Control Aguilar

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 $1 \leq j \leq m$.
- b_{ij} es el bit i-ésimo del bloque j-ésimo; $1 \leq i \leq n$
- $H(M)=C$. 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)**

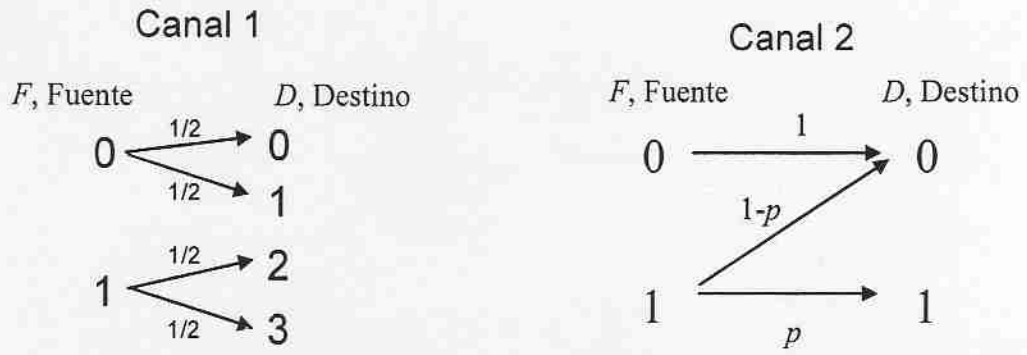
d) B desea comunicar una clave de sesión a A, $k_{sesión}$ = 6. Obtenga el criptograma que B envía a A. **(0,6p)**

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 $M_{A\to B}=M_{B\to A}=M$. El atacante pasivo captura los criptogramas $C_{A\to B}$=14 y $C_{B\to A}$=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)** Alfabeto fuente={A,B,C}

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)**

Control 12/12/06. Mónica Aguilar. Trans. de Datos

Problema 1

Módulo común para A, B:
$N = p \cdot q = 3 \cdot 11 = 33$

a) Certificado(A) = $\underbrace{e_A \| N}_{M} \| FD(M)$

$M = \underbrace{0111}_{e_A=7} \| \underbrace{0010 \| 0001}_{N_A = N = 33}$

$H(M) = 0100 \equiv 4$ (1⊕1⊕0)

0001 | 1111 (111)

$FD(M) = (H(M))^{d_A} \bmod N = 4^3 \bmod 33 = 64 \bmod 33 = 31$

$\boxed{\text{Certificado(A)} = \underbrace{\underbrace{0111}_{e_A=7} \| \underbrace{0010 \| 0001}_{N_A=33}}_{M} \| \underbrace{0001 \| 1111}_{FD(M)} \equiv 7211F}$

b)
- B recibe el Certificado(A)
- B extrae la clave pública de A, $K_{PA} = (e_A, N) = (7, 33)$
- B genera $H(M) = \dots = 4$ //
- B calcula H(M) a partir de $F_D(M) \Rightarrow H(M) = F_D(M)^{e_A} \bmod N =$

$= 31^7 \bmod 33 = \dots = 4$ //

$7 \equiv 111$ (1)

$31^7 = (31^2 \cdot 31)^2 \cdot 31$ (4)

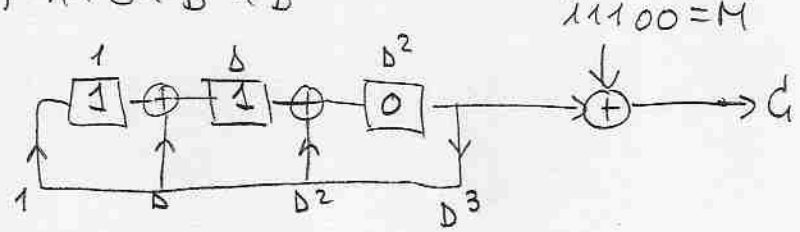
$31^2 \bmod 33 = 4$;; $124 \bmod 33 = 25$;; $25^2 \bmod 33 = 31$;; $31^2 \bmod 33$ (4)

- Como coincide H(M) generado y calculado, (e_A, N) autentificada, la ha generado A.

d) $B \xrightarrow[K_{sesion}=6]{} A$ $\quad \boxed{C_{BA}(K_{sesion}) = (K_{sesion})^{e_A} \bmod N =}$

$= 6^7 \bmod 33 = \boxed{30}$

e) $C(D) = 1 + D + D^2 + D^3$



1	D	D^2	
1	1	0	↕ L=2
0	1	1	
1	1	0	
0	1	1	
⋮			

$d = M \oplus S(i) = 11100 + 01010 =$

$= \boxed{10110}$

8) Atacante pasivo debe aprovechar que el módulo es común y se envían el mismo mensaje al inicio de la acción. ⇒ Ataque RSA por módulo común.

- El atacante pasivo conoce $e_A, e_B, N, C_{AB}, C_{BA}$.
- Si $mcd(e_A, e_B) = 1$ (7, 13), $\exists$ r, s enteros $\mid r \cdot e_A + s \cdot e_B = 1$
- $\left.\begin{array}{l} C_{AB} = M^{e_B} \bmod N = 14 \\ C_{BA} = M^{e_A} \bmod N = 26 \end{array}\right\} \left(C_{AB}^{s} \cdot C_{BA}^{r}\right)_{\bmod N} = \left(M^{s \cdot e_B} \cdot M^{r \cdot e_A}\right) \bmod N =$

$= M^{s \cdot e_B + r \cdot e_A} \bmod N =$

$= M^1 \bmod N = M \bmod N$

$\Rightarrow \left(C_{AB}^{s} \cdot C_{BA}^{r}\right) \bmod N = M \bmod N$

$\left.\begin{array}{l} e_A = 7 \\ e_B = 13 \end{array}\right\}$ ¿r, s? $\mid$ $r \cdot 7 + s \cdot 13 = 1$ (r = 2, s = −1) $\Rightarrow \boxed{\begin{array}{l} r = 2 \\ s = -1 \end{array}}$

$\boxed{M = \left(C_{AB}^{-1} \cdot C_{BA}^{2}\right) \bmod N = \left(26 \cdot 26^2\right) \bmod 33 = 17576 \bmod 33 = 20}$

(C_{AB}^{-1} = 14)

$C_{AB}^{-1} \cdot C_{AB} = 1 \bmod N = 1 + K \cdot N$

$C_{AB}^{-1} = \dfrac{1 + K \cdot 33}{14} = \dfrac{1 + K \cdot (14 \cdot 2 + 5)}{14} = 2K + \dfrac{5K + 1}{14} = 22 + 4 = 26$

(33 = 2 · 14 + 5; 14 = 2 · 5 + 4; 5 = 1 · 4 + 1; 4 = 4 · 1 + 0; $\frac{14}{2}$)

$\downarrow$ K = 11

c) Cualquiera se firma sus claves, incluso un atacante !!

Problema 2

B_1 B_2 B_3 B_4
$\|$ $\|$ $\|$ $\|$
0 1 2 3

a) Canal 1 → $p(D\backslash F) = \begin{matrix} A_1=0 \\ A_2=1 \end{matrix} \begin{pmatrix} 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 \end{pmatrix}$ (0'15)

Canal Determinista $\Rightarrow H(D\backslash F) = \emptyset \equiv$ Conocida la entrada, la salida queda determinada $\Rightarrow$ NO

Canal Sin pérdidas $\Rightarrow H(F\backslash D) = \emptyset \equiv$ Conocida la salida, la entrada queda determinada $\Rightarrow$ SÍ

Canal SIN RUIDO $\Rightarrow H(D\backslash F) = H(F\backslash D) = \emptyset \equiv$ canal Determinista Sin pérdidas $\Rightarrow$ NO

Canal Simétrico respecto entrada $\Rightarrow$ SÍ. Mismos elementos $\forall$ fila.

Canal Simétrico $\Rightarrow$ SÍ. Mismos elementos $\forall$ fila, $\forall$ column.

0'15) Canal 2 → $p(D\backslash F) = \begin{matrix} A_1= \\ A_2=1 \end{matrix} \begin{matrix} B_1=0 & 1=B_2 \end{matrix} \begin{pmatrix} 1 & 0 \\ 1-p & p \end{pmatrix}$ Canal sin simetrías.

(1) b) Canal 1

$H(F\backslash D) = \emptyset \;\Rightarrow\; C = \max_{p\{A_i\}} \underbrace{\left[H(D) - H(D\backslash F)\right]}_{I(F;D)} = \max_{p\{A_i\}} \underbrace{\left[H(F) - H(F\backslash D)\right]}_{I(F;D)}$

$$\boxed{C = \max_{p\{A_i\}} H(F) \underset{\forall A_i,\, p(A_i)=\frac{1}{2}}{=} 2 \cdot \frac{1}{2} \cdot \log_2 2 = 1 \text{ bit/símbolo}}$$

(2) Canal 2

$$H(D\backslash F) = p(A=0)\cdot \underbrace{H(D\backslash A=0)}_{1\cdot\log_2 1 = 0} + p(A=1)\cdot \underbrace{H(D\backslash A=1)}_{(1-p)\cdot\log_2\frac{1}{1-p} + p\cdot\log_2\frac{1}{p} = H(p)} = p(A=1)\cdot H(p)$$

$$H(D) = \sum_{i=1}^{2} p(B_i)\cdot\log_2\frac{1}{p(B_i)}$$

$$p(B=0) = p(A=0) + (1-p)\cdot p(A=1) = 1 - p\cdot p(A=1)$$

$$p(B=1) = p\cdot p(A=1)$$

$$C = \max_{\{p(A_i)\}} \left[H(D) - H(D\backslash F) \right] = \max_{\{p(A_i)\}} \left[p \cdot p(A=1) \cdot \log_2 \frac{1}{p \cdot p(A=1)} + \right.$$

$$\left. + \left(1 - p \cdot p(A=1)\right) \cdot \log_2 \frac{1}{1 - p \cdot p(A=1)} - H(p) \cdot p(A=1) \right] = \max_{x} \left(f(x) \right)$$

$$p(A=1) = x$$

$$\boxed{f(x) = p x \cdot \log_2 \frac{1}{p \cdot x} + (1 - p \cdot x) \cdot \log_2 \frac{1}{1 - p \cdot x} - H(p) \cdot x} \quad (*)$$

$$f'(x) = p \cdot \log_2 \frac{1}{px} + p^2 x^2 \cdot \frac{-1}{p^2 x^2} \cdot \frac{1}{\ln 2} \cdot p + (-p) \cdot \log_2 \frac{1}{1-px} + \frac{(1-px)^2}{\ln 2} \cdot \frac{+p}{(1-px)^2} - H(p$$

$$= p \cdot \log_2 \frac{1}{px} - \frac{p}{\ln 2} - p \cdot \log_2 \frac{1}{1-px} + \frac{p}{\ln 2} - H(p) =$$

$$= p \cdot \log_2 \frac{1-px}{px} - H(p)$$

$$f'(x) = 0 \Rightarrow \log_2 \frac{1-px}{px} = \frac{H(p)}{p} \Rightarrow \frac{1-px}{px} = 2^{\frac{H(p)}{p}}$$

$$1 - px = p \cdot 2^{H(p)/p} \cdot x \;\; // \;\; 1 = x \cdot p \cdot \left(1 + 2^{H(p)/p}\right)$$

$$\boxed{x_{max} = \frac{1}{p \cdot \left(1 + 2^{H(p)/p}\right)}} \qquad \boxed{C = f(x_{max}) \;\; \text{bits/symbol}} \quad (*)$$

Pregunta 1

F_1	F_2
$10 = 2 \cdot 5$	3
$12 = 3 \cdot 2^2$	5
$15 = 3 \cdot 5$	$20 = 5 \cdot 2^2$

F
1
5
10
3
1
4
3
5
5

$\equiv$

F	
1	$\rightarrow p(1) = 2/9$
3	$\rightarrow p(3) = 2/9$
4	$\rightarrow p(4) = 1/9$
5	$\rightarrow p(5) = 3/9$
10	$\rightarrow p(10) = 1/9$

a)

$$H(F) = 2 \cdot \frac{2}{9} \cdot \log_2 \frac{9}{2} + 2 \cdot \frac{1}{9} \cdot \log_2 9 + \frac{3}{9} \cdot \log_2 \frac{9}{3} = 2'1971 \text{ bits/símbolo}$$

b) $I(F;F_1) = H(F) - H(F \setminus F_1)$

$$H(F \setminus F_1) = p(F_1=10) \cdot H(F \setminus F_1=10) + p(F_1=12) \cdot H(F \setminus F_1=12) + p(F_1=15) \cdot H(F \setminus F_1=15)$$

($p(F_1=10) = 1/3$, $p(F_1=12) = 1/3$, $p(F_1=15) = 1/3$)

$P(F \setminus F_1)$

F_1 \ F	1	3	4	5	10
10	1/3	0	0	1/3	1/3
12	1/3	1/3	1/3	0	0
15	0	1/3	0	2/3	0

$$H(F \setminus F_1=10) = H(F \setminus F_1=12) = 3 \cdot \frac{1}{3} \cdot \log_2 3 = 1'5849 \text{ bits/símbolo}$$

$$H(F \setminus F_1=15) = \frac{1}{3} \log_2 3 + \frac{2}{3} \log_2 \frac{3}{2} = 0'9183 \text{ bits/símbolo}$$

$$H(F \setminus F_1) = \frac{1}{3} \cdot 1'5849 \cdot 2 + \frac{1}{3} \cdot 0'9183 = 1'3627 \text{ bits/símbolo}$$

$$I(F;F_1) = 2'1971 - 1'3627 = 0'8344 \text{ bits/símbolo}$$

Pregunta 2

a) $e_A \cdot d_A = 1 + k \cdot \phi(N_A)$;; $\phi(N_A) = (p_A - 1)\cdot(q_A - 1)$

$N_A = 91 = 7 \cdot 13 \Rightarrow p_A = 7$;; $q_A = 13 \Rightarrow \phi(N_A) = 6 \cdot 12 = 72$

↓ Consultar tabla primos

$7 \cdot d_A = 1 + k \cdot 72$;; $\boxed{d_A = \frac{1 + k \cdot 72}{7} = \frac{1 + k(7 \cdot 10 + 2)}{7} = 10k + \frac{2k+1}{7} \overset{k=3}{=} 31}$

72 | 7
2 | 10

b) $C_{BA} = 47 \Rightarrow M_{BA} = (C_{BA})^{d_A} \bmod N_A = 47^{31} \bmod 91$

$31 \equiv 11111$;; $47^{31} = (((47^2 \cdot 47)^2 \cdot 47)^2 \cdot 47)^2 \cdot 47 = 5$

25 → 83 → 64 → 5 → 25 → 83 → 64 → 5

c) $k_{sesión} = 5$

$C_{AB} = XTWY$

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

$M = (C - K) \bmod 26$

XTWY → **SORT**

Pregunta 3

1	A
2	B
3	C
4	AA
5	AB
6	BC
7	CA
8	ABC
9	CAB
10	BCA
11	AAC

!!

1 1 2 3 5 7 6 4 3

A A B C AB CA BC AA C

4 5 6 7 8 9 10 11

AA AB BC CA ABC CAB BCA

OJO!! pues AB ya está

(0'4)

Pregunta 4

$193^{891} \bmod 223$

Propiedad fundamental Euler:

Si $\text{mcd}(a,N)=1$;; $a^{\phi(N)} = 1 \bmod N$

- 193 y 223 son primos $\Rightarrow \text{mcd}(193,223)=1$
- 223 es primo $\Rightarrow \phi(223) = 222$

$$N = p_1^{a_1} \cdot p_2^{a_2} \cdots \Rightarrow \phi(N) = \prod_i p_i^{a_i - 1} \cdot (p_i - 1)$$

- $193^{\phi(223)} = 1 \bmod 223$;; $193^{222} \bmod 223 = 1 \bmod 223$
- $193^{k \cdot 222} \bmod 223 = 1^k \bmod 223 = 1 \bmod 223$
- busco el $k \cdot 222$ más cercano (por debajo) al 891: $k=4$

$$4 \cdot 222 = 888 \Rightarrow 4 \cdot 222 + 3 = 891$$

- $193^{891} \bmod 223 = 193^{4 \cdot 222 + 3} \bmod 223 = \left(193^{4 \cdot 222} \cdot 193^3\right) \bmod 223 =$

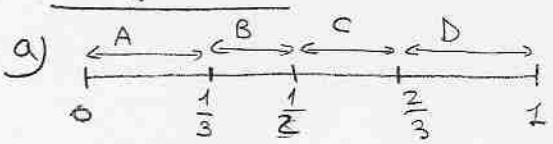
$= \underbrace{193^{4 \cdot 222} \bmod 223}_{1} \cdot 193^3 \bmod 223 = 7189057 \bmod 223 =$

$= \boxed{206}$

7189057 | 223
206 32237

Pregunta 5

a)



$0'63 \rightarrow C$

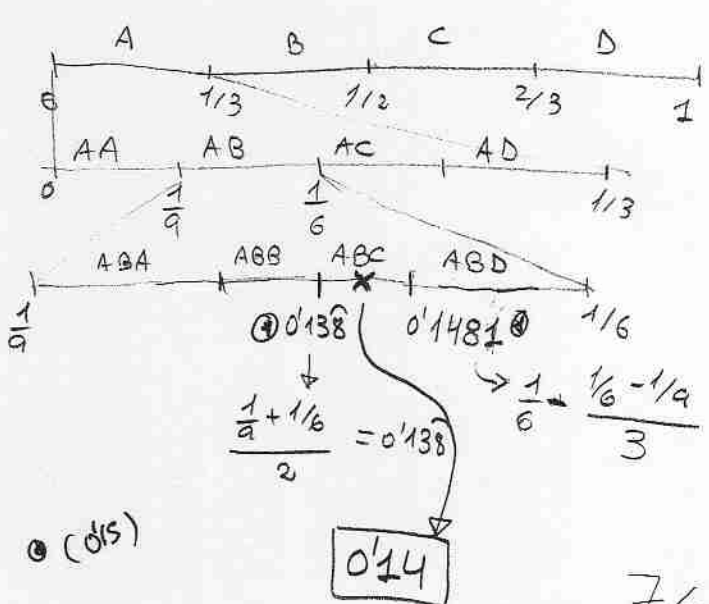
$\frac{0'63 - 0'5}{1/6} = 0'78 \rightarrow D$

$\frac{0'78 - 2/3}{1/3} = 0'34 \rightarrow B$

$\frac{0'34 - 1/3}{1/6} = 0'04 \rightarrow A$

CDBA

b)



7/7