Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

CONTROL DE TRANSMISIÓN DE DATOS
22 de mayo de 2008

NOTAS IMPORTANTES:

1.- *No se responderá ninguna pregunta acerca del enunciado o su interpretación. El alumno responderá según su criterio, especificando en sus respuestas las hipótesis que realice.*
2.- *Se valorará la justificación, discusión y claridad de los resultados.*
3.- ***Los resultados no reflejados en la hoja de resultados anexa no serán tenidos en cuenta.***
4.- *Un **error conceptual grave** puede anular todo el problema.*
5.- *Nótese que **los problemas constan de distintas partes que pueden resolverse por separado**. Se recomienda saltar aquellas partes que no sepan resolverse.*

Problema 1 (40%)

Se dispone de dos fuentes binarias de datos (α y β) caracterizadas por las probabilidades:

$$\boldsymbol{Fte_{\alpha}}: p(A) = 0.85$$
$$\boldsymbol{Fte_{\beta}}: p(A|A) = 0.95, p(B|B) = 0.85$$

También se dispone de dos canales binarios (*a* y *b*) caracterizados por las probabilidades:

$$\boldsymbol{Can_{a}}: p(0) = 0.85 \text{ (probabilidad de NO error)}$$
$$\boldsymbol{Can_{b}}: p(0|0) = 0.95, p(1|1) = 0.85$$

Se pide:

a) El valor de las entropías de ambas fuentes ($\boldsymbol{H_{\alpha}}$, $\boldsymbol{H_{\beta}}$) **(3 puntos)**
b) El valor de las capacidades de ambos canales($\boldsymbol{C_{a}}$, $\boldsymbol{C_{b}}$) **(4 puntos)**
c) Justifique qué emparejamiento de fuentes-canales realizaría **(3 puntos)**

Problema 2 (20%)

Un usuario RSA tiene por exponente público *e*=3 y por módulo *n*= 110107021. Sabiendo que $42518^2 \equiv 12497^2 \; mod \; n$ encuentre el exponente privado *d* del usuario.

Problema 3 (10%)

Un criptógrafo pretende diseñar un cifrador bloque de 8 bits. ¿Cuál es el tamaño mínimo de clave para que el cifrador pueda ser perfectamente aleatorio?

Nota.- Úsese la fórmula de Stirling para el factorial: $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

SIGUE DETRÁS

Problema 4 (30%)

Sabiendo que, según el *Teorema Chino de los Restos*, el sistema de congruencias:

$$\begin{cases} x_1 = X \bmod n_1 \\ x_2 = X \bmod n_2 \\ x_3 = X \bmod n_3 \end{cases}$$

tiene por solución:

$$X = (x_1 I_{2,3}^1 n_2 n_3 + x_2 I_{1,3}^2 n_1 n_3 + x_3 I_{1,2}^3 n_1 n_2) \bmod (n_1 n_2 n_3)$$

si los números n_1, n_2 y n_3 son primos dos a dos.

Se pide:

a) Encuentre de forma razonada cómo deben calcularse los valores $I_{2,3}^1, I_{1,3}^2, I_{1,2}^3$ **(4 puntos)**

Si se envía el mismo mensaje M en secreto a tres usuarios RSA que comparten el mismo exponente público $e=3$ y con módulos n_1=4033, n_2=4223, n_3=4343, se obtienen los criptogramas c_1=1022, c_2=1678, c_3=1341

b) Encuentre el valor concreto de $I_{1,2}^3$ **(3 puntos)**

c) Sabiendo que $I_{2,3}^1 = 3191, I_{1,3}^2 = 1609$ Sabiendo encuentre el valor de M usando el *Teorema Chino de los Restos* **(3 puntos)**