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.**

**Solución:**

| A calcula: | | B calcula: |
|---|---|---|
| $X = g^x$ mód p = $2^2$ mód 17 = 4 | → | X = 4 |
| Y = 15 | ← | $Y = g^y$ mód p = $2^5$ mód 17 = 15 |
| $Y^x$ mód p = $15^2$ mód 17 = 4 | | $X^y$ mód p = $4^5$ mód 17 = 4 |
| Clave secreta calculada: **K = 4** | | Clave secreta calculada: **K = 4** |

**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.**

**Solución:**

**a)**

| A calcula: | | B calcula: |
|---|---|---|
| $X = g^x$ mód p = $7^7$ mód 13 = 6 | → | X = 6 |
| Y = 3 | ← | $Y = g^y$ mód p = $7^8$ mód 13 = 3 |
| $Y^x$ mód p = $3^7$ mód 13 = 3 | | $X^y$ mód p = $6^8$ mód 13 = 3 |
| Clave secreta calculada: **K = 3** | | Clave secreta calculada: **K = 3** |

**b)**

| A calcula: | | C calcula: | | B calcula: |
|---|---|---|---|---|
| $X = g^x$ mód p = $7^7$ mód 13 = 6 | → | X = 6 | | |
| | | | ← | $Y = g^y$ mód p = $7^8$ mód 13 = 3 |
| Z = 4 | | | → | Z = 4 |
| | ← | $Z = g^z$ mód p = $7^{10}$ mód 13 = 4 | | |
| $Z^x$ mód p = $4^7$ mód 13 = 4 | | $X^z$ mód p = $6^{10}$ mód 13 = 4 | | $Z^y$ mód p = $4^8$ mód 13 = 3 |
| | | Clave secreta: $\mathbf{K_{Alicia} = 4}$ | | |
| Clave secreta calculada: **K = 4** | | $Y^z$ mód p = $3^{10}$ mód 13 = 3 | | Clave secreta calculada: **K = 3** |
| | | Clave secreta: $\mathbf{K_{Berta} = 3}$ | | |

**c)**

El problema es que se están enviando de forma no autenticada X e Y, lo que serían las claves públicas de ambos interlocutores junto con los otros parámetros públicos (las claves privadas serían x e y). Es decir, el algoritmo de Diffie-Hellman proporciona una negociación de clave no autenticada. Posibles contramedidas utilizarían métodos de autenticación de los mensajes (de las propias claves públicas). Por ejemplo, se podría utilizar funciones resumen (y comparar los valores a través de un canal autenticado como el teléfono u otros), funciones MAC (suponiendo otra clave compartida entre los dos interlocutores con anterioridad), o funciones resumen combinadas con cifrado simétrico (suponiendo también que existe una clave compartida). Otra posibilidad es que cada interlocutor posea una pareja de claves pública y privada, y que puedan acceder a las claves públicas de forma auténtica (por ejemplo un certificado); los mensajes en este caso se enviarían firmados.

**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 $C = M^K$ mod n, siendo $M = C^J$ mod 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.**

**Solución:**

**a)**

| A calcula: | | B calcula: |
|---|---|---|
| $X = g^x$ mód p = $23^{12}$ mód 47 = 27 | ⟶ | X = 27 |
| Y = 33 | ⟵ | $Y = g^y$ mód p = $23^{33}$ mód 47 = 33 |
| $Y^x$ mód p = $33^{12}$ mód 47 = 25 | | $X^y$ mód p = $27^{33}$ mód 47 = 25 |
| Clave secreta calculada: **K = 25** | | Clave secreta calculada: **K = 25** |

**b)**

$C = M^K$ mód n y $M = C^J$ mód n, por lo tanto

$$M = (M^K)^J \text{ mód } n = M^{K \cdot J} \text{ mód } n \qquad (1)$$

Por el teorema de Euler sabemos que $M^{\phi(n)}$ mód n = 1, por lo tanto multiplicando a ambos lados por M obtenemos $M \times M^{\phi(n)}$ mód n = 1 x M, es decir,

$$M^{\phi(n)+1} \text{ mód } n = M\ 1 \qquad (2)$$

De (1) y (2) se deduce que $M^{K \cdot J}$ mod n = $M^{\phi(n)+1}$ mód n, por lo tanto $K \cdot J = \phi(n) + 1$. Si tomamos módulo $\phi(n)$, obtenemos que $K \cdot J$ mód $\phi(n) = 1$ mód $\phi(n)$, es decir, **$K \cdot J$ mod $\phi(n) = 1$**, ambas claves son inversas módulo $\phi$ (n).

**c)**

M= 16, K=25, n=47
$C = M^K$ mód n; $C = 16^{25}$ mod 47 = 21; **C = 21**
$\phi(47) = 46$ por ser primo.
$25 \cdot J$ mód $\phi$ (47) = 1; $25 \cdot J$ mód 46 = 1 => J = -11 mód 46 = 35 mód 46; **J= 35**
$M = C^J$ mód n; $M = 21^{35}$ mod 47 => **M = 16** valor inicial del mensaje en claro.

**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.**

**Solución:**

a)
Un generador g de $Z_{31}$ tendrá que ser un número tal que $1<g<31$ y $g^a$ mód. p $\neq 1$ $\forall a \mid 0<a<30$.
Si p es primo, $x \in Z_p$ y $x^a$ mód. p =1 para algún a<p entonces a es divisor de p-1.
Tenemos que p = 31; p-1 = 30 = 2x3x5; luego los divisores de 30 son 2,3,5,6,10,15:
$2^2$ mód. 31 = 4; $2^3$ mód. 31 = 8; $2^5$ mód. 31 = 1; 2 no es generador
$3^2$ mód. 31 = 9; $3^3$ mód. 31 = 27; $3^5$ mód. 31 = $3^3$ $3^2$ mód. 31 = (-4) 9 mód. 31= -5 mód 31=26;
$3^6$ mód. 31 = 3 (-5) mód. 31 = 16; $3^{10}$ mód. 31 = (-5) (-5) mód. 31 = 25;
$3^{15}$ mód. 31 = (-25) 5 mód. 31 = 6 5 mód. 31= 30 ;
Por lo tanto **3 es el generador más pequeño** del cuerpo $Z_{31}$

b)
A envía a B: $g^{Xa}$ mód. p = $11^5$ mód. 31 = $11^2$ $11^2$ 11 mód. 31 = $(-3)^2$ 11 mód. 31=6
B envía a A: $g^{Xb}$ mód. p = $11^{10}$ mód. 31 = 6*6 mód. 31 = 5
B calcula: $6^{Xb}$ mód. p = $6^{10}$ mód. 31 = $5^5$ mód. 31= $(-6)^2$ 5 mód. 31 = 25
A calcula: $5^{Xa}$ mód. p = $5^5$ mód. 31 = $(-6)^2$ 5 mód. 31 = 25 .
**K= 25** es la clave que se intercambian A y B.

c)
Si Ana y Braulio no eligen un generador en el cuerpo $Z_p$, pueden seguir utilizando el protocolo, sólo que en este caso será mucho más fácil un ataque por fuerza bruta pues el problema del logaritmo discreto resulta menos complejo al no generarse todos los restos de $Z_p$.

d)
No se puede trabajar en el cuerpo $Z_{81}$ porque 81 no es primo y es condición necesaria en este protocolo que p sea primo. En caso de elegirse un número primo sería deseable que fuera un número elevado ya que el algoritmo será computacionalmente más seguro por el problema del logaritmo discreto.