EXAMEN DE TRANSMISIÓN DE DATOS 6 de mayo de 2009

Problema 1 (10 puntos)

Simon ha recibido la respuesta de su colega Aldous para continuar la propuesta de una asignatura con cierta controversia. Para ello han consensuado las siguientes pautas con el objetivo de conseguir confidencialidad:

a) Se encuentra una clave K_P de 6 letras a partir de una fuente de generación de claves. En particular se generan dos dígitos decimales por cada letra. Los de mayor peso se generan según la cadena de Markov de la Figura 1. Los de menor peso se eligen al azar y dependen de lo que salió en el de mayor peso. Si salió un 2 se eligen entre los números 0..4 y, en otro caso, entre los números 0..9. Ambos dígitos indexan una letra del alfabeto indicado en la Tabla 1
b) El mensaje a enviar se cifra según PlayFair en modo CBC con K_P. El digrama de inicio acordado es *N M*
c) Se divide K_P en 2 partes iguales, K_L y K_R, y se comprime cada una con el algoritmo de SFE binario (símbolos ordenados alfabéticamente)
d) Se toma la magnitud de las palabras código como un número entero, K_{LI} y K_{RI} respectivamente, y se genera un único número a enviar, K_{RSA}, cumpliendo que $K_{RSA} \equiv_p K_{LI}$ y $K_{RSA} \equiv_q K_{RI}$ ($p=32887$, $q=33409$)
e) Se cifra con un RSA donde $n=p*q=1098721783$, $e=420941$ y la clave privada se calcula *mod ?(n)*. Si el resultado es 1 se repite el proceso (se calcula una nueva K_P)
f) Se envía el criptograma, que en este caso ha sido (clave||mensaje): *408826838 || X T T K Y U D T* (el primer digrama cifrado está en la izquierda, es el mas antiguo y por tanto el primero en descifrarse)

Responde a las siguientes cuestiones:

1) **(0.5 puntos)** ¿Es acertado utilizar el *mod ?(n)* en el RSA en lugar del *mod f(n)*? Razona la respuesta
2) **(1.5 puntos)** Encuentra K_{LI}, K_{RI} y K_{RSA}
3) **(1.5 puntos)** Dado que $\forall K$ se cumple que $K^{mcm(jp-1)} \equiv_p 1$ con p primo y j cualquiera, encuentra el número de K distintas dado un j concreto que cumplen $K^j \equiv_p 1$. ¿Cuál es la probabilidad de repetir el proceso para crear K_P?
4) **(0.5 puntos)** ¿Tiene memoria la generación del dígito de mayor peso?
5) **(0.75 puntos)** Calcula la distribución *q(x)* de probabilidades del alfabeto a considerar y la entropía de la fuente
6) **(0.75 puntos)** Calcula la longitud mínima de K_P para que sea equivalente a una clave de más de 55 bits, ¿cómo afecta a los valores de p y q?
7) **(1 punto)** Encuentra K_L, K_R y K_P
8) **(1.5 puntos)** ¿Mejora la eficiencia codificando con Huffmann esta misma extensión de fuente? Si la fuente realmente emite símbolos con la distribución *p(x)* de la Tabla 2 y se codifica según *q(x)*, ¿en cuántos bits por símbolo se ha distanciado la longitud media de codificación conseguida con respecto la entropía real?
9) **(0.5 puntos)** Da una razón por la que Aldous y Simon han escogido el modo CBC
10) **(1.5 puntos)** Descifra el mensaje

DATOS:
$\varphi(n)=1098655488=2^8 \cdot 3^6 \cdot 7 \cdot 29^2$
$\lambda(n)=2104704=2^7 \cdot 3^4 \cdot 7 \cdot 29$
Utiliza K_P=*CHANCE* en el caso de no haberla encontrado en el apartado 7) y el mensaje cifrado *V T U Q X I H E*

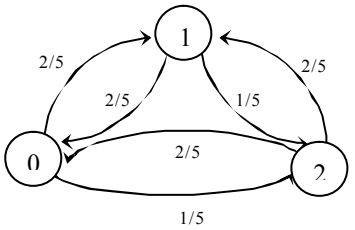

Figura 1

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
A	B	C	D	E	F	G	H	I	J	K	L	M	N/Ñ	O	P	Q	R	S	T	U	V/W	X	Y	Z

Tabla 1

x	A	B	C	D	E	F	G	H	I	J	K	L	M	N/Ñ	O	P	Q	R	S	T	U	V/W	X	Y	Z
25*p(x)	2	1	1	1	2	0.5	1	0.5	2	0.5	0.5	1	1	1	2	1	0.5	1	1	1	1	1	0.5	0.5	0.5

Tabla 2