UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
SISTEMAS DE COMUNICACIÓN

Laboratorio 3 Sistemas de Comunicación

Instrucciones

El objetivo de esta experiencia es implementar un protocolo de intercambio de claves asimétrico, que en esta ocasión será el protoloco Diffie-Hellman bajo el lenguaje de programación Java. Para encriptar los mensajes deberán utilizar el sistema de encriptación simétrico que diseñaron e implementaron durante la experiencia número 2. La implementación para este laboratorio debe contar con una interfaz gráfica en que se reflejen claramente el paso a paso del protocolo de intercambio de claves.

Para simular la comunicación entre 2 clientes deberán utilizar **Java RMI**, librería que permite emular una red con clientes remotos. Se agendará una clase de laboratorio para revisar y aclarar dudas sobre esta librería una vez liberado este enunciado.

En esta ocasión deberá realizar un manual de usuario conciso en que se expliquen los pasos claramente del protocolo. Queda a criterio de cada grupo el formato de éste. Además, junto al código fuente deben adjuntar un archivo README con las instrucciones de compilación.

Este laboratorio debe ser realizado en los mismos grupos que han sido conformados anteriormente. En caso de copia será evaluado con nota mínima y causal de reprobación del laboratorio. La fecha de entrega es el día 9 de Diciembre de 2016 a las 23:55, y tanto el código fuente como el manual de usuario deben ser entregados vía Moodle en el link habilitado para este propósito en un archivo comprimido con extensión 7z o zip.

Se bonificarán los trabajos realizados con controlador de versiones y son libres de utilizar el sistema operativo que más les acomode.

Protocolo Diffie-Hellman: Algoritmo

Se comienza bajo la situación en que existe una máquina A que quiere establecer una conexión con otra máquina B de forma segura, es por esto que necesitan intercambiar sus claves.

1. Ambas máquinas, tanto A como B deben seleccionar dos números primos al azar, “a” y “p”, y uno servirá de base. Para este ejemplo, a = 5 y p = 23

2. Al ocurrir esto, ambos seleccionan su clave privada, que será un número al azar. La máquina A escoge el 6 y la B el 15.

3. Por una parte la máquina A envía a B $5^6 mod 23 = 8$, y la B hace lo mismo con su clave secreta: $5^{15} mod 23 = 19$

4. Ahora bien, A con el resultado enviado desde la máquina B hace nuevamente el mismo cálculo, tomando como base el valor recibido: $19^6 mod 23 = 2$

5. Finalmente, la máquina B realiza el mismo procedimiento y obtiene el mismo resultado: $8^{15} mod 23 = 2$

Así, a través del intercambio de claves ambos logran obtener la clave de sesión válida para encriptar los mensajes durante el tiempo que se requiera.

Diffie-Hellman Key Exchange

Step	Alice	Bob
1	Parameters: p, g	
2	$A = \text{random}()$ $a = g^A \pmod p$	$\text{random}() = B$ $g^B \pmod p = b$
3	$a \longrightarrow$ $\longleftarrow b$	
4	$K = g^{BA} \pmod p = b^A \pmod p$	$a^B \pmod p = g^{AB} \pmod p = K$
5	$\longleftarrow E_K(data) \longrightarrow$	

Recurso asociado: `https://youtu.be/M-0qt6tdHzk`