CONTROL DE TRANSMISIÓN DE DATOS. 3 de Diciembre de 2009

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.
4. Las secuencias binarias tienen MPI (Más Peso a la Izquierda).
5. Lista de los 101 primeros números primos: 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

Problema 1 (50%)

Sean A y B dos usuarios de un sistema de **clave pública RSA**. CA es la autoridad certificadora. A y B solicitan a CA sus certificados digitales. **El sistema trabaja en bloques de 4 bits.** Considere **MPI** (Más Peso a la izquierda) en las secuencias.

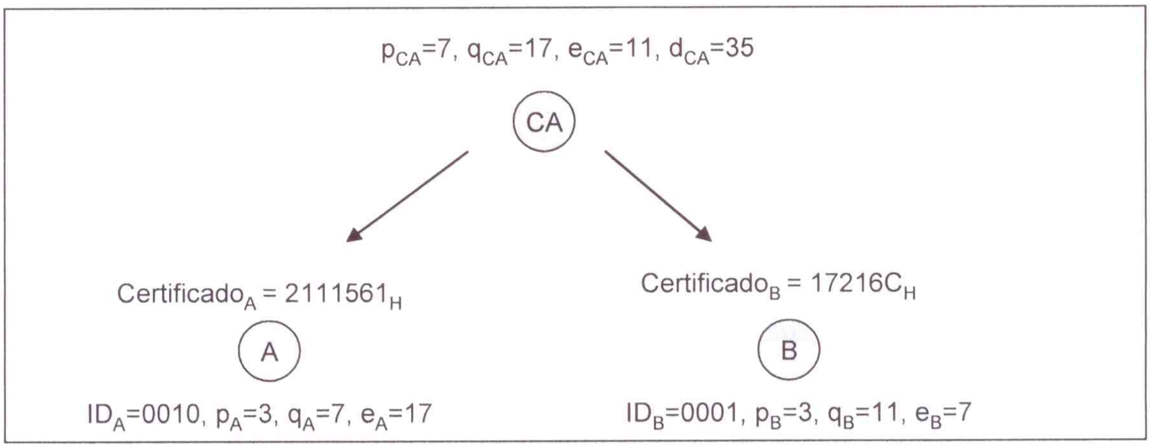


Figura 1. Sistema de clave pública RSA. Certificados Digitales expendidos por CA a A y B.

Para la firma se utiliza la función de *hash* H(M), calculada de la siguiente forma. Considere k=4:

1. Se añade al final del mensaje el número de ceros necesario para que la longitud sea múltiplo de k.
2. Se divide el mensaje resultante en n bloques de k bits, m_i, $0 \leq i \leq n-1$
3. H(M) se calcula iterativamente de la siguiente manera:

$$h_0 = m_0$$
$$h_{i+1} = h_i \oplus m_{i+1} \quad 0 \leq i \leq n-2 \qquad \text{(XOR bit a bit)}$$
$$H(M) = h_{n-1}$$

Los usuarios utilizan RSA para intercambiar una **clave de sesión**, la cual utilizan junto a un algoritmo de **cifrado de flujo** implementado con un **LFSR** para cifrar sus mensajes.

La **clave de sesión** es el **estado inicial** del **LFSR** con polinomio de conexiones $C(D)=1+D+D^4$. **Nota**: El 1er bit generado por el LFSR cifra al bit más significativo del mensaje.

1p a) A y B se intercambian sus certificados. Haga las operaciones que hace B para autenticar la procedencia del certificado de A. ¿La clave pública de A es auténtica?

1p b) B desea comunicar a A la clave de sesión $\mathbf{K_s}$=12. Obtenga qué mensaje envía B a A.

1p c) Calcule qué operación realiza A para acceder a la clave de sesión.

2p d) Obtenga el criptograma que genera B para enviar codificado a A el mensaje M=E5A312F$_H$.

Problema 2 (50%)

Sean X e Y dos variables aleatorias discretas con la siguiente función de distribución (**probabilidades conjuntas**):

Y,X	X_1	X_2	X_3	X_4
Y_1	1/12	1/18	2/27	1/9
Y_2	1/12	2/18	2/27	2/9
Y_3	0	2/18	2/27	0

0.6 a) Calcule la entropía conjunta, H(X, Y).

0.6 b) Calcule la entropía de X, H(X).

0.6 c) Calcule la entropía condicionada, H(Y\X).

0.6 d) Calcule la información mutua, I(X; Y).

0.6 e) Calcule la entropía condicionada, H(X\Y). Comente el resultado comparándolo con c)

0.6 f) Diseñe un código Huffman binario para una fuente que emita los valores asociados a la variable aleatoria X. Calcule la eficiencia de dicho código y comente el resultado.

0.6 g) Codifique aritméticamente la secuencia $X_3X_3X_1$ generada por la fuente X (use 4 decimales siempre).

0.8 h) Compare el número de bits necesario para codificar la secuencia anterior, utilizando el código Huffman binario del apartado f) y utilizando el código aritmético anterior. Utilice el estándar IEEE 754 para codificar números reales en coma flotante. Codifique el número real obtenido.

Nota: Ejemplo de codificación de un número real en coma flotante. Codifiquemos el número decimal -118.625 usando el estándar de la IEEE para aritmética en coma flotante (**IEEE 754**). Necesitamos obtener el **signo** (1bit), el **exponente** (8b) y la **mantisa** (23b).

Dado que es un número negativo, el signo es "1", en caso contrario sería un "0".

Busquemos los demás valores:

Primero, escribimos el número (sin signo) usando notación binaria. El resultado es 1110110.101

$118 \equiv 1110110 \qquad 0.625 \equiv 2^{-1} + 2^{-3}$

Ahora, movamos el punto decimal a la izquierda, dejando sólo un 1 a su izquierda. El exponente indica el número de desplazamientos que hemos hecho.

$1110110.101 = 1.110110101 \cdot 2^6$ Esto es un número en coma flotante normalizado.

La mantisa es la parte a la derecha del punto, rellenada con ceros a la derecha hasta que obtengamos todos los 23 bits. Es decir 11011010100000000000000.

El exponente es 6, pero necesitamos convertirlo a binario y desplazarlo (de forma que el exponente más negativo es 0, y todos los exponentes son solamente números binarios no negativos). Para el formato IEEE 754 de 32 bits, el desplazamiento es 127, así que el exponente es 6+127=133. En binario, esto se escribe como 10000101.

Poniendo todo junto:

```
------------------------------------------------------------------

 1     8                  23               <-- tamaño en bits
+-----------------------------------+
|S|  Exp    |   Mantisa              |
|1|10000101|11011010100000000000000|
+-----------------------------------+
31 30    23 22                     0   <-- índice del bit (0 a la derecha)
   desplazado -127

------------------------------------------------------------------
```

Control 3/12/09. Transmisión de Datos. Prof: Mónica Aguilar

---

① Certificado deigital (A) = $2111561_h = \overbrace{\underbrace{0010}_{ID_A} \,|\, \underbrace{0001\;0001}_{e_A=17} \,|\, \underbrace{0001\;0101}_{N_A=21} \,|\, \cdots}^{M_A}$

a)

$\cdots \underbrace{0110\;0001}_{FD(M_A)\,\equiv\,97}$

$$H(M_A) = FD(M_A)^{e_{CA}} \bmod N_{CA} =$$

$$= 97^{11} \bmod 119 = 6 //$$

Hallamos $H(M_A)$ desde el M_A del certificado:

$h_0 = m_0 = 0010$

$h_1 = h_0 \oplus m_1 = 0010 \oplus 0001 = 0011$

$h_2 = h_1 \oplus m_2 = 0011 \oplus 0001 = 0010$

$h_3 = h_2 \oplus m_3 = 0010 \oplus 0001 = 0011$

$h_4 = h_3 \oplus m_4 = 0011 \oplus 0101 = 0110 = H(M_A) = 6 //$ → El Certificado de A es auténtico, pues lo firmó CA.

b) $K_S = 12$ $\quad C'_{K_S} = K_S^{e_A} \bmod N_A = 12^{17} \bmod 21 = 3$

c) $K_S = C'^{\,d_A}_{K_S} \bmod N_A = 3^{d_A} \bmod N_A$

$e_A \cdot d_A = 1 \bmod \phi(N_A)$

$d_A = e_A^{-1} \bmod \phi(N_A) = e_A^{\phi(\phi(N_A))-1} \bmod \phi(N_A) = 17^{\phi(12)-1} \bmod 12$

↓

$\phi(N_A) = (p_A - 1)\cdot(q_A - 1) =$

$= 2 \cdot 6 = 12$

↓

NOTA: $\phi < \frac{d}{e} < \phi(N)$

$e=17$ en mod 12 !!

No está bien diseñado...

Pero funciona...

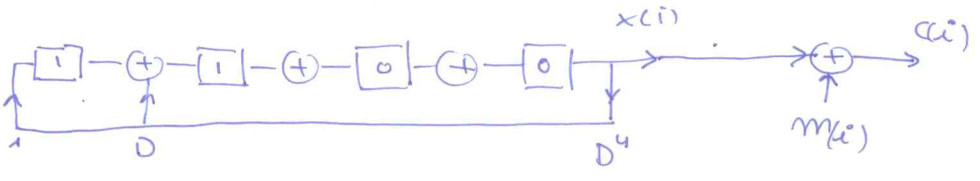
$12 = 2^2 \cdot 3$

$\phi(12) = 2^1 \cdot (2-1) \cdot 3^0 \cdot (3-1) = 4$

$d_A = 17^{4-1} \bmod 12 = 17^3 \bmod 12 = 5$

$k_s = 3^5 \bmod 21 = 12$

d)



Cifrado de Flujo

$K_S = p^{(0)}(D) = 12 \equiv 1100$

$C(D) = 1 + D + D^4$ es primitivo → $L_{max} = 2^m - 1 = 2^4 - 1 = 15$

1	D	D^2	D^3	
1	1	0	0	$= p^{(0)}(D)$
0	1	1	0	$= p^{(1)}(D)$
0	0	1	1	$= p^{(2)}(D)$
1	1	0	1	$= p^{(3)}(D) = D \cdot p^{(2)}(D) \bmod c(D) = D(D^2+D^3) \bmod c(D)$
1	0	1	0	$= p^{(4)}(D)$
0	1	0	1	$= p^{(5)}(D)$
1	1	1	0	$= p^{(6)}(D)$
0	1	1	1	$= p^{(7)}(D)$
1	1	1	1	$= p^{(8)}(D)$
1	0	1	1	$= p^{(9)}(D)$
1	0	0	1	$= p^{(10)}(D)$
1	0	0	0	$= p^{(11)}(D)$
0	1	0	0	
0	0	1	0	
0	0	0	1	$= p^{(14)}(D)$
1	1	0	0	$= p^{(15)}(D) = p^{(0)}(D)$

...

$$\underbrace{\;0\;}_{x(i)}$$

$p^{(4)}(D) \rightarrow$

$$\begin{array}{l|l} D^4+D^2+D & D^4+D+1 \\ D^4+D+1 & 1 \\ \hline D^2+1 & \end{array}$$

$$\begin{array}{l|l} D^4+D^3 & D^4+D+1 \\ D^4+D+1 & 1 \\ \hline D^3+D+1 \equiv 1101 & \end{array}$$

$p^{(6)}(D) \rightarrow$

$$\begin{array}{l|l} D^4+D^2 & D^4+D+1 \\ D^4+D+1 & 1 \\ \hline D^2+D+1 & \end{array}$$

$p^{(8)}(D) \rightarrow$

$$\begin{array}{l|l} D^4+D^3+D^2 & D^4+D+1 \\ D^4+D+1 & 1 \\ \hline D^3+D^2+D+1 & \end{array}$$

$p^{(9)}(D) \rightarrow$

$$\begin{array}{l|l} D^4+D^3+D^2+D & D^4+D+1 \\ D^4+D+1 & 1 \\ \hline D^3+D^2+1 & \end{array}$$

$$\begin{array}{l|l} D+D^3+D^4 & D^4+D+1 \\ D^4+D+1 & 1 \\ \hline D^3+1 & \end{array}$$

$$\begin{array}{l|l} D+D^4 & D^4+D+1 \\ D^4+D+1 & 1 \\ \hline 1 & \end{array}$$

$$\begin{array}{rl} & x(i) = 0011\ 0101\ 1110\ 001|0\ 0110\ 1011\ 1100 \\ \oplus & m(i) = 1110\ 0101\ 1010\ 001|1\ 0001\ 0010\ 1111 \\ \hline & c(i) = 1101\ 0000\ 0100\ 000|1\ 0111\ 1001\ 0011 \end{array}$$

②

a) $$\boxed{H(X,Y)} = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(x_i, y_j)} =$$

$$= 2 \cdot \frac{1}{12} \log_2 12 + 2 \cdot \frac{2}{18} \log_2 \frac{18}{2} + \frac{1}{18} \log_2 18 + 3 \cdot \frac{2}{27} \log_2 \frac{27}{2} +$$

$$+ \frac{1}{9} \log_2 9 + \frac{2}{9} \log_2 \frac{9}{2} = \boxed{3'2024 \text{ bits/símbolo}}$$

b) $p(x_i) = \sum_j p(x_i, y_j) \longrightarrow p(x_1) = \frac{1}{12} + \frac{1}{12} = \frac{1}{6} = 0'1\hat{6}$

$p(x_2) = \frac{1}{18} + \frac{2}{18} + \frac{2}{18} = \frac{5}{18} = 0'2\hat{7}$

$p(x_3) = 3 \cdot \frac{2}{27} = \frac{2}{9} = 0'\hat{2}$

$p(x_4) = \frac{1}{9} + \frac{2}{9} = \frac{1}{3} = 0'\hat{3}$

(Nótese que $\sum_i p(x_i) = 1$.)

$$\boxed{H(X)} = \sum_i p(x_i) \cdot \log_2 \frac{1}{p(x_i)} = \frac{1}{6} \log_2 6 + \frac{5}{18} \log_2 \frac{18}{5} + \frac{2}{9} \log_2 \frac{9}{2} + \frac{1}{3} \log_2 3 =$$

$$= \boxed{1'9547 \text{ bits/símbolo}}$$

c) $p(y_j \backslash x_i) = \frac{p(y_j, x_i)}{p(x_i)} = \frac{p(x_i, y_j)}{p(x_i)}$

Y\X	x1	x2	x3	x4
Y1	1/2	1/5	1/3	1/3
Y2	1/2	2/5	1/3	2/3
Y3	0	2/5	1/3	0

$$H(Y \backslash X) = \sum_i \sum_j p(x_i, y_j) \cdot \log_2 \frac{1}{p(y_j \backslash x_i)} =$$

$$= \frac{1}{12} \cdot \log_2 2 \cdot 2 + \frac{1}{18} \log_2 5 + 2 \cdot \frac{2}{18} \log_2 \frac{5}{2} + \frac{2}{27} \cdot 3 \cdot \log_2 3 + \frac{1}{9} \log_2 3 + \frac{2}{9} \log_2 \frac{3}{2} =$$

$$= 1'2477 \text{ bits/símbolo}$$

$$\boxed{H(Y \backslash X)} = H(X,Y) - H(X) = 3'2024 - 1'9547 = \boxed{1'2477 \text{ bits/símbolo}}$$

d) $I(X;Y) = H(X) - H(X \backslash Y) = H(Y) - H(Y \backslash X)$

$p(y_j) = \sum_i p(x_i, y_j) \longrightarrow p(y_1) = \frac{1}{12} + \frac{1}{18} + \frac{2}{27} + \frac{1}{9} = 0'3241$

$p(y_2) = \frac{1}{12} + \frac{2}{18} + \frac{2}{27} + \frac{2}{9} = 0'4907$

$p(y_3) = \frac{2}{18} + \frac{2}{27} = 0'1852$

(Nótese que $\sum_j p(y_j) = 1$.)

$$H(Y) = 0'3241 \log_2 \frac{1}{0'3241} + 0'4907 \log_2 \frac{1}{0'4907} + 0'1852 \cdot \log_2 \frac{1}{0'1852} =$$

$$= 1'4813 \text{ bits/símbolo}$$

$$\boxed{I(X;Y) = H(Y) - H(Y\backslash X) = 1'4813 - 1'2477 = 0'2336 \ \frac{\text{bits}}{\text{símbolo}}}$$

e) $I(X;Y) = H(X) - H(X\backslash Y) = 0'2336$

$H(X) = 1'9547 \rightarrow \boxed{H(X\backslash Y) = H(X) - I(X;Y) = 1'7211 \ \frac{\text{bits}}{\text{símbolo}}}$

$$\underset{3'2024}{H(X,Y)} = \underset{1'9547}{H(X)} + \underset{1'2477}{H(Y\backslash X)} = \underset{1'4813}{H(Y)} + \underset{1'7211}{H(X\backslash Y)}$$

$H_{MAX}(X) = \log_2 4 = 2$ $\qquad$ $H_{MAX}(Y) = \log_2 3 = 1'5849$

Podemos decir que conocida X queda menos de Y por conocer que lo que queda por conocer de X dada Y conocida.

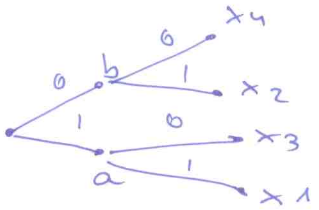
La incertidumbre en X conocida Y es mayor que la incertidumbre en Y conocida X.

f)

	$P(x_i)$	
x_4	0'33	
x_2	0'27	
x_3	0'22	a 0'38
x_1	0'16	

a 0'38
x_4 0'33 } b 0'60
x_2 0'27

b 0'60
a 0'38



Símbolo Fuente	Palabra Código
x_1	11
x_2	01
x_3	10
x_4	00

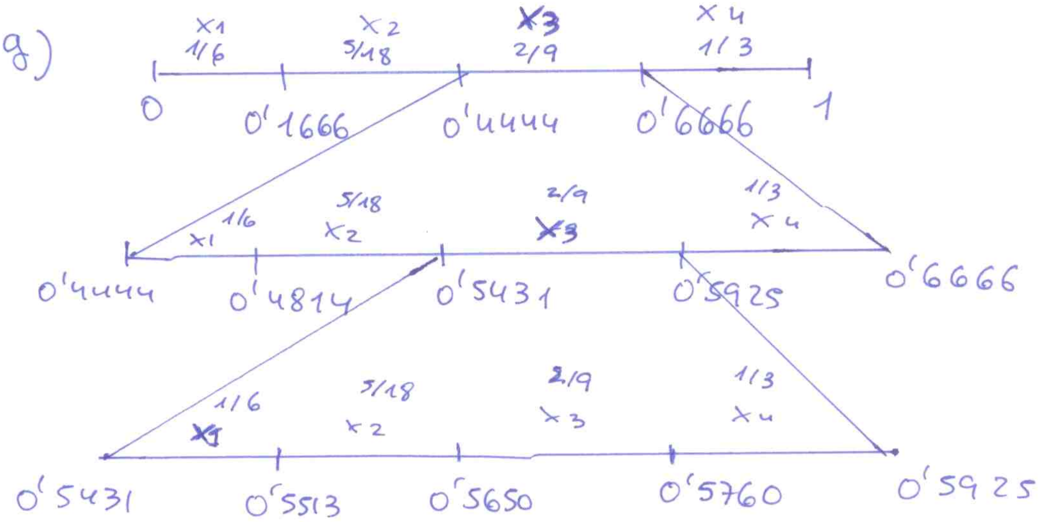
$\bar{L} = 2 \ \frac{\text{bits}}{\text{símbolo}}$

$H(X) = 1'9547$

$$\boxed{E = \frac{H}{\bar{L}} = 0'9773 \rightarrow 97'73\%}$$ muy eficiente

Al tener $p(x_i) \simeq \frac{1}{4}$, sale una codificación de longitud fija 2 bits/símbolo.

g)



Codificación = nº Real ∈ (0'5431 , 0'5513)

Por ejemplo, $x_3\, x_3\, x_1 \longrightarrow \boxed{0'5449}$

h) $x_3 x_3 x_1 \longrightarrow$ 10 10 11 con el código Huffman.

0'5449 → signo = 0 (por ser positivo)

parte entera = 0

parte decimal = $2^{-1} + 2^{-5} + 2^{-7} + 2^{-8} + 2^{-9} = 0'5449$

$$0.\underset{2^{-1}}{1}000\underset{2^{-5}}{1}0\underset{2^{-7}}{1}\underset{2^{-8}}{1}\underset{2^{-9}}{1}$$

exponente

$$1.\underbrace{00010111}_{\text{mantisa}} \cdot 2^{\textcircled{-1}} \longrightarrow -1 + 127 = 126 \equiv 1111110$$

0	01111110	00010111000000000000000
signo (1b)	exponente (8b)	mantisa (23b)

Nota: La longitud de la secuencia, 3, también hay que transmitirla, aunque no se especifica en el enunciado.

Si supongo tengo 1 octeto reservado para ello, enviaría:

0000⋮0011