Universidad
Carlos III de Madrid

COSEC Lab · *Dpto. Informática*

Universidad Carlos III de Madrid

Firma Electrónica. PKI Enunciados

Criptografía y Seguridad de la Información
Seguridad en las Tecnologías de la Información

Pablo Martín

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.

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 ·13 =39 e_A=5
B: N_B=5 ·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.

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

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 las 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?

5.- Alicia desea enviar a Benito un mensaje M firmado mediante RSA. Las claves públicas de Alicia y Benito están certificadas por las Autoridades de Certificación AC_A y AC_B respectivamente. Existe una tercera Autoridad, AC, que certifica a AC_A y AC_B. Suponga que los certificados de las tres Autoridades de Certificación constan exclusivamente de la firma RSA del exponente de la clave pública de los clientes, es decir, F(e).

Datos:

- **Todas las Autoridades de Certificación trabajan con el mismo módulo N=55.**
- **La clave pública de AC es (e_{AC}, N) = (7, 55).**
- **Los exponentes públicos de las claves públicas de AC_A $(e_{AC_A}, N) = (e_{AC_A}, 55)$ y A (e_A, N) = (e_A, 55) no se proporcionan.**
- **El certificado de AC_A emitido por AC es 8.**
- **El certificado de A emitido por AC_A es 7.**

Se pide:

a) **Calcule la clave pública de AC_A. Analice si es un exponente público válido.**

b) **Calcule la clave pública de A. ¿Sería posible en vista del resultado del apartado anterior?**

c) **Independientemente del resultado del apartado anterior, suponga que la clave pública de A es (e_A, N) = (49, 55). Calcule la firma RSA por parte de A del mensaje M = 4.**

2.) Firman y Cifran A=00, B=01,... RSA para firmar y cifrar.

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

Cifran XX/XX las 2 primera Firman X/X 1ºletra

A= París B=Lisboa

a.) ¿C_a y C_b?

Para A: $C_a = M_a^{e_B} \bmod N_B = 16^9 \; 00^9 \bmod 55 = 31 \; 0 = C_a$

$(16^3)^3$ 0

PA= 16 00

Para B: $C_B = M_b^{e_A} \bmod N_A = 11^5 \; 8^5 \bmod 39 = 20 \; 8 = C_b$

20

L1 = 11 8

b.) ¿$F_A(M_A)$ y $F_B(M_B)$?

Para A: $F_A(M_A) = M_A^{d_a} \bmod N_A = 16^5 \bmod 39 = 22$

P= 16

Para B: $F_B(M_B) = M_B^{d_b} \bmod N_B = 11^9 \bmod 55 = 11$

L = 11

$d_a = e_A^{-1} \bmod \underset{4 \cdot 2 \cdot 11}{\varphi(p_a \cdot q_a)} = 5^{-1} \bmod 24 = 5$

$24 = 5 \cdot 4 + 4 \qquad 1 = 5 - 24 + 5 \cdot 4 = -1 \cdot 24 + \underbrace{5}_{d_a} \cdot 5$

$5 = 4 \cdot 1 + 1 \qquad 1 = 5 - 4$

$d_B = e_B^{-1} \bmod \underset{4 \cdot 4 \cdot 10}{\varphi(p_b \cdot q_b)} = 9^{-1} \bmod 40 = 9$

$40 = 9 \cdot 4 + 4 \qquad 1 = 9 - 2(40 - 9 \cdot 4) = -2 \cdot 40 + \underbrace{9}_{d_b} \cdot 9$

$9 = 4 \cdot 2 + 1 \qquad 1 = 9 - 2 \cdot 4$

c.) Descifrar y comprobar

Para A: Recibe 20^{C_B} 8 y 11^{F_B}

Descifrar ⇒ $M = C_B^{d_a} \bmod N_A = 20^5\ 8^5 \bmod 39 = \underset{L}{11}\ \underset{I}{8}$ } Coincide la letra 11 = L Comprobado

Verificar firma ⇒ $V = F_B^{e_b} \bmod N_B = 11^9 \bmod 55 = \underset{L}{11}$ }

Para B: Recibe 31^{C_a} 0 y 22^{F_A}

Descifrar ⇒ $M = C_a^{d_b} \bmod N_B = 31^9\ 0^9 \bmod 55 = \underset{P}{16}\ \underset{A}{0}$ } Coincide la letra 16 = P Comprobado

Verificar firma ⇒ $V = F_a^{e_a} \bmod N_A = 22^5 \bmod 39 = \underset{P}{16}$ }

d) Se puede crear una clave de sesion mediante Diffie-Hellman para enviarse puntualmente el mensaje PARIS junto a su MAC, para asegurar que no se ha modificado la ciudad.