Mónica Aguilar

CONTROL DE TRANSMISIÓN DE DATOS. 15 de Diciembre de 2005

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.

Problema 1 (35%)

Considere dos monedas: una moneda normal (X_1) y otra moneda falsa con dos caras (X_2). Se realiza el experimento de seleccionar una de las dos monedas y lanzarla dos veces seguidas. Se desea saber **qué información da el resultado respecto de la moneda que se lanzó**. Para ello, siga los siguientes pasos y conteste las preguntas.

0'5 a) Considere que X es la variable aleatoria que indica de qué moneda se trata, $X=\{X_1, X_2\}$. Considere que Y es la variable aleatoria que indica el resultado de los dos lanzamientos, $Y=\{Y_1=CC, Y_2=CX, Y_3=XC, Y_4=XX\}$. Deduzca las **probabilidades condicionadas**:

$P(Y_j \backslash X_i)$	Y_1	Y_2	Y_3	Y_4
X_1				
X_2				

0'5 b) Calcule las **probabilidades conjuntas**:

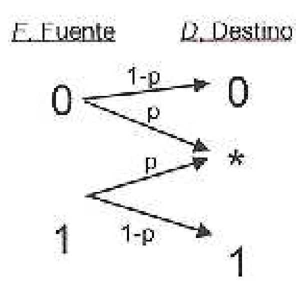
$P(Y_j, X_i)$	Y_1	Y_2	Y_3	Y_4
X_1				
X_2				

0'75 c) Calcule la entropía de Y, H(Y).
0'75 d) Calcule la entropía condicionada, $H(Y \backslash X)$.
0'5 e) Calcule la información mutua, I(X; Y).
0'5 f) Calcule la entropía conjunta, H(X, Y).

Problema 2 (35%)

Considere un **canal discreto binario con borrado** (símbolo *), con el siguiente diagrama de transiciones:

Canal



a) Obtenga la capacidad de canal discreto (en función de p), expresada en bits/símbolo. Justifique todos los pasos seguidos.

Nota: Para mayor comodidad en las operaciones, utilice: $H(p) = p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{(1-p)}$

Problema 3 (30%)

Sea un sistema de clave pública RSA. Considere dos usuarios A y B y una entidad CA que expende certificados para autenticar el origen de los mensajes. Los usuarios del sistema utilizan criptografía asimétrica **RSA** para intercambiar una clave de sesión, utilizada a su vez para **codificar mensajes** mediante la técnica de sustitución monoalfabética monográmica vista en clase (**Cifrado de César**). Las secuencias binarias se consideran con más peso a la izquierda (MPI).

Parámetros RSA de los usuarios y de la entidad certificadora, e identificadores de cada usuario:

Usuario A	$p_A=11$, $q_A=13$, $e_A=7$, $\boldsymbol{d_A}$	$ID_A=1001$
Usuario B	$p_B=7$, $q_B=11$, $e_B=17$, $d_B=53$	$ID_B=0111$
Entidad certificadora CA	$p_{CA}=3$, $q_{CA}=11$, $e_{CA}=7$, $d_{CA}=3$	

La función resumen o *Hash* H(M) de un mensaje M, se obtiene aplicando la operación OR-exclusiva ($\oplus$), 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: $C_i=b_{i1}\oplus b_{i2}\oplus b_{i3}\oplus\ldots\oplus b_{im}$.

La autoridad certificadora CA sigue el siguiente esquema para expender los certificados: Un usuario i entrega a la CA el certificado en claro correspondiente a la concatenación (||) de su identificador ID_i y de su clave pública K_{P_i}. La CA firma digitalmente dicho certificado en claro y añade la firma detrás: *Certificado firmado = certificado en claro || firma digital.*

Los certificados (en hexadecimal) que CA generó a los usuarios A y B son:

- Certificado de A = 978F3
- Certificado de B = 7114D5

0'75 a) Indique qué pasos seguirá el usuario B para autenticar la clave pública de A. Realice los cálculos necesarios.

0'75 b) B desea comunicar una **clave de sesión** a A, $k_{sesión}$ = **4**. Obtenga el criptograma que B envía a A.

0'75 c) Realice la operación que hará A para averiguar la clave de sesión. Obténgala. Realice todos los cálculos necesarios.

0'75 d) A desea enviar a B el mensaje "BON NADAL". **Codifique dicho mensaje.**

(1) $X = \{X_1, X_2\}$ $X_1 \to C,X$ $X_2 \to C,C$ $Y = \{Y_1, Y_2, Y_3, Y_4\}$ Y_1: CC, Y_2: CX, Y_3: XC, Y_4: XX

0'5 a) $P(Y_j \backslash X_i)$

	Y_1	Y_2	Y_3	Y_4
X_1	1/4	1/4	1/4	1/4
X_2	1	0	0	0

Elegir una u otra moneda, es equiprobable

$$\boxed{P(X_1) = P(X_2) = \frac{1}{2}}$$

Teorema Bayes:

0'5 b) $P(X_i, Y_j) = P(Y_j \backslash X_i) \cdot P(X_i)$

$P(Y_j, X_i)$

	Y_1	Y_2	Y_3	Y_4
X_1	1/8	1/8	1/8	1/8
X_2	1/2	0	0	0

(*) $H(X) = \frac{1}{2} \cdot 2 \cdot \log_2 2 = 1$ bit/símbol

0'75 c) $H(Y) = \sum_{j=1}^{m} P(Y_j) \cdot \log_2 \frac{1}{P(Y_j)}$

$P(Y_j) = \sum_{i=1}^{n} P(Y_j \backslash X_i) \cdot P(X_i)$

$P(Y_j) = \sum_{i=1}^{m} p(X_i, Y_j) \Rightarrow \begin{cases} P(Y_1) = \frac{1}{8} + \frac{1}{2} = \frac{5}{8} = P(Y_1 \backslash X_1) \cdot P(X_1) + P(Y_1 \backslash X_2) \cdot P(X_2) \\ P(Y_2) = P(Y_3) = P(Y_4) = \frac{1}{8} \end{cases}$

$$\boxed{H(Y) = \frac{5}{8} \cdot \log_2 \frac{8}{5} + 3 \cdot \frac{1}{8} \cdot \underbrace{\log_2 8}_{3} = 1'55 \text{ bits/símbolo}}$$

0'75 d) $\boxed{H(Y \backslash X)} = \sum_{i=1}^{m} \sum_{j=1}^{m} p(X_i, Y_j) \cdot \log_2 \frac{1}{P(Y_j \backslash X_i)} = H(Y \backslash X_1) \cdot P(X_1) + H(Y \backslash X_2) \cdot P(X_2) =$

ver probab. a)

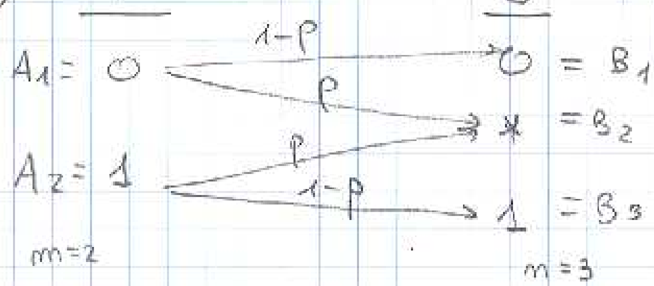
$\begin{cases} H(Y \backslash X_1) = 4 \cdot \frac{1}{4} \cdot \log_2 4 = 2 \\ H(Y \backslash X_2) = 1 \cdot \log_2 1 = \emptyset \end{cases} = 2 \cdot \frac{1}{2} + \emptyset \cdot \frac{1}{2} = \boxed{1 \text{ bit/símbol}}$

0'5 e) $\boxed{I(X;Y)} = \overset{1'55}{H(Y)} - \overset{1}{H(Y \backslash X)} = 0'55$ bit/símbol

0'5 f) $H(Y \backslash X) = H(X,Y) - \overset{(*)}{H(X)} \to \boxed{H(X,Y) = 1 + 1 = 2 \text{ bit/símbol}}$

PROBLEMA 3

(2) 0'5



$$P(D\backslash F) = \begin{array}{c c} & \begin{array}{ccc} \overset{0}{B_1} & \overset{*}{B_2} & \overset{1}{B_3} \end{array} \\ \begin{array}{c} 0 = A_1 \\ 1 = A_2 \end{array} & \begin{pmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{pmatrix} \end{array}$$

$$C = \max_{p\{A_i\}} \left[H(D) - H(D\backslash F) \right]$$

0'5

$$H(D\backslash F) = \sum_{i=1}^{m=2} p(A_i)\cdot H(D\backslash A_i) = p(A=0)\cdot H(D\backslash A=0) + p(A=1)\cdot H(D\backslash A=1) =$$

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

$$= H(p)\cdot \left(\underbrace{p(A=0) + p(A=1)}_{1} \right) = H(p)$$

0'5

$$H(D) = \sum_{j=1}^{n=3} p(B_j)\cdot \log_2 \frac{1}{p(B_j)} \underset{\uparrow}{=} (1-p)\cdot p(A=0)\cdot \log_2 \frac{1}{(1-p)\cdot p(A=0)} + p\cdot \log_2 \frac{1}{p} +$$

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

$$+ (1-p)\cdot p(A=1)\cdot \log_2 \frac{1}{(1-p)\cdot p(A=1)} = (1-p)\cdot p(A=0)\cdot \left\{ \log_2 \frac{1}{1-p} + \log_2 \frac{1}{p(A=0)} \right\}$$

2

$$+ p\cdot \log_2 \frac{1}{p} + (1-p)\cdot p(A=1)\cdot \left\{ \log_2 \frac{1}{1-p} + \log_2 \frac{1}{p(A=1)} \right\} =$$

$$= \underbrace{(1-p)\cdot \log_2 \frac{1}{1-p} + p\cdot \log_2 \frac{1}{p}}_{H(p)} + (1-p)\cdot \underbrace{\left\{ p(A=0)\cdot \log_2 \frac{1}{p(A=0)} + p(A=1)\cdot \log_2 \frac{1}{p(A=1)} \right\}}_{H(X)} =$$

$$= H(p) + (1-p)\cdot H(X)$$

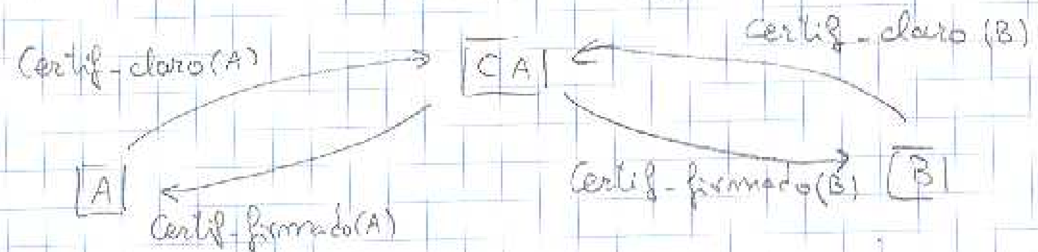
$$C = \max_{p\{A_i\}} \left[\cancel{H(p)} + (1-p)\cdot H(X) - \cancel{H(p)} \right] = \max_{p\{A_i\}} \left[(1-p)\cdot H(X) \right]$$

El máximo será para F equiprobable, $p(A=0) = p(A=1) = 1/2$, donde $H(X) = 2\cdot \frac{1}{2}\cdot \log_2 2 = 1$ bit/símbolo.

$$C = (1-p)\cdot \max_{p\{A_i\}} H(X)$$

$$\boxed{C_{(p)} = (1-p) \text{ bits/símbolo}}$$

Problema 3



Certif_claro(A) = $ID_A \| e_A \| N_A$

Certif_firmado(A) = $\underbrace{ID_A \| e_A \| N_A}_{M_A} \| FD(M_A)$;

$M_A \to H(M_A)$

$FD(M_A) = \left(H(M_A)\right)^{d_{CA}} \bmod N_{CA}$

lo mismo para B.

a) 1.- B tiene el Certif_firmado(A) ya, pues A y B se los han intercambiado previamente.

$$978F3 \equiv \underbrace{\underbrace{1001}_{ID_A}\ \underbrace{0111}_{e_A}\ \underbrace{1000\ 1111}_{N_A}}_{M_A}\ \underbrace{0011}_{FD(M_A)\,\equiv\,3}$$

$N_A = p_A \cdot q_A = 11 \cdot 13 = 143 \equiv 1000\ 1111$, ok.

2.- B extrae K_{PA} del certificado de A: $e_A = 7$, $N_A = 143$

3.- B calcula la $H(M_A)$ descodificando $FD(M_A)$ con K_{PCA}:

$$H(M_A) = \left(FD(M_A)\right)^{e_{CA}} \bmod N_{CA} = 3^7 \bmod 33 =$$

$N_{CA} = p_{CA} \cdot q_{CA} = 3 \cdot 11 = 33$

$$= 2187 \bmod 33 = 9$$

4.- B recalcula $H(M_A)$ a partir de $M_A = 1001|0111|1000|1111$

$$H(M_A) = 1001 \equiv 9$$

5.- Como coinciden, B ha autenticado la K_{PA} $= (e_A, N_A)$ y ya la puede usar.

b) $C_{K_{sesión}} = (K_{sesión})^{e_A} \bmod N_A = 4^7 \bmod 143 = 16384 \bmod 143 =$
$= 82$

$\boxed{\text{Extra}}$:

Problema 1

aplicar probab. de b), $p(x_i, y_j) = p(y_j, x_i)$

g) $H(X,Y) = \sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i, y_j) \cdot \log_2 \frac{1}{p(x_i, y_j)} =$

$= 4 \cdot \frac{1}{8} \cdot \log_2 8 + \frac{1}{2} \cdot \log_2 2 = \frac{3}{2} + \frac{1}{2} = 2$ bit/símbolo

aplicar a), b)

d) $H(Y \setminus X) = \sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i, y_j) \cdot \log_2 \frac{1}{p(y_j \setminus x_i)} =$

$= 4 \cdot \frac{1}{8} \cdot \log_2 4 + \frac{1}{2} \cdot \log_2 1 = \frac{1}{2} \cdot 2 + \emptyset = 1$ bit/símbolo

Problema 3

$(p_A - 1) \cdot (q_A - 1) = 10 \cdot 12 = 120$

c) Necesitamos saber d_A: $e_A \cdot d_A = 1 + k \cdot \Phi(N_A)$;; $7 \cdot d_A = 1 + k \cdot 120$

$d_A = \frac{1 + k \cdot 120}{7} = \frac{1 + k \cdot (17 \cdot 7 + 1)}{7} = 17k + \frac{k+1}{7} \underset{k=6}{=} \boxed{103 = d_A}$

$120 \,|\, 7$ → 1, 17

A ha recibido $C_{K_{sesión}} = 82$ y lo descodifica con su clave secreta, d_A:

$K_{sesión} = 82^{d_A} \bmod N_A = 82^{103} \bmod 143 = \cdots = 4$

$82^{103} = ((((((82)^2 \cdot 82)^2)^2)^2 \cdot 82)^2 \cdot 82)^2 \cdot 82$;; $103 \equiv 1100111$

$82^2 = 6724 \xrightarrow{\bmod 143} 3$

$3 \cdot 82 = 246 \longrightarrow 103$

$103^2 = 10609 \longrightarrow 27$

$27^2 = 729 \longrightarrow 14$

$14^2 = 196 \longrightarrow 53$

$53 \cdot 82 = 4346 \longrightarrow 56$

$56^2 = 3136 \longrightarrow 133$

$133 \cdot 82 = 10906 \longrightarrow 38$

$38^2 = 1444 \longrightarrow 14$

$14 \cdot 82 = 1148 \longrightarrow \boxed{4 = K_{sesión}}$

d) $C_i = (M + K_{sesión}) \bmod 26 = (M + 4) \bmod 26$

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

+4

B O N NADAL

↓ cifrado César

F S R REHEP