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.

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 ·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.

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.

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?