EXAMEN DE TRANSMIISIÓN DE DATOS 22 de mayo de 2008

Problema 1 (2 puntos)

Se ha construido una fuente de bits $\mathfrak{X}$ a partir de un dodecaedro tal que en 6 de sus caras aparece escrito el 00, en 3 el 11, en 2 el 01 y en una el 10 (se transmite en primer lugar el MSB). Calcula:

1) **(1 punto)** $H(X_{LSB})$, $H(X_{MSB})$ y $H(X)$
2) **(1 punto)** ¿Cómo cambiarías las etiquetas de las caras del dado (manteniendo que 6 son iguales, etc.) para minimizar el número de bits emitidos?, ¿ha mejorado la $H(X)$?

Problema 2 (8 puntos)

Aldous no confía en la transmisión telemática de un mensaje S_1 para Simon. Por ello decide enviarlo a través de emisarios cada uno con una información parcial calculada a partir de S_1: $U_j = S_1 \bmod p_j$. Asimismo ha modelado la fidelidad de cualquier emisario con una probabilidad igual a 0.7.

1) **(1 punto)** ¿Cuál es el valor mínimo y máximo de S_1 para que únicamente sea posible encontrarlo con 3 o más de 3 informaciones parciales?, ¿con qué probabilidad ocurre?
2) **(0.5 puntos)** Calcula el mensaje S_{12} enviado cuando Simon recibe U_1 y U_2
3) **(1punto)** Encuentra $S_{12\text{-}3}$ a partir de S_{12} y U_3, ¿es el S_1 enviado?

S_1 es el último de varios mensajes recibidos por Simon. Concatenados (S_2=933080 || 15400 || 20120 || S_1) son en realidad un sobre digital donde los 6 dígitos de menor peso identifican a la clave del cifrador simétrico del resto de dígitos de S_2. Aldous ha cifrado esta clave con un doble RSA de parámetros e_1=510047, e_2=969091=31*43*727 y n_1=1009*1013=1022117 que junto a los U_j son los únicos valores públicos del algoritmo. Una vez Simon la descifra encuentra K, diferente de 0, y calcula $K^i \bmod n_2$, $K^{2i} \bmod n_2$,… para indexar una memoria de n_2=999983 registros con texto aleatorio. La concatenación de estos textos (más antiguo en la izquierda) conforma la clave de Vigenère para descifrar el mensaje del resto de dígitos de S_2 aún no considerados, dado que éstos indican por pares las posiciones de las letras del alfabeto (debe añadirse un cero en la izquierda si es necesario) tal como sigue:

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

Responde a las siguientes cuestiones:

4) **(0.5 puntos)** ¿Es más robusto el doble RSA que el RSA convencional? Razona la respuesta
5) **(1 punto)** Encuentra la clave K del algoritmo simétrico
6) **(1.25 puntos)** Si el orden de $K \bmod n_2$ es r, encuentra una expresión para calcular el orden de $K^i \bmod n_2$ función del $mcd(i,r)$, ¿qué relación tienen con la función phi?
7) **(1.25 puntos)** ¿Qué condición debe cumplir K para que sus sucesivas potencias indexen el máximo número de registros de la memoria?, ¿K^i cumple esa condición si K la cumple?, ¿cuántas K diferentes cumplen esa condición (utiliza el resultado del apartado 6)?
8) **(0.75 puntos)** Si los registros pueden tener hasta 4 letras, ¿cuál es el tamaño equivalente en bits del número de claves diferentes del cifrado de Vigenère que pueden utilizar Aldous y Simon?
9) **(0.75 puntos)** Descifra el mensaje cuando el valor de i es 3

DATOS:
Todos los valores se presentan factorizados, en otro caso son primos
(U_1=3, p_1=99=3*3*11), (U_2=5, p_2=100=2*2*5*5), (U_3=47, p_3=103), (U_4=80, p_4=107), (U_5=75, p_5=109)
$j(n_1)$=1020096=2^6*3^2*7*11*23, $l(n_1)$=255024=2^4*3^2*7*11*23
$j(n_2)$=999982=2*79*6329
Utiliza S_1=41279 en el caso de no haberlo encontrado en el apartado 3)
Memoria: el #registro mod 23 tiene la misma codificación que el alfabeto salvo los siguientes

#11144=2^3·7·199	TGE	#168338=2·73·1153	MQ	#395791=11^2·3271	Z	#686531=739·929	QBH
#28034=2·107·131	LSCA	#229810=2·5·7^3·67	CJK	#457954=2·7^2·4673	UNFJ	#690429=3·230143	L
#97336=2^3·23^3	LG	#307941=3·102647	RCSY	#523036=2^2·229·571	UK	#826605=3^4·5·13·157	HG
#100005=3·5·59·113	X	#308003	QW	#604738=2·83·3643	MJFY	#874305=3^2·5·19429	CVJX
#168336=2^4·3^2·7·167	HI	#343000=2^3·5^3·7^3	DTR	#609579=3^3·107·211	SDWI	#981374=2·541·907	KJDC