Examen Final

Informació i Seguretat (Universitat Autònoma de Barcelona)

INFORMACIÓ I SEGURETAT
21 de juny de 2012

Nom i cognoms: ____ Grup: ______

- **Cal que justifiqueu convenientment totes les respostes**
- $\log 3 = 1.58$, $\log 5 = 2.32$, $\log 7 = 2.8$
- $28441 \bmod 360 = 1$, $28441 \bmod 407 = 358$, $97273 \bmod 119 = 50$, $15^{119} \bmod 407 = 278$, $15^{239} \bmod 407 = 124$.
- Equivalència entre lletres i números:

$$\begin{bmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \end{bmatrix}$$

1. (25%=10%+10%+5%) Sigui $S = \{A, B, C, D, E\}$ una font amb probabilitats $\{0.1, 0.1, 0.2, 0.2, 0.4\}$ i $H(S) = 2.122$.

   (a) Doneu un codi binari òptim per codificar la font. Comproveu que aquest codi verifica el Primer Teorema de Shannon.

   (b) Considereu el codi $C_1 = \{111, 110, 01, 00, 10\}$ per codificar S. És instantani? És òptim?

   (c) Comprimiu el missatge "BCCEADEB" fent servir el codi de l'apartat (b) i doneu la taxa de compressió (suposem que cada caràcter de l'alfabet enviat sense comprimir ocupa 3 bits).

   Solució:

   (a) Aplicant l'algorisme de Huffman, obtenim el següent codi (no és únic): $C_H = \{0000, 0001, 001, 01, 1\}$ que té una longitud mitjana $\bar{L} = 0.4 + 0.4 + 0.6 + 0.4 + 0.4 = 2.2$. El Primer Teorema de Shannon diu que tot codi D-ari de descodificació única amb longitud mitjana $\bar{L}$ verifica $\bar{L} \geq \frac{H(S)}{\log(D)}$. En aquest cas, $\log(D) = \log(2)$ i per tant tenim que efectivament $2.2 \geq 2.122$ i es verifica el Primer Teorema de Shannon.

   (b) Sí que és instantani ja que cap paraula és prefix d'una altra. També és òptim ja que la seva longitud mitjana és $\bar{L}_1 = 0.3+0.3+0.4+0.4+0.8 = 2.2$ i coincideix amb la longitud mitjana del codi de Huffman obtingut a l'apartat anterior.

   (c) El missatge comprimit és "`1100101100001110001`". Si cada caràcter ocupa 3 bits, aleshores la taxa de compressió és $R = \frac{19}{3*8} = \frac{19}{24}$ bpb.

2. (25%=5%+10%+10%) Tenim un canal discret i sense memòria amb un alfabet d'entrada $A = \{A_1, A_2\}$, un alfabet de sortida $B = \{B_1, B_2, B_3, B_4\}$ i una matriu de transicions

$$\Pi = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

(a) Quin és el valor màxim de $H(B)$?

(b) Doneu el valor de $H(A)$ i $H(B)$ si la distribució inicial és equiprobable.

(c) Doneu la informació mútua de l'entrada i la sortida si la distribució inicial és equiprobable.

Solució:

(a) Si tenim n esdeveniments, la informació (o entropia) màxima es dóna quan tots els esdeveniments són equiprobables. Per tant, el màxim valor de $H(B)$ és $H(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) = \log(4) = 2$ bits.

(b) La distribució inicial és equiprobable; per tant, $H(A) = \log(2) = 1$. Per trobar $H(B)$ tenim que $p(B_1) = p(B_3) = p(B_4) = \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$ i $p(B_2) = \frac{1}{2} \cdot \frac{1}{4} + 1 \cdot \frac{1}{2} = \frac{5}{8}$. Aleshores, $H(B) = \frac{3}{8}\log(8) + \frac{5}{8}\log(\frac{8}{5}) = \frac{9}{8} + \frac{5}{8}(\log(8) - \log(5)) = 1.5 + \frac{5}{8}(3 - 2.32) = 1.125 + 0.425 = 1.55$.

(c) $I(A, B) = H(B) - H(B|A) = 1.55 - 1 = 0.55$ bits.

3. (25%=5%+5%+5%+10%) Considereu el codi binari C de matriu de control,

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(a) Doneu la longitud n i la dimensió k de C. Quantes paraules-codi té C? Quina és la seva taxa de transmissió?

(b) A partir de la matriu de control H, determineu la distància mínima d. Quants errors pot corregir i quants errors pot detectar aquest codi?

(c) Trobeu una matriu generadora G del codi C.

(d) Si hem codificat la informació amb el codi C i hem rebut la seqüència de bits `1011011 1101111 1101001`, indiqueu si s'han produit errors. Els podrem corregir?

Solució:

(a) Com que H és la matriu de control, aleshores $n = 7$ i $n - k = 4$. Per tant, $k = 3$. Com que $k = 3$, el codi C tindrà $2^3 = 8$ paraules-codi. La taxa de transmissió serà $R_T = \frac{3}{7}$.

(b) Totes les columnes de la matriu H són diferents. A més, si sumem dues columnes qualssevol no obtenim una altra columna d'H. Per tant, $d \geq 4$. En canvi, si sumen les tres primeres columnes obtenim la cinquena. Per tant, $d = 4$. Aleshores, el codi pot detectar $d - 1 = 3$ errors i pot corregir $\lfloor \frac{d-1}{2} \rfloor = 1$ errors.

(c) Una matriu G seria,

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(d) El codi és 1-corrector. Calculem la taula estàndard:

Líder	Síndrome
0	**0**
1000000	$H(1000000) = 1000$
0100000	$H(0100000) = 0100$
0010000	$H(0010000) = 0010$
0001000	$H(0001000) = 0001$
0000100	$H(0000100) = 1110$
0000010	$H(0000010) = 0111$
0000001	$H(0000001) = 1101$

Com que $H(1011011) = 0001$ podem afirmar que s'ha produit un error en el bit número 4 i la paraula-codi enviada ha estat, 1010011.

Com que $H(1101111) = 1001$ podem afirmar que s'ha produït més d'un error i no els podrem corregir.

Com que $H(1101001) = 0000$ podem afirmar que no s'ha produït cap error.

4. (25%=6.25%+6.25%+6.25%+6.25%) Justifiqueu si són certes o falses les següents afirmacions:

(a) L'AES és menys segur que el DES ja que el nombre d'iteracions de l'AES és com a màxim 14 que és inferior al nombre d'iteracions del DES.

(b) Si $(407 = 11 * 37, 119)$ és la clau pública d'un sistema RSA aleshores 239 és la clau privada.

(c) Si $(407 = 11 * 37, 119)$ és la clau pública d'un sistema RSA, la signatura digital de $m = 15$ serà 278.

(d) Les funcions *Hash* s'utilitzen en criptografia per accelerar el procés de la signatura digital.

Solució:

(a) Fals. L'AES és molt més segur que el DES; de fet, el DES es pot trencar en 22 hores. La seguretat de l'AES i el DES es basa, sobretot, en la seva clau privada. En el cas del DES, la clau és de 56 bits i en el cas de l'AES, la clau és, com a mínim, de 128 bits.

(b) Cert. La clau privada $d = 239$ ha de complir $e \cdot d \bmod 10 \cdot 36 = 1$. Es a dir, $119 \cdot 239 \bmod 360 = 28441 \bmod 360 = 1$.

(c) Fals. 278 és el resultat de xifrar $m = 15$ amb la clau pública, $15^{119} \bmod 407 = 278$.

(d) Cert. La signatura digital consisteix en aplicar la clau privada de l'usuari al missatge original. Aquest procés és lent i, per aquest motiu, en comptes de signar el missatge sencer, es signa un resum del missatge obtingut amb la funció *Hash*.