PROBLEMA 1

a) $H(X|A) = 0'2 \log_2 \frac{1}{0'7} + 0'3 \log_2 \frac{1}{0'3} = 0'8813$ bits/símb

$H(X|B) = 0'8 \log_2 \frac{1}{0'8} + 0'2 \log_2 \frac{1}{0'2} = 0'7219$ bits/símb

$p(A) = p(A|A)\cdot p(A) + p(A|B)\,p(B)$; $p(A)+p(B) = 1$ $\Rightarrow$ $p(A) = 0'7\cdot p(A) + 0'8\,(1-p(A))$

$p(A) = 0'3/1'1 = 0'7273$ $\quad p(B) = 0'2727$

$$H = H(X|A)\,p(A) + H(X|B)\,p(B) = 0'8378 \text{ bits/símb}$$

b)

$H_S = H_S(X|A)\,p(A) + H_S(X|B)\,p(B)$

($p(A)$: prob. emitir A; $p(B)$: prob. emitir B)

$H_S(X|A) = p_S(A|A)\log_2 \frac{1}{p_S(A|A)} + p_S(B|A)\log_2 \frac{1}{p_S(B|A)}$

$H_S(X|B) = p_S(A|B)\log_2 \frac{1}{p_S(A|B)} + p_S(B|B)\log_2 \frac{1}{p_S(B|B)}$

$p_S(A|A) = p(A|A)\cdot(1-p) + p(B|A)\,p$; $p_S(B|A) = 1 - p_S(A|A)$

$p_S(B|B) = p(A|B)\,p + p(B|B)(1-p)$; $p_S(A|B) = 1 - p_S(B|B)$

$p_S(A|A) = 0'66$

$p_S(B|A) = 0'34$

$p_S(B|B) = 0'26$

$p_S(A|B) = 0'74$

$H_S(X|A) = 0'9248$

$H_S(X|B) = 0'8267$

$H_S = 0'9248\cdot 0'7273 + 0'8267\cdot 0'2727 = 0'8978$

c) Se produce un error a la salida si el canal introduce 2 errores. En bloque el número de bits emitido en un bloque es de 3. La probabilidad de error a nivel de bit:

$p_e = \frac{3}{7}\binom{7}{2} p^2 (1-p)^5 = 0'05314$ $\Rightarrow$ Repitiendo los mismos con esa probabilidad

$$\Rightarrow H_S = 0'8786$$

PROBLEMA 2

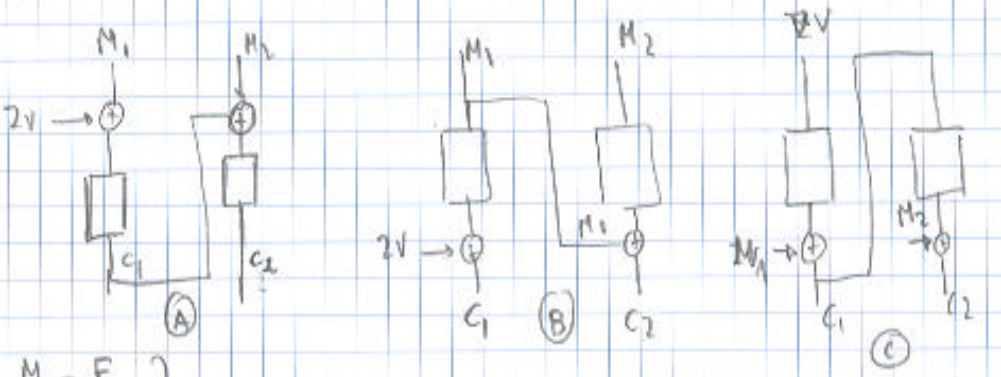
a) Nº biyecciones $16! = 20.922.789.888.000$

Nº bits $\log_2 16! = 44.25 \Rightarrow$ Longitud = 45 bits

b) Porque el cifrado de un mensaje uniforme produce un criptograma no uniforme

c) Se puede utilizar un número de secuencia o un estampado de tiempos. La ventaja que aportan es que no se producen mensajes estereotipados

d) Posibilidades de encadenado:



$M_1 = F$

$M_2 = F$

$C_1 = 6$

$C_2 = A$

(A) $E_K[C_1 + M_2] = E_K[6+F] = E_K[9] = C_1 \neq C_2 = A \Rightarrow$ NO

(B) $E_K[M_2] + M_1 = E_K[F] + F = A + F = 5 \neq C_2 = A \Rightarrow$ NO

(C) $E_K[C_1] + M_2 = E_K[6] + F = 5 + F = A = C_2 = A \Rightarrow$ OK

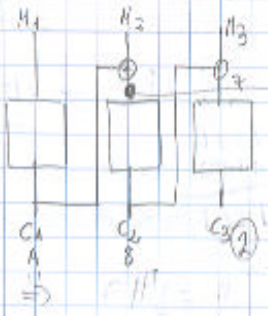
$$\begin{cases} C_i = M_i + E_k(C_{i-1}) \\ M_i = C_i + E_k(C_{i-1}) \end{cases}$$

$Z_v = D_k[C_1 + M_1] = D_k[6+F] = D_k[9] = (A)$

e) $h_1 = E_k[F] = A$

$h_2 = E_k[F+A] = E_k[5] = 8$

$h_3 = E_k[F+8] = E_k[7] = 2 = H$



Ponto de colisão = F+A = 5

$C_1 + M_2 = C'_1 + M'_2 = E_k(M'_1) + M'_2$

$A+F = 5 = C'_1 + M'_2 = E_k(M'_1) + M'_2$

$\Rightarrow M'_1 = F \Rightarrow 5 = A + M'_2 \Rightarrow M'_2 = 5+A = F \Rightarrow$ 15 valores distintos

pois que $M_1 = F \Rightarrow M_2 = F$.

f)

$E_k[H] + A = 5 \Rightarrow [M = D_k[4] = A]$

Hoja de respuestas

Apellidos ____________________ Nombre ____________

Problema 1

a) Entropía de la fuente = 0'8378

b) Entropía a la salida del canal = 0'898

Comentario: Puesto que el canal introduce incertidumbre la entropía a su salida debe ser mayor.

c) Entropía a la salida del decodificador = 0'8718

Problema 2

a) Long. Clave = $\log_2 16! = 45$

b) El cifrado de un uniforme produce un criptograma no uniforme

c) Nº de secuencia o estampado de tiempos. No produce mensajes extemporáneos

d) Cifrado: $C_i = E_k[C_{i-1}] + M_i$ IV= A

Descifrado: $M_i = C_i + E_k[C_{i-1}]$

e) HASH: 2 Num. Mensajes= 15

f) Valor de M= A