EXAMEN DE TRANSMISIÓN DE DATOS 11 de mayo de 2006

Problema (10 puntos)

Aldous tiene preparado el próximo examen final de Transmisión de Datos y decide enviar secretamente las respuestas a Simon. En esta ocasión han decidido realizar lo siguiente:

1) Codificar el mensaje de fuente m_F con un código de Huffman ternario y la salida volverla a comprimir pero ahora con un LZ77. Tanto las probabilidades de los símbolos de fuente como la configuración del LZ77 son secretos. La secuencia secreta generada por ambas codificaciones es *545240823*
2) Para cada 3 cifras (m_i) de la secuencia generada encontrar el criptograma c_i como $((a*m_i+b) mod n_1)^e mod n_2$, donde a,b y n_1 son secretos y e es primo con $phi(n_2)$
3) Una vez pasado el c_i a binario, enviar los bits por un canal discreto sin memoria

El cifrado combinado que utilizan consiste en uno simétrico denominado sustitución afín, y otro asimétrico, en este caso un RSA. Para este cifrado afín:

1) **(1 punto)** Demuestra que para que 2 mensajes distintos $mod n_1$ tengan siempre un criptograma distinto debe cumplirse que el $mcd(a,n_1)=1$
2) **(0,5 puntos)** Da el número posibles de claves para $n_1=59*97$
3) **(0,25 puntos)** Encuentra c_A como el cifrado afín de $m_1=545$ si $a=55$ y $b=4460$

Para la segunda parte del cifrado han elegido los parámetros $(e=328517, n_2=n_1*59)$.

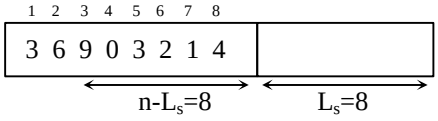
4) **(1 punto)** Demuestra que si t^l es un factor de n_2 y es primo con (n_2/t^l) entonces se cumple que $t^{l+phi(n_2)} \equiv t^l \pmod{n_2}$
5) **(0,75 puntos)** Encuentra c_1 utilizando la expresión anterior
6) **(0,75 puntos)** Demuestra que si c_A es congruente con 0 módulo algún factor t^l de n_2 (t^l primo con n_2/t^l) entonces el criptograma c_1 es congruente con 0 módulo ese mismo factor de n_2. Intenta encontrar ese factor a partir únicamente del c_1 enviado y n_2

Un bit cualquiera de c_1 enviado por el canal se pierde con probabilidad $1-a$, y se entrega al receptor de forma correcta con probabilidad a. En este caso:

7) **(1,5 puntos)** Calcula la Capacidad del Canal en función de a y da una explicación intuitiva del resultado

Asumiendo que se han recibido todos los bits de forma correcta:

8) **(1 punto)** Calcula la clave secreta d del RSA (inversa de e mod $phi(n_2)$) y demuestra que a partir del c_1 enviado se recupera c_A
9) **(0,75 puntos)** Encuentra m_1 a partir de c_A
10) **(1 punto)** Calcula la secuencia descomprimida a partir de *545240823*, resultado de la compresión LZ77 en la que los índices, al igual que las longitudes y los símbolos de fuente, están representados por 1 único dígito decimal. El buffer utilizado en la codificación está inicializado como sigue:



11) **(1,5 puntos)** Si el mensaje de fuente m_F es *DBABCCABCCBBABBBBBBD* especifica la codificación de Huffman utilizada por símbolo de fuente así como la eficiencia conseguida por este código. Para ello considera que cada dígito decimal son 2 símbolos ternarios y que las probabilidades (no verdaderas pero secretas) de los símbolos de fuente son: P(A)=0,31; P(B)=0,29; P(C)=0,19; P(D)=0,19 y P(E)=0,02