Universidad
Carlos III de Madrid

Grupo COSEC · *Dpto. Informática*

Universidad Carlos III de Madrid

Intercambio de clave Diffie-Hellman

Criptografía y Seguridad Informática
Seguridad en las Tecnologías de la Información
Curso 2016/2017

Pablo Martín

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.

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.**

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.**

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.

DH

a, g, p b

$A = g^a \bmod p \longrightarrow A$

$B \longleftarrow B = g^b \bmod p$

$k = B^a \bmod p$ $k = A^b \bmod p$

1.) $g = 2$ $b = 5$

$p = 17$

$a = 2$

$A = 2^2 \bmod 17 \longrightarrow A = 4$

$B = 15 \longleftarrow B = 2^5 \bmod 17$

$k = 15^2 \bmod 17 = 4$ $k = 4^5 \bmod 17 = 4$

2.) $p = 13$ $g = 7$

$a = 7$ $b = 8$

a.) $A = 7^7 \bmod 13 = 6 \longrightarrow A = 6$

$B = 3 \longleftarrow 13 = 7^8 \bmod 17 = 3$

$k = 3^7 \bmod 13 = 3$ $k = 6^8 \bmod 13 = 3$

b) Carlos "man in the midde" con $C = 10$

$A = 7^7 \bmod 13 = 6 \longrightarrow A = 6$

$C = 4 \longleftarrow C = 7^{10} \bmod 13 = 4 \longrightarrow C = 4$

$k = 4^7 \bmod 13 = 4$ $k_A = 6^{10} \bmod 13 = 4$ $B = 7^8 \bmod 13 = 3$

$B = 3$

$k_B = 3^{10} \bmod 13 = 3$ $k = 4^8 \bmod 13 = 3$

C) Como contramedida es mandar g y p por canal seguro

3.) $g=23$ $\quad a=12$ $\quad b=33$

$p=47$

a) $A = 23^{12} \bmod 47 = 27 \longrightarrow A=27$

$23^6 \cdot 23^6 = (23^6)^2$

$B=33 \quad \longleftarrow \quad B = 23^{33} \bmod 47 = 33$

$k = 33^{12} \bmod 47 = 25 \qquad k = 27^{33} \bmod 47 = 25$

b) $C = M^k \bmod n$ } ¿J?

$M = C^J \bmod n$ }

$k=25$

Como es $\phi(n)$ completo, es su mod sobre 1

$M = C^J \bmod n = (M^k)^J \bmod n$

$\phi(n)+1 = kJ$

Por euler queremos $M^{\phi(n)}$

$M^{\phi(n)} \bmod n = 1$

$kJ \bmod \phi(n) = 1$

$M^{\phi(n)-1} \bmod n = M = M^{kJ} \bmod n$

Coinciden

$J = k^{-1} \bmod \phi(n)$

c.) $C = 16^{25} \bmod 47 = 21 \qquad M = 21^J \bmod 47 = 21^{35} \bmod 47 = 16$

$J = 25^{-1} \bmod \underset{\phi(47)}{46} = -11 \bmod 46 = 35 \bmod 46$

$46 = 25 \cdot 1 + 21$

$25 = 21 \cdot 1 + 4$

$21 = 4 \cdot 5 + 1 \quad ; \; 1 = 21 - 5 \cdot 4$

$4 = 1 \cdot 4$

$1 = 21 - 5(25 - 21)$

$1 = \overset{(46-25)}{-5 \cdot 25 + 5(46 - 25)} \quad \overset{5 \cdot 46 - 5 \cdot 25}{;}$

$1 = 6 \cdot 46 - 11 \cdot 25$

4.) $g = 11$ $\quad a = 5 \quad b = 10$

$p = 31$

a.) Hacer nosotros.

b) $A = 11^5 \bmod 31 = 6 \longrightarrow A = 6$

$B = 5 \longleftarrow B = 11^{10} \bmod 31 = 5$

$k = 5^5 \bmod 31 = 25 \quad K = 6^{10} \bmod 31 = 25$

c.) El algoritmo secreto sería mucho mas sencillo.

d.) No es más seguro, ya que rompe la regla de que p sea primo.