Organización de Datos – Curso Servetto

Evaluación Módulo Criptografía-Archivos Multimediales, 09 de Diciembre de 2005

Resolver los ejercicios de criptografía y archivos multimediales en hojas separadas.

Criptografía

> *Nota: Por protocolo criptográfico se entiende conjunto finito de pasos que deben realizar las partes involucradas para llevar a cabo un objetivo. El mismo debe ser de previo conocimiento de las partes participantes. Además debe ser completo (no existen situaciones que no abarque) y no ambiguo (para cada situación un único resultado)*

1. Alejandro y Lucas desean jugar al poker de forma **remota**, pero no se tienen confianza entre sí. El problema consiste en conseguir que ninguno de los dos pueda ni ver las cartas del contrario, ni influir en las propias cartas. Para simplificar se supone que no hay descarte.
   Se pide diseñar un protocolo criptográfico que resuelta la problemática planteada. Recordar que la baraja francesa tiene 54 cartas.

2. Explique el esquema de encriptación que utiliza PGP.

3. ¿Cuanto tiempo llevaría romper por fuerza bruta el algoritmo TDES?

Archivos Multimediales

4. ¿Cuál es la diferencia entre pasar una secuencia de imágenes y un video MPEG? Explique.
5. ¿Cómo se logra el funcionamiento de avance rápido y rebobinado en un CD de música estándar? ¿Debería cambiar algo esta solución si se aplica a Video XVID (archivos de PC)?

Posible solución:

1. Protocolo Poker:

Solución 1: (no arbitrado)

Hipótesis: juegan con dos mazos de cartas.

1. Alejandro elige un par de claves (K_{puA}, K_{prA})
2. Alejandro comunica a Lucas su clave pública (K_{puA})
3. Lucas elige un par de claves (K_{puL}, K_{prL})
4. Lucas comunica a Alejandro su clave pública (K_{puL})
5. Alejandro genera una clave de sesión simétrica aleatoria. Con ella encripta las 54 cartas (mensajes), obteniendo: $\{c_1, c_2, \ldots c_{54}\}$ donde $c_i = E_{KSA}(m_i)$
6. Alejandro envía los 54 criptogramas a Lucas (no los puede leer por no tener la clave de sesión de Alejandro).
7. Lucas elige entre los 54 criptogramas, 5 que corresponderán a las cartas de Alejandro.
8. Lucas envía los 5 criptogramas a Alejandro.

9. Lucas genera una clave de sesión simétrica aleatoria. Con ella encripta las 54 cartas (mensajes), obteniendo: $\{c_1, c_2, \ldots c_{54}\}$ donde $c_i = E_{KSL}(m_i)$
10. Lucas envía los 54 criptogramas a Alejandro (no los puede leer por no tener la clave de sesión de Lucas).
11. Alejandro elige entre los 54 criptogramas, 5 que corresponderán a las cartas de Lucas
12. Alejandro s envía los 5 criptogramas a Lucas.
13. Alejandro y Lucas realizan sus apuestas
14. Alejandro comunica su clave de sesión a Lucas
15. Lucas comunica su clave de sesión a Alejandro
16. Alejandro y Lucas comprueban que el otro no haya hecho trampa, verificando las copias de los criptogramas con la correspondiente clave de sesión.

Solución 2: (no arbitrado)

1. al 8 ídem anterior
9. Lucas elige entre los 54 criptogramas otros 5 que corresponderán a sus propias cartas.
10. Lucas cifra estos 5 criptogramas con su propia clave pública, obteniendo: $c_i' = E_{KpuL}(c_i)$
11. Lucas envia estos 5 criptogramas (c_i') a Alejandro, que no puede leerlos por no disponer de la clave privada de Lucas.
12. Alejandro desencripta cada uno de los criptogramas enviados por Lucas (ci') con su clave privada, obteniendo $D_{KprA}(E_{KpuL}(E_{KpuA}(m_i))) = E_{KpuL}$
    Importante: para que funcione lo anterior, el algoritmo debe ser conmutativo, es decir, que permita hacer cifrados sucesivos sin importar el orden (ej. RSA)
    Alejandro retira su propio cifrado de los criptogramas, pero sin poder retirar el que ha introducido Lucas.
13. Alejandro devuelve los 5 mensajes parcialmente descifrados a Lucas ($E_{KpuL}(m_i)$)
14. Lucas descifra cada uno de los 5 criptogramas devueltos por Alejandro con su clave privada, permitiéndole conocer sus propias cartas.
15. Alejandro y Lucas realizan sus apuestas
16. Alejandro comunica su clave privada a Lucas
17. Lucas comunica su clave privada a Alejandro
18. Alejandro y Lucas comprueban que el otro no haya hecho trampa, verificando las copias de los criptogramas

Solución 3: (no arbitrado) – Propuesta por: Andrés Giachini (2005 2C)

1. Lucas genera una clave de sesión simétrica aleatoria (Klsa1)
2. Alejandro genera una clave de sesión simétrica aleatoria (Kasa1)
3. Lucas encripta todas las cartas con su clave de sesión (Klsa1)
4. Lucas le envía todos los criptogramas a Alejandro
5. Alejandro vuelve a encriptar los criptogramas pero con su clave de sesión (Kasa1).
6. Alejandro le envía a Lucas los nuevos criptogramas.
7. Lucas y Alejandro elijen sus 5 criptogramas de los que envió Alejandro.
8. Lucas genera una nueva clave de sesión y encripta una copia de sus criptogramas elegidos (Klsa2).
9. Alejandro genera una nueva clave de sesión y encripta una copia de sus criptogramas elegidos (Kasa2).
10. Lucas y Alejandro se envían la copia de sus criptogramas (se envían copias de los criptogramas Eligio cada uno para evitar fraude)

    Obs.: Este punto es clave para evitar que hagan trampa, ya que ambos tienen acceso al mazo encriptado. Pero para que las cartas del adversario no se puedan ver se encriptan otra vez con la segunda clave de sesión.

11. Lucas y Alejandro intercambian sus primeras claves de sesión (Klsa1, Kasa1).

    Obs.: En este momento, cada jugador puede ver sus cartas desencriptándolas con su Kasa1 y luego con Klsa1, en ese orden.

12. Lucas y Alejandro realizan sus apuestas. (Ambos son capaces de ver sus cartas pero no la del adversario)
13. Lucas y Alejandro intercambian sus segundas claves de sesión. (Klsa2,Kasa2)
14. Alejandro y Lucas comprueban que el otro no haya hecho trampa verificando las copias de los criptogramas con la correspondiente segunda y primera clave de sesión.

A continuación se indica una posible solución con una cuarta persona cumpliendo el rol de árbitro. Es a modo informativo, dado que en el ejercicio se pedía un protocolo no arbitrado.

Solución 3: (arbitrado)

1. Arturo elige al azar 5 cartas y se las envía a Alejandro
2. Arturo elige al azar 5 cartas y se las envía a Lucas
3. Alejandro y Lucas realizan sus apuestas
4. Arturo informa a Alejandro de la jugada de Lucas, y a Lucas de la jugada de Alejandro.

2. Ver ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf sección "How PGP Works"

3. TDES

Tamaño de clave: 112 bits (56 x 2) => espacio de claves = 2^{112}
Procesamiento: N claves / unidad de tiempo

Criptoanálisis por fuerza bruta (peor caso): **2^{112} / N unidad de tiempo**