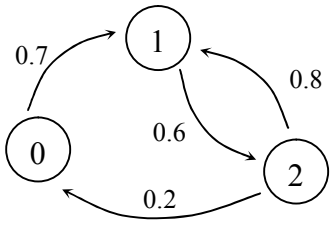
Problema 1 (5 puntos)

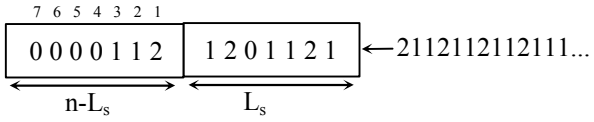
Una fuente de símbolos se puede modelar según la cadena de Markov siguiente:



1) Razónese si se trata de una fuente con memoria
2) Calcúlese la entropía de la fuente en bits/símbolo

La fuente genera la secuencia S= 12011212112112112111, comenzando a emitir primero el 1, luego el 2, el 0… Calcúlese para una extensión de orden 2 (agrupaciones de 2 símbolos) los siguientes apartados:

3) Codificación binaria de Huffman para cada símbolo y la eficiencia del código
4) Codificación binaria de Shanon-Fano-Elias para los dos últimos símbolos de S: 2111 y la eficiencia del código
5) Codificación LZ77 de S, partiendo de un Look Ahead Buffer con L_s=7 símbolos ternarios y del estado inicial que se indica a continuación:



Considérese ahora una fuente binaria X sin memoria con p(X=1)=0.68. Los símbolos de esta fuente atraviesan un canal ruidoso que se modela como la suma XOR con otra fuente binaria sin memoria Z con entropía igual a 0.8 bits/símbolo y p(Z=0)>p(Z=1). Encuéntrese para los símbolos recibidos (variable aleatoria Y):

6) H(Y) y la entropía de la extensión de orden n: $H(Y^n)$
7) H(Y/X) y $H(Y^n/X^n)$

NOTAS:
a) Utilícese la precisión de los números reales que se considere conveniente
b) $\lim_{p\to 0} p*\log(p) = 0$

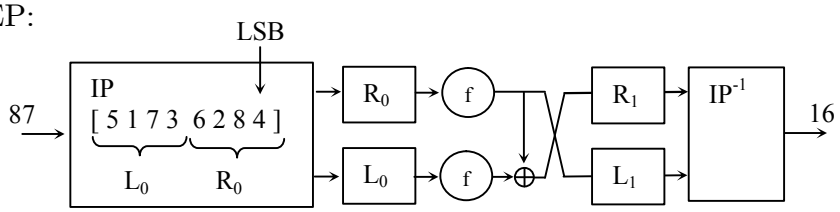
Problema 2 (5 puntos)

Aldous y Simon, viejos amigos, viven en islas diferentes y trabajan en el desarrollo de una nueva molécula. Para la seguridad de sus transacciones electrónicas utilizan ligeras modificaciones de los algoritmos convencionales, y así intentar despistar a los "enemigos". En particular, la función de Hash es muy parecida al algoritmo DES y el cifrado al algoritmo RSA con una operación adicional. Por motivos de simplicidad se analizará solamente el funcionamiento básico de ambos.

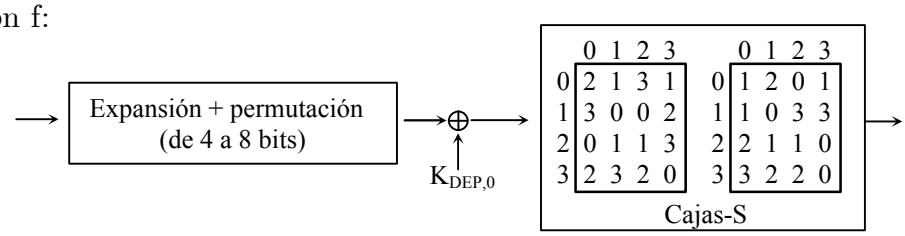
El primer objetivo del problema es encontrar el hash del mensaje M=A187, expresado en notación hexadecimal. Considérese que la función H(m) proporciona el último bloque cifrado por un algoritmo de clave simétrica, que llamaremos DEP, en modo CBC.

1) Proponga IP^{-1}, una matriz inversa a la permutación inicial IP. Valore si la clave $K_{DEP,0}$ del DEP debe ser secreta
2) Proponga una matriz de expansión y permutación con el mismo criterio del algoritmo DES
3) Considerando la clave $K_{DEP,0}$=E6 (hexadecimal), calcule H(M)

- Cifrador DEP:



- Función f:



El segundo objetivo del problema es cifrar y para ello se utiliza un RSA. Los parámetros para Simon son: d=6493, n=p*q=157*71. Sin embargo, para incrementar la confusión de un posible atacante, se intercambian primero una clave adicional (antes de cifrar M) mediante un algoritmo Diffie-Hellman, y se sabe que es k_{DH} =43 (=g^{xy}mod59). Se calcula entonces un segundo mensaje M_2 función de esta clave k_{DH}, y es M_2 quien se transmite cifrado con el RSA. Resolver:

4) El valor de M_2 si es la inversa de M (mod k_{DH})
5) El criptograma de M_2. Demuéstrese que Simon recibe M_2
6) El valor del mensaje recibido por Simon, y en el caso de no ser M propóngase una solución
7) Indique cómo se conseguiría autenticidad de origen y contenido