Name: ..... Student ID: .....

UNSW School of Mathematics and Statistics

MATH3411 Information Codes and Ciphers

2017 S2 **TEST 2** **VERSION A**

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**;
each multiple choice question is worth **1 mark**.
For the true/false and written answer questions, use extra paper.
Staple everything together at the end.

1. Using the LZ78 algorithm a message is encoded as $(0,b)(0,a)(2,a)(3,b)(3,a)$. What is the last dictionary entry after decoding?

(a) aaa (b) aab (c) aba (d) baa (e) bab

2. A 2-symbol Markov source has transition matrix $M = \begin{pmatrix} 0.7 & 0.4 \\ 0.3 & 0.6 \end{pmatrix}$ and equilibrium distribution $\mathbf{p} = \frac{1}{4}\begin{pmatrix} 3 \\ 1 \end{pmatrix}$. The (binary) Markov entropy H_M is approximately

(a) 0.811 (b) 0.904 (c) 0.926 (d) 0.949 (e) 0.961

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 $H(B\,|\,A) = 0.4p + 0.1$ in bits with $H(B) = H(0.2 + 0.7p)$ in bits and $p = P(a_1)$. The channel capacity is achieved when p has the value approximately

(a) 0.29 (b) 0.33 (c) 0.36 (d) 0.40 (e) 0.43

4. Use Euler's Theorem or otherwise to calculate $5^{2272} \pmod{3411}$.
The answer is

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

5. Use Fermat factorisation to factor $n = 1113$ as a product $n = ab$ where $2 \le b < a$. Then $a - b$ equals

(a) 21 (b) 32 (c) 42 (d) 53 (e) None of these

6. **[5 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 $\frac{1}{2}$ **mark** for a correct true/false answer, and if your true/false answer is correct, then you will get $\frac{1}{2}$ **mark** for a good reason.

Begin each answer with the word "True" or "False".

i) If arithmetic coding with source symbols a, b and stop symbol $\bullet$ corresponding to the intervals $[0, 0.3)$, $[0.3, 0.7)$ and $[0.7, 1)$ is used, then the message $bb\bullet$ is encoded by 0.55.

ii) For a 3-symbol source $S = \{s_1, s_2, s_3\}$ with probabilities $p_1 = 4/9$, $p_2 = 2/9$, $p_3 = 1/3$ it is possible to find a **binary** encoding of some extension S^n with average word length per original source symbol less than 1.5.

iii) For a source $S = \{a, b\}$ with probabilities $P(a) = \frac{3}{4}$ and $P(b) = \frac{1}{4}$, the second shortest codewords in the binary Shannon-Fano code for the fourth extension S^4 have length 7.

iv) There are 60 primitive elements in the field GF(125).

v) The number 3 is one of the pseudo-random numbers generated by the linear congruential $x_{i+1} \equiv 2x_i + 5 \pmod{17}$, seeded with $x_0 = 1$.

7. **[5 marks]** Let $\mathbb{F} = \mathbb{Z}_3(\alpha)$ where α is a root of the polynomial $x^2 + 1 \in \mathbb{Z}_3[x]$.

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

(ii) Find the primitive elements of $\mathbb{F}$.

(iii) Simplify $\dfrac{\gamma^4 + \alpha}{\gamma^4 + \gamma}$, giving your answer as a linear combination of 1 and α. Show your working.

Name: ..... Student ID: .....

UNSW School of Mathematics and Statistics

MATH3411 Information Codes and Ciphers

2017 S2 **TEST 2** **VERSION B**

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**;
each multiple choice question is worth **1 mark**.
For the true/false and written answer questions, use extra paper.
Staple everything together at the end.

1. If arithmetic coding with source symbols a, b and stop symbol • with probabilities 0.5, 0.4 and 0.1 is used, then what is the message ab• encoded as?

(a) 0.02 (b) 0.21 (c) 0.36 (d) 0.44 (e) None of these

2. A 2-symbol Markov source has transition matrix $M = \begin{pmatrix} 0.7 & 0.4 \\ 0.3 & 0.6 \end{pmatrix}$ and equilibrium distribution $\mathbf{p} = \frac{1}{5}\begin{pmatrix} 3 \\ 2 \end{pmatrix}$. The (binary) Markov entropy H_M is approximately

(a) 0.971 (b) 0.226 (c) 0.936 (d) 0.966 (e) 0.971

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 $H(B|A) = 0.5p + 0.1$ in bits with $H(B) = H(0.3 + 0.7p)$ in bits and $p = P(a_1)$. The channel capacity is achieved when p has the value approximately

(a) 0.11 (b) 0.16 (c) 0.27 (d) 0.38 (e) 0.41

4. Use Fermat factorisation to factor $n = 1215$ as a product $n = ab$ where $2 \le b < a$. Then $a - b$ equals

(a) 12 (b) 14 (c) 16 (d) 18 (e) 20

5. Using Euler's Theorem or otherwise, calculate $5^{66} \pmod{99}$.
The answer is

(a) 5 (b) 14 (c) 25 (d) 31 (e) 82

6. **[5 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 $\frac{1}{2}$ **mark** for a correct true/false answer, and if your true/false answer is correct, then you will get $\frac{1}{2}$ **mark** for a good reason.

Begin each answer with the word "True" or "False".

i) Using the LZ78 algorithm a message is encoded as $(0,a)(0,b)(2,a)(2,b)(4,a)$. The last dictionary entry after decoding is aba.

ii) For a 3-symbol source $S = \{s_1, s_2, s_3\}$ with probabilities $p_1 = 0.6$, $p_2 = 0.3$, $p_3 = 0.1$, it is possible to find a **ternary** encoding of some extension S^n with average word length per original source symbol less than 0.82.

iii) $n = 65$ is a pseudo-prime to base 8.

iv) For symbols s_1, s_2, s_3, s_4 with probabilities 0.5, 0.2, 0.2, 0.1 respectively, the binary Shannon-Fano encoding 01001100 encodes the string of symbols $s_1 s_2 s_4$.

v) Given that 5 is a primitive element of $\mathbb{Z}_{23}$, then 20 is also a primitive element.

7. **[5 marks]** Let $\mathbb{F} = \mathbb{Z}_2(\alpha)$ where α is a root of the polynomial $x^3 + x + 1 \in \mathbb{Z}_2[x]$.

(i) Express all nonzero elements of $\mathbb{F}$ as powers of α and as linear combinations over $\mathbb{Z}_2$ of 1, α, and α^2.

(ii) Find the value of $k \in \{1, \ldots, 7\}$ for which $(\alpha + 1)^k = \alpha^2 + \alpha + 1$.

(iii) Find the minimal polynomial of α^6.
Show your working.