Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

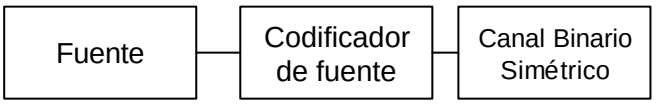
CONTROL DE TRANSMISIÓN DE DATOS
21 de mayo de 2004

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 (50%)

El emisor de un sistema de transmisión de datos está formado por los siguientes módulos:



La **fuente** emite cuatro símbolos independientes con probabilidades 0.7, 0.1, 0.1 y 0.1.
La salida del **codificador de fuente** es binaria.

Se pide:

a) El valor H_F de la entropía de la fuente **(1 punto)**

Si el codificador de fuente realiza la codificación:

A:00, B:01, C:10, D:11

a la salida del canal se tiene un 71% de ceros.

b) ¿Cuál es la capacidad del canal? **(4 puntos)**

Si el codificador de fuente realiza una codificación de Huffman:

c) ¿Cuál es el valor de la entropía a la entrada del canal? **(1 puntos)**
d) Estime la entropía que se observaría a la salida del canal considerada como una fuente binaria sin memoria **(4 puntos)**

SIGUE DETRÁS

Problema 2 (50%)

Supóngase que se dispone de un procesador criptográfico capaz de realizar una multiplicación módulo N en n^2 operaciones máquina, donde $n = \left\lceil \frac{\log_2 N}{32} \right\rceil$

Se pide:

a) Estime el número medio de operaciones máquina necesarias para realizar la operación:

$$A^{e_N} \bmod N, \quad 0 \le A, e_N < N$$

donde e_N tiene una longitud de L_{e_N} bits y N tiene una longitud de L_N. Suponga que se emplea el método del campesino ruso **(1.5 puntos)**

Sea $N = pq$ donde tanto p como q son números primos distintos con el mismo número de bits.

b) Estime el número medio de operaciones máquina necesarias para realizar la operación:

$$A_p^{\ e_p} \bmod p, \quad 0 \le A_p, e_p < p$$

donde $A_p = A \bmod p, \quad e_p = e_N \bmod (p-1)$ **(1 punto)**

Sean

$$\begin{cases} S_p = A_p^{\ e_p} \bmod p \\ S_q = A_q^{\ e_q} \bmod q \end{cases}$$

entonces, por el teorema chino del resto, se tiene que:

$$S = A^{e_N} \bmod N = (S_p I_q^{\ -1} q + S_q I_p^{\ -1} p) \bmod (pq)$$

c) Encuentre, de forma razonada, el valor de $I_q^{\ -1}$ y de $I_p^{\ -1}$ **(2 puntos)**

d) Suponiendo despreciables cualquier operación que no sea una exponenciación modular, estime el número de operaciones máquina necesarias para realizar la exponenciación modular por medio del teorema chino del resto **(1.5 puntos)**

e) Esta mejora de eficiencia ¿puede usarse en el cifrado RSA?¿y en el descifrado? Razone ambas respuestas **(1 puntos)**

Supóngase que, durante un descifrado RSA de parámetros $\{e, d, N = pq\}$, en el cálculo de S_p se produce un error de computación obteniéndose un valor $\hat{S}_p$, pero que el cálculo de S_q se realiza correctamente. Es tal caso, al combinar S_p y S_q se obtiene un $\hat{S}$ erróneo que satisfará que:

$$\begin{cases} \left(\hat{S}\right)^e \neq A \bmod p \\ \left(\hat{S}\right)^e = A \bmod q \end{cases}$$

f) Razone como obtener la factorización de N una vez conocidos A y $\hat{S}$ **(2 puntos)**

g) En este principio se basa el ataque a dispositivos "tamper-proof" conocido como *criptoanálisis diferencial de fallos*. Explique como procedería para encontrar la clave secreta RSA almacenada en una tarjeta inteligente que utilizara el teorema chino del resto para el descifrado **(1 punto)**