Name: .... Student Id: .... Tutor/tutorial ....

UNSW **School of Mathematics and Statistics**

MATH3411 Information Codes and Ciphers

Semester 2, 2012 **TEST 2** **VERSION A**

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**; each multiple choice question is worth 2 marks.
For the true/false and written answer questions, use extra paper.
Staple everything together at the end.

1. A source $S = \{s_1, s_2\}$ has probabilities $P(s_1) = \frac{5}{7}$, $P(s_2) = \frac{2}{7}$. The second most likely codewords in the binary Shannon-Fano code for the third extension S^3 have length

(a) 1 (b) 2 (c) 3 (d) 4 (e) 5

2. If a channel has input entropy $H(A) = 0.57$, output entropy $H(B) = 0.29$ and joint entropy $H(A, B) = .73$ (all in bits), the mutual information $I(A, B)$ in bits is approximately

(a) 0.16 (b) 0.86 (c) 0.44 (d) 1.01 (e) 0.13

3. Let $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$, so that $H'(x) = \log_2(x^{-1} - 1)$. An asymmetric binary channel with input $A = \{a_1, a_2\}$ and output $B = \{b_1, b_2\}$ has noise entropy $H(B \,|\, A) = 0.5p + 0.7$ in bits, output entropy $H(B) = H(0.2 + 0.7p)$ in bits and $p = P(a_1)$ The channel capacity is achieved when p has the value approximately

(a) 0.47 (b) 0.26 (c) 0.41 (d) 0.38 (e) 0.31

4. Using Euler's Theorem or otherwise, calculate $3^{2011} \pmod{2012}$. The answer is

(a) 1 (b) 3 (c) 9 (d) 27 (e) 81

5. Use Fermat factorisation to factor $n = 3569$ as a product $n = ab$ where $2 \leq a < b$. Then $b - a$ equals

(a) 34 (b) 36 (c) 38 (d) 40 (e) 42

6. **[10 marks]** For each of the following, say whether the statement is true or false giving a brief reason or showing your working. You will get one mark for a correct true/false answer, and if your true/false answer is correct then you will get one mark for a good reason.

Begin each answer with the word “true” or “false”.

i) If the message *abaabbaaa* is encoded using the LZ78 algorithm, the last entry in the message after compression is $(3, a)$.

ii) For a 2-symbol source $S = \{s_1, s_2\}$ with probabilities $p_1 = 4/5$, $p_2 = 1/5$ it is possible to find a binary encoding of some extension S^n with average word length per original source symbol less than 0.75.

iii) The inverse of 22 in $\mathbb{Z}_{175}$ does not exist.

iv) Given that 5 is a primitive element of $\mathbb{Z}_{17}$, then 6 is also a primitive element.

v) The composite number 25 is a pseudoprime to base 7.

7. **[10 marks]** Let $\mathbb{F} = \mathbb{Z}_3(\alpha)$ where α is a root of the polynomial $x^2 + 2x + 2 \in \mathbb{Z}_3[x]$.

(i) Express all nonzero elements of $\mathbb{F}$ as a power of α and as a linear combination over $\mathbb{Z}_3$ of 1, α.

(ii) Solve the set of linear equations

$$\begin{pmatrix} \alpha^4 & \alpha^5 \\ \alpha^2 & \alpha^7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ \alpha^3 \end{pmatrix}$$

in $\mathbb{F}$.

(iii) Find the minimal polynomial of α^7. Show your working.

Name: .... Student Id: .... Tutor/tutorial...............

UNSW **School of Mathematics and Statistics**

MATH3411 Information Codes and Ciphers

Semester 2, 2012 **TEST 2** **VERSION B**

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**; each multiple choice question is worth 2 marks.
For the true/false and written answer questions, use extra paper.
Staple everything together at the end.

1. A source $S = \{s_1, s_2\}$ has probabilities $P(s_1) = \frac{6}{7}$, $P(s_2) = \frac{1}{7}$. The second least likely codewords in the binary Shannon-Fano code for the third extension S^3 have length

(a) 5 (b) 6 (c) 7 (d) 8 (e) 9

2. If a channel has input entropy $H(A) = 0.93$, output entropy $H(B) = 0.76$ and mutual information $I(A, B) = 0.56$ (all in bits), the joint entropy $H(A, B)$ in bits is approximately

(a) 1.69 (b) 0.20 (c) 1.13 (d) 0.73 (e) 0.37

3. Let $H(x) = -x \log_2 x - (1-x) \log_2(1-x)$, so that $H'(x) = \log_2(x^{-1} - 1)$. An asymmetric binary channel with input $A = \{a_1, a_2\}$ and output $B = \{b_1, b_2\}$ has noise entropy $H(B \,|\, A) = 0.5p + 0.9$ in bits, output entropy$H(B) = H(0.3 + 0.6p)$ in bits and $p = P(a_1)$. The channel capacity is achieved when p has the value approximately

(a) 0.32 (b) 0.35 (c) 0.19 (d) 0.26 (e) 0.10

4. Using Euler's Theorem or otherwise, calculate $5^{2011} \pmod{2012}$. The answer is

(a) 1 (b) 5 (c) 25 (d) 125 (d) 625

5. Use Fermat factorisation to factor $n = 5141$ as a product $n = ab$ where $2 \le a < b$. Then $b - a$ equals

(a) 44 (b) 46 (c) 48 (d) 50 (e) 52

6. **[10 marks]** For each of the following, say whether the statement is true or false giving a brief reason or showing your working. You will get one mark for a correct true/false answer, and if your true/false answer is correct then you will get one mark for a good reason.

Begin each answer with the word “true” or “false”.

i) If the message *abbababbb* is encoded using the LZ78 algorithm, the last entry in the message after compression $(3, b)$.

ii) For a 2-symbol source $S = \{s_1, s_2\}$ with probabilities $p_1 = 7/9$, $p_2 = 2/9$ it is possible to find a binary encoding of some extension S^n with average word length per original source symbol less than 0.8.

iii) The inverse of 21 in $\mathbb{Z}_{175}$ does not exist.

iv) Given that 3 is a primitive element of $\mathbb{Z}_{17}$, then 13 is also a primitive element.

v) The composite number 21 is a pseudoprime to base 8.

7. **[10 marks]** Let $\mathbb{F} = \mathbb{Z}_3(\alpha)$ where α is a root of the polynomial $x^2 + x + 2 \in \mathbb{Z}_3[x]$.

(i) Express all nonzero elements of $\mathbb{F}$ as a power of α and as a linear combination over $\mathbb{Z}_3$ of 1, α.

(ii) Solve the set of linear equations

$$\begin{pmatrix} \alpha^2 & \alpha^4 \\ \alpha & \alpha^5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha^2 \end{pmatrix}$$

in $\mathbb{F}$.

(iii) Find the minimal polynomial of α^7. Show your working.