Criptografía y Cifrado de Información 2021

Lab 08

07.octubre.2021

En este laboratorio simulamos un intercambio de claves usando el método de Diffie-Hellman.

1. Simular un intercambio de claves usando el algoritmo de Diffie-Hellman. Para ello, debe hacer lo siguiente

   - Fijar un número primo $p > 2$, con un tamaño de bits elegido;
   - Fijar un generador g, donde $1 < g < p - 1$;
   - Simular dos participantes: Alice y Bob. Para cada uno, generar claves secretas ($\mathbf{a}$ para Alice y $\mathbf{b}$ para Bob), donde $\mathbf{a}$ y $\mathbf{b}$ son elementos aleatorios en el rango $1 < \mathbf{a}, \mathbf{b} < p - 1$.
     Alice debe enviar el valor $A = g^{\mathbf{a}}$ a Bob, mientras que Bob debe enviar el valor $B = g^{\mathbf{b}}$ a Alice.
   - Luego, Alice debe calcular $B^{\mathbf{a}}$; Bob debe calcular $A^{\mathbf{b}}$, y verificar que este resultado coincide.

   Repetir el ejercicio con diferentes primos p:

   - p de 6 dígitos;
   - p de 10 dígitos;
   - p de 14 dígitos.

   Los primos pueden ser generados aleatoriamente, o se puede consultar una tabla de números primos. Por ejemplo, `http://compoasso.free.fr/primelistweb/page/prime/liste_online_en.php`

2. Utilizar la librería **pyDH**, la cual ya contiene una implementación del método de Diffie-Hellman. Las referencias a esta librería pueden encontrarse en:
   `https://pypi.org/project/pyDH/`
   `https://github.com/amiralis/pyDH`.

   En combinación con otro equipo de trabajo (los cuales se indican a continuación), hacer lo siguiente:

   - Acordar entre ambos equipos un método de generación de claves de Diffie-Hellman. Por ejemplo, usando el parámetro `group=14`.
   - Cada equipo generar una clave secreta d_i, y su respectiva clave pública.
   - La clave pública deberá ser compartida con el otro equipo, sólo la clave pública.
   - Cada grupo debe calcular la llave compartida según el protocolo de Diffie-Hellman.
   - Con la clave compartida, ambos equipos deberán enviar un mensaje al otro equipo de trabajo, haciendo alguna pregunta de un tema libre. Para ello, antes deberán acordar en común un esquema de cifrado, por ejemplo AES con SHA-256, o similar, y en dicho cifrado deberán usar la clave compartida proveniente del método de Diffie-Hellman.
   - El mensaje cifrado recibido, deberá ser descifrado, respondido y enviado de vuelta al otro equipo, usando el esquema de cifrado acordado. resultado coincide.

   Los equipo a trabajar en conjunto son los siguientes:

   - Equipos 1 y 12,
   - Equipos 2 y 11,
   - Equipos 3 y 10,
   - Equipos 4 y 9,
   - Equipos 5 y 8,
   - Equipos 6 y 7.