EXAMEN DE TRANSMISIÓN DE DATOS *23 de mayo de 2007*

Problema 1 (2 puntos)

Un canal está caracterizado por la siguiente matriz de probabilidades de transición:

$$X \begin{bmatrix} & & & Y & & & \\ 0 & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 \\ 1/6 & 1/3 & 1/3 & 1/6 & 0 & 0 & 0 \end{bmatrix}$$

1) Calcula la Capacidad de Canal

Problema 2 (8 puntos)

Hace unos meses Aldous terminó la valoración confidencial de un proyecto docente. Para notificar su resultado a Simón utilizó el último mecanismo de seguridad por e-mail que tenían acordado, el cual es como sigue:

A) Permutar el mensaje con la matriz (6 4 2 1 3 5 12 10 8 7 9 11…) y luego codificarlo con un compresor ARI de extensión variable. Para ello se fija un intervalo mínimo de compresión, igual a 0.0000024, y se aumenta un orden si el intervalo a codificar es superior o igual a este valor. Una vez encontrada la extensión, elegir un número de ese intervalo con la precisión mínima necesaria y enviarlo sin el 0 ni el punto.

C) Tal como sucede en PGP enviar el mensaje, encriptado con un algoritmo simétrico, y concatenar la clave de sesión de ese algoritmo, encriptada de forma asimétrica. En este caso el cifrado síncrono simétrico realiza la suma módulo 10 dígito a dígito de la salida del compresor con una secuencia pseudo-aleatoria S_3 de dígitos decimales. La clave de sesión x_{30} es el número necesario para la inicialización del generador S_3 y se envía cifrado con un RSA. Para generar S_3 mezclan 2 secuencias S_1 y S_2, de forma que un valor x_{3n} de S_3 mod p pertenece a S_1 y mod q pertenece a S_2. El valor n-ésimo de x_{1n} de S_1 es $a_1 \cdot x_{1n-1}$ mod p y el de S_2 es $a_2 \cdot x_{2n-1}$ mod q, con n=1, p y q primos, a_1 y a_2 raíces primitivas en $\boldsymbol{Z}p$ y $\boldsymbol{Z}q$ respectivamente. La secuencia S_3 es la concatenación de todos los x_3 generados.

1) **(0.5 puntos)** ¿Cuál es el periodo de S_1 y S_2?
2) **(0.5 puntos)** ¿Cuál es el número de inicializaciones posibles para generar S_3?
3) **(1 punto)** ¿Cuál es el periodo de S_3?, ¿es el máximo posible? , ¿el número 1 está en S_3?

Si se ha recibido el criptograma **3897 21352824628** (clave de sesión cifrada | | mensaje cifrado)**:**

4) **(2 puntos)** Encuentra la clave de sesión x_{30}
5) **(0,25 puntos)** ¿Cuál es la extensión mínima y máxima que permite el compresor?
6) **(1.5 puntos)** Calcula el mensaje en claro sin descomprimir
7) **(2 puntos)** Encuentra el mensaje descomprimido
8) **(0,25 puntos)** Encuentra el mensaje enviado

DATOS: En el compresor ARI los símbolos están ordenados alfabéticamente:

x_i	$p(x_i)$	$F(x_i)$
A	1/13	1/13=0.07692…
B	1/182	15/182=0.082…
C	1/182	8/91=0.08791…
D	1/182	17/182=0.093…
E	1/13	31/182=0.170…
F	1/182	16/91=0.1758…
G	1/182	33/182=0.181...
H	1/182	17/91=0.1868…

I	1/13	24/91=0.2637…
J	1/182	7/26=0.26923…
K	1/182	25/91=0.2747…
L	1/182	51/182=0.280…
M	1/182	2/7=0.285714…
N	1/182	53/182=0.291...
O	1/13	67/182=0.368…
P	1/182	34/91=0.3736…
Q	1/182	69/182=0.379…

R	1/182	5/13=0.3846…
S	1/13	6/13=0.4615…
T	1/13	7/13=0.5384…
U	1/13	8/13=0,6153…
V	1/13	9/13=0.6923…
W	1/13	10/13=0.769…
X	1/13	11/13=0.846…
Y	1/13	12/13=0.923…
Z	1/13	1

RSA: e=9301963, p=4591 y q=6229, n=pq, ?(n)=mcm(p-1,q-1)=1588140
S_1 y S_2: p=4591 y q=6229, a_1=4136 y a_2=3787
Las secuencias de salida del compresor y del generador siempre comienzan por el dígito de mayor peso
Para el apartado 7) utilizar el mensaje **46945026419** si no se encontró el del apartado 6)