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)

"Distribución y establecimiento de clave"

Ejercicios propuestos

Ejercicio 1:

Obtenga la clave secreta que A y B negociarían utilizando el algoritmo de Diffie-Hellman y supuestos los siguientes parámetros: generador del grupo g = 2, módulo común p = 17, el entero elegido por A (x) = 2, el entero elegido por B (y) = 5.

Ejercicio 2:

Alicia (A) y Berta (B) desean intercambiar una clave K usando el algoritmo de Diffie y Hellman. Para ello han elegido previamente el primo p = 13 como módulo común y el generador g = 7 del cuerpo p.

a) Si Alicia elige x = 7 y Berta elige y = 8, calcule qué clave se intercambian.

b) Carlos que conoce g y p, intercepta la comunicación anterior y elige c = 10. ¿Cómo procede Carlos para engañar a Alicia y Berta y realizar un ataque de hombre en el medio (tercera persona)? Indique numéricamente los mensajes que envía Carlos.

c) Comente qué contramedidas se pueden utilizar para evitar este atacante activo.

Ejercicio 3 :

Dos interlocutores A y B se conciertan para intercambiar mensajes cifrados mediante un cierto algoritmo y una clave obtenida a través del protocolo de Diffie-Hellman. Acuerdan trabajar módulo p, con p = 47, y con una base para las subsiguientes exponenciaciones g = 23.

a) Supuesto que cada uno elige los números aleatorios x = 12 y y = 33, calcule las cifras que se deben intercambiar para computar la clave K. Obtenga el valor de ésta.

b) Para enviar cifrado un mensaje en claro M mediante la clave K obtenida en el punto anterior ambas partes convienen en emplear el algoritmo $C = M^K \bmod n$, siendo $M = C^J \bmod n$ la fórmula del descifrado. Obtenga el valor de J de forma teórica.

c) Utilizando el algoritmo anterior calcule el criptograma e correspondiente a M = 16 con K = 25, suponga que n = 47. A continuación obtenga la clave J de descifrado y compruebe que al aplicarla sobre C obtiene el valor M de partida.

Ejercicio 4:

Ana (A) y Braulio (B) desean intercambiar una clave secreta K mediante el algoritmo de Diffie-Hellman. Para este propósito eligen el primo p = 31 y sopesan qué generador g en el cuerpo Z_p escoger.

a) Encuentre el generador g más pequeño dentro del cuerpo Z_p.

b) Ignore el resultado del apartado anterior y considere que escogen g=11. Ana (A) elige como entero

aleatorio secreto $X_a = 5$ y Braulio (B) $X_b = 10$. Calcule qué clave K se intercambian.
c) ¿Qué ocurriría si Ana (A) y Braulio (B) hubiesen elegido un número g que no fuese generador del cuerpo Z_p ?
d) En lugar de trabajar en Z_{31}, ¿sería más seguro hacerlo en Z_{81}? Razone la respuesta.