DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

Diseño de algoritmos
Algoritmo Diffie-Hellmann

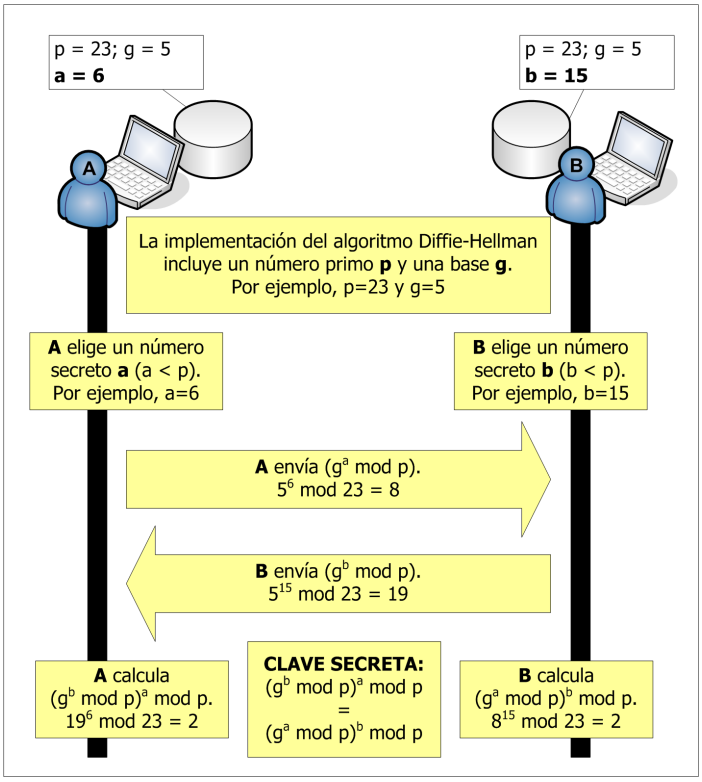
Fernando Cuartero

1. Introducción

El algoritmo de Diffie-Hellman (en honor a sus creadores, Whitfield Diffie y Martin Hellman) permite acordar una clave secreta entre dos máquinas, a través de un canal inseguro y enviando únicamente dos mensajes. La clave secreta resultante no puede ser descubierta por un atacante, aunque éste obtenga los dos mensajes enviados por el protocolo. La principal aplicación de este protocolo es acordar una clave simétrica con la que posteriormente cifrar las comunicaciones entre dos máquinas.

El protocolo de Diffie-Hellman fue publicado en 1976. Actualmente se sabe que es vulnerable a ataques de Man in the Middle (MitM): un atacante podría situarse entre ambas máquinas y acordar una clave simétrica con cada una de las partes, haciéndose pasar por el host A de cara al host B y viceversa. Una vez establecidas las 2 claves simétricas, el atacante haría de puente entre los 2 hosts, descifrando toda la comunicación y volviéndola a cifrar para enviársela al otro host.

Para corregir la vulnerabilidad del protocolo, éste debe ser utilizado conjuntamente con algún sistema que autentique los mensajes. Esto ocurre, por ejemplo, durante el establecimiento de la asociación HIP, donde los paquetes R1 e I2, además de contener los mensajes de Diffie-Hellman, están firmados digitalmente. No obstante, en el desarrollo de la práctica usaremos la forma básica.



2. Objetivos

En esta práctica se estudiará la forma de establecer una clave secreta compartida utilizando un canal no seguro de comunicación mediante el algoritmo Diffie-Hellman.

Los objetivos detallados a alcanzar son los siguientes:

1. Entender el funcionamiento del algoritmo.

Algoritmo 1 Algoritmo Diffie-Hellman

```
1:  procedimiento DiffieHellman
2:      Establecer un primo p y un generador n
3:          Se publican n y p por el canal inseguro
4:      Alice escoge un valor x secreto
5:          Calcula z_1 = n^x mod p
6:          Envía a Bob z_1 por el canal inseguro
7:      Bob escoge un valor y secreto
8:          Calcula z_2 = n^y mod p
9:          Envía a Alice z_2 por el canal inseguro
10:     Alice calcula la clave secreta z = z_2^x mod p
11:     Bob calcula la clave secreta z = z_1^y mod p
12: fin procedimiento
```

   Los valores de p y n son públicos y cualquier atacante puede conocerlos, pero esto no supone una vulnerabilidad. Aunque un atacante conociese dichos valores y capturara los dos mensajes enviados entre Alice y Bob, no sería capaz de averiguar la clave secreta.

   Supongamos un ejemplo basado en los valores de la figura, $p = 23$ y $n = 5$.

$$\begin{array}{rcrcl} z_1 & = & (5^x \bmod 23) & = & 8 \\ z_2 & = & (5^y \bmod 23) & = & 19 \end{array}$$

   La base del algoritmo es que, si x e y son suficientemente grandes, a partir de z_1 y z_2 no es posible recuperar, en tiempo razonable, los valores x e y, que se calculan mediante la función conocida como *logaritmo discreto*, y para que la que no existe una formulación eficiente conocida. En este caso concreto, se deberían probar todos los valores entre 1 y 22 para encontrar los valores de x e y.

2. Elaborar una función en python que codifique la función de exponenciación modular $z = n^x \bmod p$. Sígase el método visto en clase.

   No sirve usar la función exponencial de serie en el lenguaje, pues puede tener errores de redondeo, y es necesaria la precisión exacta para el funcionamiento del algoritmo. Por lo que es necesario implementarla mediante secuencia de multiplicaciones, pasando al módulo cuando se exceda del valor representable.

   Como el número de multiplicaciones es elevado, deberá usarse la técnica "Divide y Vencerás".

3. Utilizando el foro creado en la asignatura en Campus Virtual para la práctica por pares de alumnos (Alice y Bob) deben ponerse de acuerdo en la generación de una clave secreta para ambos.

   Cada componente de la pareja debe enviar un mensaje al foro con los siguientes datos:

- Destinatario
- Valores de p y n (deben coincidir con el mensaje de la contraparte)
- Valor z_i particular

Utilizando la función del ejercicio calcular el valor z común y secreto a ambos.

4. Ataque. Los ataques posibles son *Man in the Middle* o fuerza bruta. Usaremos éste, para ello seleccionad una pareja rival, y descubrir su secreto. Para realizar el ataque se consideran el p y n comunes a los dos. Se toman los valores z_1 y z_2 enviados por Alice y por Bob, y se calcula mediante un bucle por pruebas los valores x e y tales que dan lugar a z_1 y z_2. Basta encontrar uno de ellos para disponer de la clave común z.

   En particular, encontrar la clave común para estos datos:

$$\begin{aligned} n &= 12\ 345\ 701 \\ p &= 66\ 666\ 667 \\ z_1 &= 8\ 049\ 097 \\ z_2 &= 6\ 438\ 362 \end{aligned}$$

   Responder a las siguientes cuestiones:

   - Cuál es la clave común
   - Tiempo empleado en encontrarla
   - Cuales son los valores secretos a y b ideados por Alice y Bob.

     En principio, bastaría encontrar sólo uno de ellos si el objetivo es exclusivamente la clave común. No obstante, calculad los dos, indicando cual se ha encontrado primero, y el tiempo empleado, así como el total temporal hasta el segundo.

   NOTA.

   El tiempo empleado debe estar en el orden de los 15 minutos, para este caso de unos 8 dígitos. Aumentar el número de dígitos de los valores implicaría multiplicar el tiempo por un factor 10, aproximadamente, por cada uno de aumento. Explicad las consecuencias de esto.

   Los valores n y p son primos, en el primer caso, el menor primo que sigue a 12 345 678 y en el segundo, el primo menor que sigue a 66 666 666. En caso de no ser primos, el algoritmo funciona igual, pero se podría reducir el espacio de búsqueda y mejorar los ataques para tardar un tiempo menor.

3. Entregables, evaluación y normas

Para esta práctica, la entrega consiste en un archivo `.zip` que contenga los archivos de código y la memoria, en la que debe constar el desarrollo, los mensajes enviados al foro mediante captura, los ataques, y las conclusiones.

Criterios de evaluación:

- Cualquier práctica cuyo código no sea ejecutable se considerará no entregada. El hecho de que funcione es requisito para que sea correcta, pero puede no ser suficiente.

- El plazo para la entrega de la práctica concluye el día indicado en el entregable de la plataforma. Todos aquellos que entreguen después, serán penalizados multiplicando la nota por un factor 0,8.

Normas de entrega

- La práctica debe hacerse por parejas, o de manera individual adoptando los dos roles.
- La copia o plagio se penalizará con el suspenso de la asignatura.