B verifica la firma y lo descifra devolviéndole a A el mensaje PARIS cifrado y firmado por él. A verifica la firma de B y descifra el mensaje. A envía a B un acuse de recibo.

Ejercicio 3:
Calcular y verificar la firma, mediante El Gamal, del mensaje M=5, con g=2, p=11, $X_A=8$, y k=9.

Solución:

g es raíz primitiva en Z p
$1 < X_A < p-1 \rightarrow 1 < 8 < 10 \rightarrow$ Se cumple
$1 < k < p-1 \rightarrow 1 < 9 < 10 \rightarrow$ Se cumple
$\text{mcd}(9,10) = 1 \rightarrow$ Se cumple
$r = g^k\ (\text{mód } p) = 2^9\ (\text{mód } 11) = 512(\text{mód } 11) = 6(\text{mód } 11)$

$M = X_A \cdot r + k \cdot s\ (\text{mód } p-1) \rightarrow 5 = 8 \cdot 6 + 9 \cdot s \text{ mód } (10) \rightarrow 5 = 8 + 9 \cdot s \text{ mód } (10) \rightarrow 5 = 8 - s \rightarrow$ **$s=3$**

:::::::::::::::::::::::::::ALTERNATIVA ACADÉMICA::::::::::: :::::::::::::::
$M = X_A \cdot r + k \cdot s(\text{mód } p-1) \rightarrow 5 = 8 \cdot 6 + 9 \cdot s \text{ mód } (10) \rightarrow 5 = 8 + 9 \cdot s \rightarrow -3 = 9 \cdot s(\text{mód } 10)$

$7 = 9 \cdot s(\text{mód } 10)$

Hacemos el cambio de variable $z = s / 7\ (\text{mód } 10)$
$7 = 9 \cdot z \cdot 7(\text{mód } 10)$;$1 = 9 \cdot z\ (\text{mód } 10) = (-1) \cdot z\ (\text{mód } 10) \rightarrow$ **$z=-1=9$** mód (10)
$s = 7 \cdot z\ (\text{mód } 10) = 7 \cdot 9(\text{mód } 10) =$ **3**(mód 10)

:::::::::::::::::::::::::: ::::::::::::: :::::::::::::: ::::::::::::: :::::::::::::: ::::::::::::::

El emisor envía entonces (M,r,s): (5,6,3)

Verificamos la firma:
$V_1=Y_A^r \cdot r^s$ (mód p) ;
$Y_A=g^{XA}$(mód p)=2^8 (mód 11)=256(mód 11)=3mód (11)
$V_1=Y_A^r \cdot r^s$ (mód p)=$3^6 \cdot 6^3$ (mód 11)=$3^9 \cdot 2^3$(mód 11)=$(-1) \cdot 3^{10}$ (mód 11)=$(-1) \cdot (-2)^5$(mód 11)=
=32(mód 11)=10

$V_2=g^M$ (mód p)=2^5 (mód 11)=10

Como V_1 y V_2 coinciden, la firma es válida.

Ejercicio 4:
Un usuario A desea enviar a otro B un mensaje M, constituido por una ristra de dígitos hexadecimales, firmado (con firma separada del mensaje). Desea usar para ello el método de El Gamal utilizando como función resumen la función o-exclusivo (⊕), donde ⊕ aplicado sobre x e y se define como x ⊕ y = (x+y) mód 16, con x e y dígitos hexadecimales.

Suponga el siguiente mensaje (de longitud 16):

0 1 2 3 4 5 6 7 8 9 A B C D E F

a) Aplique la función o-exclusivo anterior, de modo que se obtenga como resumen, R, un solo dígito hexadecimal.

b) Supuesto que A elige, p=17, g=7, X_A=5, Y_A=11, k=9. ¿cumplen estos valores la condiciones para ser usados como constantes en el método El Gamal?

c) Obtenga la firma del mensaje M.

d) Realice los cálculos que permiten a B comprobar la integridad del mensaje recibido. ¿Es la firma correcta?

Solución:

a) Tenemos que calcular 0⊕1⊕ 2⊕3⊕ 4⊕ 5⊕ 6⊕ 7⊕ 8⊕ 9⊕ A⊕ B⊕ C⊕ D⊕ E⊕ F.
Como es una progresión aritmética, 0+1+2+3+4+5+6+7+8+9+A+B+C+D+E+F=120
0⊕1⊕ 2⊕3⊕ 4⊕5⊕6⊕7⊕8⊕9⊕ A⊕ B⊕C⊕ D⊕ E⊕ F=120(mód 16)=8

b) • p es primo (aunque no grande)
• g es generador mód p:
7^0mód 17=1 ;7^1mód 17=7 ;7^2mód 17=15 ;7^3mód 17=3 ;7^4=4 ;7^5=11 ;7^6=9 ;7^7mód 17=12 ;
7^8mód 17=16 ;7^9mód 17=10 ;7^{10}=2 ;7^{11}=14 ;7^{12}=13 ;7^{13}=6 ;7^{14}=8 ;7^{15}=5
• X_A cumple que 1 < 11 < 16
• k cumple que 1 < 9 < 16 y que mcd(9,16) = 1

c) $r=g^k$ (mód p)$=7^9$(mód 17)=10
$H(M)=X_A\cdot r+k\cdot s$ mód (p−1) → 8=5·10+9·s (mód 16); 8=2+9·s (mód 16); 6=9·s(mód 16)

Hacemos un cambio de variable: z= s/6 (mód 16) → 1=9·z (mód 16) → z=9

Deshaciendo el cambio de variable: s = 9·6 (mód 16) = 6 (mód 16)

Por lo tanto, el emisor enviará (M,r,s) = (**0 1 2 3 4 5 6 7 8 9 A B C D E F**,10,6)

d) $Y_A=g^{XA}$(mód p)$=7^5$ (mód 17)=15·15·7(mód 17)=8·12(mód 17)=−6(mód 17)=11
$V_1=Y_A^r\cdot r^s$ (mód p)$=11^{10}\cdot 10^6$ (mód 17)$=2^5\cdot(-2)3$ (mód 17)$=(-1)\cdot 2^8$(mód 17)=16 (mód 17)
$V_2=g^{H(M)}$ (mód 17)$=7^8$(mód p)= 16

Por lo tanto la firma es correcta.