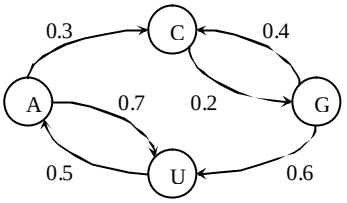
EXAMEN DE TRANSMSIÓN DE DATOS *5 de diciembre de 2006*

Problema (10 puntos)

Aldous necesita transmitir de forma secreta a Simon un fragmento de una secuencia genética (alfabeto de 4 símbolos, *A*, *C*, *G* y *U*). Para despistar a los curiosos primero realiza un cifrado de Vigenère (con idéntico alfabeto *A*, *C*, *G* y *U*) utilizando la siguiente cadena de Markov para generar la clave:



1) **(0,5 puntos)** Razona si modela una fuente con memoria
2) **(1,5 puntos)** Calcula la entropía para esta generación particular de claves
3) **(1 punto)** Si se utiliza *GUAC* como clave para la secuencia *S=GGAGGCGGGGGU*, ¿cuál es el criptograma resultante?

Ahora realiza una codificación de SFE junto a un cifrado de las probabilidades de los símbolos. Para ello primero genera 4 números aleatorios (iguales a *33*, *22*, *13* y *75*) en $\mathbf{Z}n_1$, $\mathbf{Z}n_2$, $\mathbf{Z}n_3$ y $\mathbf{Z}n_4$. A partir de estos números encuentra una clave K_s de sesión tal que $K_s mod n_1=33$, $K_s mod n_2=22$, $K_s mod n_3=13$ y $K_s mod n_4=75$. Los valores $n_1=p_1q_1=2\cdot31$, $n_2=p_2q_2=3\cdot29$, $n_3=p_3q_3=5\cdot17$, $n_4=p_4q_4=7\cdot13$ son públicos, y los p_i, q_i son secretos.

4) **(1,5 puntos)** ¿Cuál es la clave K_s de sesión?
5) **(1,5 puntos)** Si esta clave de sesión se envía cifrada con un RSA de parámetros ($e=1693$, $n=n_1n_2$), ¿cuál es el criptograma?, ¿y la clave secreta d?
6) **(0,25 puntos)** Si en lugar de utilizar n_2 se publicase $n_2=143\ (11\cdot13)$, demuestra que sería muy fácil factorizar dos de los cuatro n_i

Para realizar el cifrado de la secuencia, Aldous calcula $p_{si1} = K_t mod n_i / (K_t mod n_1 + K_t mod n_2 + K_t mod n_3 + K_t mod n_4)$ con $K_t=K_s mod n$ como la probabilidad del símbolo s_i del primer paso del algoritmo aritmético, p_{si2} igual que p_{si1} pero con $K=d\cdot K_s mod n$ con d y n los valores utilizados en el RSA, y más generalmente el paso t con:

$p_{si1} = K_t mod n_i / ? K_t mod n_i$ para todo i con $s_i ? \{s_1=A, s_2=C, s_3=G, s_4=U\}$ y $n_i ? \{n_1, n_2, n_3, n_4\}$
$K_t=d^{(t-1)}\cdot K_s\ mod n$

7) **(0,5 puntos)** ¿Cuál es el número posible de claves?
8) **(0,75 puntos)** ¿d^t pertenece al *CRRn*?, ¿a cuántos valores diferentes puede dar lugar?
9) **(0,5 puntos)** ¿Qué restricción impondrías a K_s y d para que la secuencia $K_s, d\cdot K_s, \ldots, d^{(t-1)}\cdot K_s$ en $\mathbf{Z}n$ esté compuesta por números distintos diferentes de *0*?
10) **(0,5 puntos)** Calcula las probabilidades de los tres primeros pasos del algoritmo de compresión
11) **(1,5 puntos)** Tomando la *A* como el *0* en base 4, la *C* como el *1*, la *G* como el *2* y la *U* como el *3*, encuentra la codificación cuaternaria según SFE para los tres primeros símbolos de la secuencia *S* (extensión de orden 3) dado que el orden importa y es *ACGU*

DATOS:

La inversa de *672945 mod 62* es *-21*
La inversa de *479570 mod 87* es *-10*
La inversa de *490854 mod 85* es *4*