EXAMEN DE TRANSMISIÓN DE DATOS 9 de diciembre de 2003

Problema (10 puntos)

En su línea habitual de seguridad, Aldous y Simon deciden actualizar de nuevo sus sistemas de compresión y cifrado. En esta ocasión utilizan la idea de El Gamal para cifrar el módulo del RSA con el que transmitirán el mensaje. Es decir, Aldous publicará el par (e,n) donde e será la clave de cifrado RSA y n el módulo utilizado por el método de El Gamal modificado. Para ello comparten como secreto el conjunto de primos $P=\{239, 241, 263, 307\}$. El mecanismo es como sigue:

- Aldous elige 2 números aleatorios, x_1 y x_2
- Calcula dos valores, g y k, tales que cumplen que el $mcd(x_1,x_2)=g*x_1+k*x_2$
- Calcula kmod t como k_2
- Al igual que El Gamal calcula los números a y b pero con g y k_2. Para ello utiliza como clave secreta un valor p de *P* y como mensaje a cifrar otro valor q de *P*. El módulo del RSA será p*q
- Simon al recibir a y b descifra utilizando como clave secreta un valor i de *P*. Si el resultado es otro valor de *P* obtiene los factores del módulo del RSA, en otro caso prueba otro i

Dado que Aldous publica e=41 y $n=2^3*5^2=200$, responded a las siguientes cuestiones

1) Si t=80 demostrar que el valor de a es el mismo utilizando k en lugar de k_2 (**1 punto**)
2) Encontrar g y k para $x_1=1342813$ y $x_2=8451823$ (**1 punto**)
3) Calcular a y b si p=241 y q=307 (**1 punto**)
4) Demostrar que dado un a no puede existir 2 b iguales con diferente q de *P* (**1 punto**)
5) ¿Qué clave de descifrado encuentra Simon? (**1 punto**)

Para un buen mecanismo de cifrado es conveniente realizar antes una compresión de fuente para eliminar toda la redundancia posible del mensaje. Para ello realizan los siguientes pasos:

- Se codifica el alfabeto con símbolos ternarios, tal que indica la posición en el alfabeto. Por ejemplo para la K se considerará el 102 (posición 11 de la tabla)
- Se utiliza un algoritmo LZ78 para el texto a transmitir, con índices ternarios
- Por último se realiza un segundo algoritmo de compresión, en este caso SFE, teniendo en cuenta una extensión de orden 3 de los dígitos ternarios de entrada

La estadística de los símbolos ternarios (sin memoria) se puede consultar en la tabla adjunta. Simon recibe como respuesta a su mensaje "¿de quién es el trabajo?", después de haber descifrado y de realizar la descompresión SFE, la secuencia S=00102100111020022011121022002110021010110220210120 2 (el primero es el de la izquierda). Debéis encontrar:

6) La secuencia después del paso de descompresión LZ78 y el mensaje recibido (**1,5 puntos**)
7) Da una posible codificación binaria de SFE de 112 e indica el intervalo codificado (**1 punto**)
8) Realiza una codificación ternaria de SFE de 112 y da el nuevo intervalo codificado (**1,5 puntos**)
9) A partir de la condición que cumple la longitud de las palabras código en una codificación D-aria de SFE para garantizar que sea instantáneo, relaciona la longitud media L con la entropía D-aria de S, $H_D(S)$, para una codificación D-aria de SFE con longitud media L_n de una extensión n de la fuente, S^n (**1 punto**)

0	NULL
1	A
2	B
3	C
4	D
5	E
6	F
7	G
8	H

9	I
10	J
11	K
12	L
13	M
14	N
15	Ñ
16	O
17	P

18	Q
19	R
20	S
21	T
22	U
23	V
24	X
25	Y
26	Z

x_i	$P(x_i)$
0	0,25
1	0,44
2	0,31