StuDocu.com

Examen 23 de junio 2015, preguntas y respuestas

Informació i Seguretat (Universitat Autònoma de Barcelona)

StuDocu is not sponsored or endorsed by any college or university
Downloaded by Això L'audio (presidencialodisseu@gmail.com)

INFORMACIÓ I SEGURETAT
23 de juny de 2015

Nom i cognoms:_____ Grup: _____ Niu: _____

- Cal que justifiqueu convenientment totes les respostes.
- Valoració dels exercicis: 1) 0.5+1+1 punts; 2) 1+0.5+1 punts; 3) 0.5+1+1 punts 4) 2.5 punts.

1. (2.5 punts) Considereu el canal amb matriu

$$\Pi = \begin{pmatrix} 1 & 0 \\ 1/2 & 1/2 \\ 0 & 1 \end{pmatrix},$$

i distribució de probabilitats inicial $\{p_1, p_2, p_3\}$.

   (a) Digueu quant val la probabilitat mitjana d'error si descodifiquem a màxima versemblança.

   (b) Quina és la informació mútua entre l'entrada i la sortida d'aquest canal si els tres senyals inicials són equiprobables?

   (c) Calculeu la informació mútua, en funció de p_1, suposant que $p_2 = 2p_1$.

   Solució: Diguem $A = \{A_1, A_2, A_3\}$ a les entrades i $B = \{B_1, B_2\}$ a les sortides.

   (a) La descodificació a màxima versemblança és $f(B_1) = A_1$, $f(B_2) = A_3$. La probabilitat mitjana d'error és:

$$\overline{P}_e = 1 - p_1 - p_3 = p_2.$$

   (b) Tenim que $P(B_1) = 1/3 + 1/6 = 1/2$. Aleshores, $H(B) = H(1/2, 1/2) = 1$. El resultat és:

$$I(A, B) = H(B) - H(B|A) = 1 - p_2 = 1 - 1/3 = 2/3.$$

   (c) En aquest cas, $P(B_1) = p_1 + p_2/2 = 2p_1$. Aleshores, $H(B) = H(2p_1, 1 - 2p_1)$ i $H(B \mid A) = p_1 H(0, 1) + p_2 H(1/2, 1/2) + p_3 H(0, 1) = p_2 = 2p_1$. Per tant,

$$I(A, B) = H(2p_1, 1 - 2p_1) - 2p_1.$$

2. (2.5 punts) Sigui $S = \{a, e, i, o, u\}$ una font discreta amb distribució de probabilitats $\{0.4, 0.2, 0.2, 0.1, 0.1\}$ i $H(S) = 2.122$.

   (a) Calculeu un codi binari òptim C_1 per codificar aquesta font i calculeu-ne la seva eficiència.

   (b) Considereu un altre codi $C_2 = \{00, 01, 10, 110, 111\}$ per codificar la font S. És de descodificació única? En cas afirmatiu, és òptim?

   (c) Comprimiu el missatge "*eieieieia*" utilitzant l'algorisme LZ77. Comprimiu-lo també utilitzant el codi de l'apartat (a). Quin dels dos mètodes és millor per comprimir aquest missatge (suposant que cada caràcter es codifica en 8 bits i les posicions en 3 bits)?

Downloaded by Això L'audio (presidencialodisseu@gmail.com)

Solució:

(a) Aplicant l'algorisme de Huffman, obtenim el codi $C_1 = \{0, 10, 110, 1110, 1111\}$ amb una longitud mitjana $\bar{L} = 0.4 + 2 \cdot 0.2 + 3 \cdot 0.2 + 4 \cdot 0.1 + 4 \cdot 0.1 = 2.2$. L'eficiència serà $\eta = \frac{H(S)}{\bar{L}} = \frac{2.122}{2.2} = 0.96$.

(b) El codi C_2 és instantani i, per tant, també és de descodificació única. A més, $\bar{L} = 2 \cdot 0.4 + 2 \cdot 0.2 + 2 \cdot 0.2 + 3 \cdot 0.1 + 3 \cdot 0.1 = 2.2$ que coincideix amb la longitud mitjana del codi C_1. Per tant el codi C_2 també és òptim.

(c) Utilitzant l'algorisme LZ77 obtenim la compressió, $(0, 0, e)(0, 0, i), (2, 6, a)$ amb una taxa de compressió, $R = \frac{42}{72} = 0.58$ bpb. Utilitzant el codi C_1 obtenim 101101011010110101100 amb una taxa de compressió $R = \frac{21}{72} = 0.29$ bpb. En aquest cas és millor utilitzar el mètode de Huffman.

Downloaded by Això L'audio (presidencialodisseu@gmail.com)

3. (2.5 punts) Considereu l'assignació entre diferents bases nitrogenades i elements de $\mathbb{F}_2^3$:

Base nitrogenada	$\mathbb{F}_2^3$
Adenina (A)	000
Guanina (G)	001
Citosina (C)	010
Timina (T)	110
Uracil (U)	111

Enviem dades a través d'un canal binari simètric amb soroll. Per tal de corregir possibles errors, fem servir el següent codi lineal:

$$C = \{000000, 100111, 010110, 110001, 001101, 101010, 011011, 111100\}.$$

(a) Doneu la matriu generadora G de C en forma sistemàtica. A partir de G, doneu la matriu de control H de G.

(b) Justifiqueu quins són els paràmetres $[n, k, d]$ de C. Codifiqueu la seqüència d'ADN CGT fent servir la taula d'assignació i el codi C.

(c) Quants errors pot corregir el nostre codi per cada 6 bits enviats? Hem rebut la cadena 111100000000011110 a la sortida d'el canal que es correspon a una seqüència d'ARN. Descodifiqueu la cadena i doneu la seqüència enviada.

Solució:

(a) La matriu sistemàtica amb la identitat a les tres primeres coordenades seria:

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

La matriu de control és:

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

(b) La longitud del codi, n, és el nombre de columnes de G, la dimensió, k és el nombre de files de G i la distància mínima, d, és el pes mínim de les paraules de C. A partir de C i G obtenim que $[n, k, d] = [6, 3, 3]$.
Per codificar CGT, hem de codificar la informació $i_1 = 010$, $i_2 = 001$, $i_3 = 110$. La codificació és $i_1 \cdot G = 010110$, $i_2 \cdot G = 001101$, $i_3 \cdot G = 110001$. Per tant, la seqüència codificada és: 010110001101110001.

(c) La capacitat correctora del codi és $t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = 1$. El codi pot corregir 1 error per cada 6 enviats. Com que podem corregir tots el vectors d'errors de pes 1, la taula de síndromes serà,

Líder	Síndrome
0	**0**
100000	111
010000	110
001000	101
000100	100
000010	010
000001	001

Downloaded by Això L'audio (presidencialodisseu@gmail.com)

Calculem la síndrome dels vectors rebuts $w_1 = (1,1,1,1,0,0)$, $w_2 = (0,0,0,0,0,0)$, $w_3 = (0,1,1,1,1,0)$. Com que $H(w_1) = (0,0,0)$ i $H(w_2) = (0,0,0)$, no hi ha hagut error als dos primers vectors rebuts. $H(w_3) = (1,0,1) = H(0,0,1,0,0,0)$, hi ha hagut un error en la posició 3 i el vector enviat és, $v_1 = (0,1,0,1,1,0)$. Un cop corregit els errors, sabem que la cadena enviada és 111100000000010110 i, com el codi és sistemàtic, la informació és 111000010 i la seqüència d'ARN és UAC.

4. (2.5 punts) Justifiqueu si són certes o falses les següents afirmacions:

   (a) Per a xifrar un text llarg utilitzant un criptosistema en bloc el més segur és fer servir el mode de xifrat ECB.

   (b) En una xarxa amb molts usuaris, la criptografia de clau pública complica la gestió de claus perquè, a diferència de la criptografia de clau simètrica, en comptes de tenir una única clau per xifrar i desxifrar se'n necessiten dues.

   (c) En un sistema de clau pública, si jo sóc l'usuari A, per enviar un missatge xifrat a l'usuari B, utilitzaré la meva clau privada.

   (d) En un esquema de signatura digital amb RSA, el procés de signatura equival al procés de desxifrat i el de validació de signatura al procés de xifrat.

   (e) Un certificat digital és una estructura de dades pública que inclou el nom de l'usuari, la seva clau pública, la seva clau privada i una signatura de l'autoritat de certificació que li dóna validesa.

Solució:

(a) Fals. Perquè el ECB no encadena els blocs i blocs iguals queden xifrats de la mateixa manera, permetent realitzar atacs basats en mesures estadístiques del text en clar.

(b) Fals. En una xarxa de molts usuaris, malgrat que la criptografia de clau simètrica permeti xifrar i desxifrar amb la mateixa clau, hi ha el problema que és necessari tenir una clau diferent per a cada usuari amb el que et vols comunicar. Així, la gestió de claus és molt més simple amb criptografia de clau pública perqué el nombre total de claus que necessita el sistema és molt menor.

(c) Fals. Si l'usuari A vol enviar un missatge xifrat a l'usuari B haurà d'utilitzar la clau pública de B. D'aquesta manera, només B, que coneix la corresponent clau privada, en prodrà desxifrar el contingut.

(d) Cert. Donat que la realització d'una signatura digital ha d'estar restringida, la informació per realitzar-la també ho ha d'estar i per aquest motiu es fa servir la clau privada, que s'utilitza en el procés de desxifrat. D'altra banda, la validació de la signatura l'ha de poder realitzar qualsevol usuari i per tant s'ha de fer amb informació pública, en aquest cas, la clau pública de l'usuari. Per això, la validació equival al procés de xifrat.

(e) Fals. En un certificat digital, donat que és una informació pública no hi pot constar de cap manera la clau privada de l'usuari ja que això trencaria tota la seguretat del sistema.

Downloaded by Això L'audio (presidencialodisseu@gmail.com)