CONTROL DE TRANSMISIÓN DE DATOS. 12 de Diciembre de 2006

Notas Importantes:

1. Los resultados no justificados, no serán tenidos en cuenta.
2. Los problemas se entregan por separado, ponga su nombre y apellidos en cada hoja, enumerándolas.
3. Un error conceptual grave, puede anular todo el problema.

Nota: Lista de los números primos menores que 300: 1 2 3 5 **7** 11 **13** 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 **193** 197 199 211 **223** 227 229 233 239 241 251 257 263 269 271 277 281 283 293.

Problema 1 (33%)

Sea un sistema sencillo de clave pública RSA **de módulo común**. Considere dos usuarios A y B y un **atacante pasivo** C. Los usuarios del sistema utilizan criptografía asimétrica RSA para intercambiar una clave de sesión. Las secuencias binarias se consideran con más peso a la izquierda (MPI). El sistema trabaja en bloques de 4 bits.

Parámetros RSA de los usuarios:

Usuario A	p=3, q=11, e_A=7, d_A=3
Usuario B	p=3, q=11, e_B=13, d_B=17

La función resumen o *Hash* H(M) de un mensaje M, se obtiene aplicando la operación OR-exclusiva (⊕), bit a bit, sobre los sucesivos bloques del mensaje M de entrada. El funcionamiento es el siguiente:

- Las secuencias binarias se consideran con más peso a la izquierda (MPI).
- Se añaden a la izquierda del mensaje tantos ceros como sea necesario para que la longitud sea múltiplo de 4.
- Se divide el mensaje resultante desde la izquierda en m bloques b_j, de n=4 bits cada uno, siendo $1 = j = m$.
- b_{ij} es el bit i-ésimo del bloque j-ésimo; $1 = i = n$
- $H(M)=C$. La función *Hash* de M es un bloque resultante $C=C_1C_2C_3\ldots C_n$ de n=4 bits, donde:
- El bit i-ésimo del bloque C es: $C_i=b_{i1}\oplus b_{i2}\oplus b_{i3}\oplus\ldots..\oplus b_{im}$.

El sistema no dispone de autoridad certificadora que expenda certificados firmados. Para autenticar la procedencia de una clave pública, cada usuario envía a su comunicante su propia clave pública **completa** y concatenada a la misma, añade la firma digital de su propia clave pública.

a) Obtenga el certificado digital que A envía a B, para que B pueda autenticar a A. Expréselo en hexadecimal. **(0,6p)**

b) Indique qué pasos seguirá el usuario B para autenticar la clave pública de A. Realice los cálculos necesarios. **(0,3p)**

c) Haga una brevísima crítica del sistema de autenticación de este sistema. **(0,3p)**

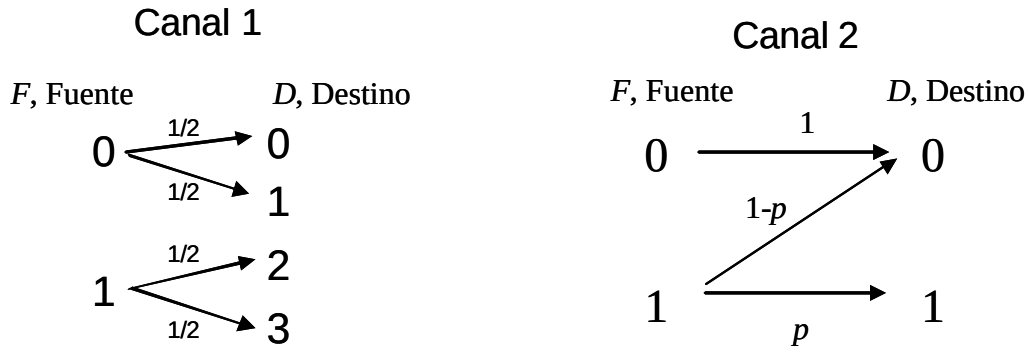
d) B desea comunicar una clave de sesión a A, $k_{sesión}$ = 6. Obtenga el criptograma que B envía a A. **(0,6p)**

e) Dicha clave de sesión es el estado inicial del LFSR con polinomio de conexiones C(D) completo de grado 3, que se utiliza para cifrar en flujo. Obtenga el criptograma que genera B para enviar codificado a A el mensaje M=11100. **(0,6p)**

f) En un momento dado, los usuarios A y B se intercambian el mismo mensaje $M_{A\rightarrow B}=M_{B\rightarrow A}=M$. El atacante pasivo captura los criptogramas $C_{A\rightarrow B}=14$ y $C_{B\rightarrow A}=26$. Qué hace el atacante para averiguar el mensaje M? Hágalo usted. **(0,9p)**

Problema 2 **(33%)**

Considere 2 canales discretos con los siguientes diagramas de transiciones:



a) Obtenga la matriz de probabilidades de transición P(D\F), para cada canal. Diga si se trata de un canal determinista, sin pérdidas, sin ruido, simétrico respecto de la entrada, simétrico o sin simetría. **(0,3p)**

b) Calcule la capacidad de canal, para cada canal. Exprésela en función de *p* para el canal 2. **(3p)**

Nota: Para mayor claridad de la solución, utilice $H(p) = p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{(1-p)}$

Pregunta 1 **(8%)**

Sean F_1={10, 12, 15} y F_2={3, 5, 20} dos fuentes equiprobables independientes. Sea una fuente F cuya salida es el **mcd** (F_1, F_2).

a) Calcule H(F). **(0,3p)**

b) Calcule I(F; F_1). **(0,5p)**

Pregunta 2 **(6%)**

Sea un sistema RSA con dos usuarios A y B. La clave pública de A es (e_A, N_A)=(7, 91)

a) Obtenga una clave secreta para A, d_A. **(0,2p)**

b) A recibe este criptograma de B C_{BA}=47. Qué hace A para descifrarlo? Hágalo usted. **(0,2p)**

c) El mensaje obtenido, es la clave de sesión que utilizan para cifrase información, mediante el algoritmo simétrico de César. A envía a B el criptograma XTWY. Qué hace B para descifrarlo? Hágalo usted. **(0,2p)**

Pregunta 3 **(6%)**

Descodifique el mensaje 112357643 codificado mediante el algoritmo LZW (Lempel-Ziv-Welch). **(0,6p)**

Pregunta 4 **(8%)**

Realice la operación 193^{891} mod 223. No utilice el método del Campesino Ruso. No utilice la calculadora para obtener el resultado final directamente. **(0,8p)**

Pregunta 5 **(6%)**

Se dispone de un codificador aritmético para una fuente de alfabeto {A, B, C, D}. Las probabilidades asociadas a los símbolos fuente son p(A)=p(D)=1/3, p(B)=P(C)=1/6.

a) Decodifique el valor 0,63 si procede de una secuencia de 4 caracteres. **(0,3p)**

b) Codifique la secuencia ABC. **(0,3p)**