Data provided: Data Sheet

MAS345

The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2012–2013**

Codes and Cryptography **2 hours 30 minutes**

Attempt all the questions. The allocation of marks is shown in brackets.

1 (i) Let p be prime and let C be an $[n, k]$-linear code over $\mathbb{F}_p$. Show that C has precisely p^k codewords. ***(3 marks)***

(ii) Let C be the linear code over $\mathbb{F}_2$ that has generator matrix

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

(a) How many codewords are there in C? How many codewords are there in the dual code $C^\perp$? ***(2 marks)***

Let $\mathcal{E}_7$ be the even weight code of length 7. How many of the codewords of C are in $\mathcal{E}_7$? ***(2 marks)***

(b) Find a parity check matrix H for C. ***(5 marks)***

(iii) Let D be an $[n, k]$-linear code over $\mathbb{F}_2$ and let $d \in D \cap D^\perp$. Show that $\mathrm{wt}(d)$ is even. ***(3 marks)***

With C as in (ii), find all elements of $C \cap C^\perp$. ***(3 marks)***

(iv) Let $v = 0001110 \in \mathbb{F}_2^7$ and let S be the Hamming sphere with centre v and radius 4. How many words are there in S? How many of these words are also in the even weight code $\mathcal{E}_7$? ***(5 marks)***

Is S a linear code? Justify your answer. ***(2 marks)***

2 (i) Let p be prime and let C be an $[n, k, d]$-linear code over $\mathbb{F}_p$. State, without proof, a result which expresses d in terms of linear dependence of columns of a parity check matrix for C. Deduce that $d \leq n - k + 1$ (the Singleton Bound). ***(4 marks)***

(ii) Let C be an $[n, k, 3]$-linear code over $\mathbb{F}_p$ and let H be a parity check matrix for C with columns $h_1, h_2, \ldots, h_n$. Let $a = a_1 a_2 \ldots a_i \ldots a_n \in C$ and let $b = a_1 a_2 \ldots b_i \ldots a_n$ be obtained from a by a single error which occurs in the ith bit. Show that $Hb^T = (b_i - a_i)h_i$. Show also that the position i of the error and the correct ith bit a_i are uniquely determined by Hb^T. ***(5 marks)***

(iii) Let

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 \end{pmatrix} \in \mathrm{M}_{3\times 11}(\mathbb{F}_3)$$

and let C be the linear code over $\mathbb{F}_3$ with parity check matrix H.

(a) Show that C has minimum distance 3. ***(2 marks)***

(b) A codeword $a \in C$ is transmitted and 10101111011 is received. Explain why at least one error must have occurred and, on the assumption that a single error has occurred, identify the codeword a. ***(5 marks)***

Show that 11111111111 cannot be obtained from a codeword in C by an error in a single bit but that it can be obtained from a codeword in C by errors in two bits. ***(3 marks)***

(c) The columns of H are the base 3 representations, written as columns, of the first 15 positive integers with $2, 6, 7$ and 8 omitted. Show that if H is replaced by a 3×12 matrix over $\mathbb{F}_3$ obtained from H by inserting an extra column corresponding to the base 3 representation of 2, 6, 7 or 8, then the resulting code does not correct single errors. ***(2 marks)***

(d) Is C a perfect code? Justify your answer. ***(4 marks)***

3 (i) A message of fifty-seven characters, each of which is a capital letter, is encoded in $\mathbb{Z}_{26}$, using the correspondence in the table on the provided data sheet, and then encrypted using the one-time pad method, deleting spaces and any punctuation marks, working modulo 26 and using the following translation of Euclid's Proposition 20 as key:
PRIME NUMBERS ARE MORE THAN ANY ASSIGNED MULTITUDE OF PRIME NUMBERS.

The first eight characters of the encrypted message are IYQEIKUY. Decrypt these eight characters. ***(3 marks)***

Later in the unencrypted message, the word EASY appears and the E is encrypted as K. How are the other three letters of EASY encrypted? ***(2 marks)***

(ii) Messages are broken up into units that can be encoded using the 27 elements of $\mathbb{F}_3^3$. Elements of $\mathbb{F}_3^3$ are then written as columns and encrypted using 3-dimensional affine encryption modulo 3, with the transformation $f : \mathbb{F}_3^3 \to \mathbb{F}_3^3$ given by $f(V) = KV + L$, where

$$K = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix} \text{ and } L = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}.$$

Find $a, b, c, d, e \in \mathbb{F}_3$ such that K has inverse

$$\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ d & 0 & e \end{pmatrix}.$$

(1 mark)

Find $V \in \mathbb{F}_3^3$ such that V is encrypted as $(1\ 2\ 0)^T$ and find $W \in \mathbb{F}_3^3$ such that W is encrypted as itself. ***(6 marks)***

(iii) (a) Gavin and Stacey are members of a group who use the ElGamal encryption method with $p = 101$ and the generator $g = 27$ of $\mathbb{F}_{101}$. Gavin's secret key is 69. He receives the encrypted message $(6, 6)$ from Stacey. Decrypt the message. You may use the squares in $\mathbb{F}_{101}$ shown on the data sheet as an aid to calculation. ***(5 marks)***

(b) Horatio is a member of a consortium that uses the ElGamal encryption method with a prime number p and a generator g of $\mathbb{F}_p$. Let a_H be Horatio's secret key and let $(x, y) = (g^k, P(g^{a_H})^k)$ be the encryption of a message P sent to Horatio by another consortium member. Show that

$$x = y \quad \Leftrightarrow \quad P = x^{p-a_H}$$
$$\text{and that } P = x^2 \quad \Leftrightarrow \quad x^{2+a_H} = y.$$

(8 marks)

4 (i) Let p be a prime number and let the prime factorization of $p-1$ be $p_1^{m_1}p_2^{m_2}\dots p_k^{m_k}$, where $p_1, p_2, \dots, p_k$ are distinct prime numbers and each $m_i > 0$. For $1 \leq i \leq k$, let $q_i = (p-1)/p_i$. Let $a \in \mathbb{F}_p^*$. Show that a is a generator of $\mathbb{F}_p$ if and only if $a^{q_i} \neq 1$ for $1 \leq i \leq k$. ***(5 marks)***

Question 3 refers to 27 as a generator of $\mathbb{F}_{101}$. Show that 27 is indeed a generator of $\mathbb{F}_{101}$. You may use the squares in $\mathbb{F}_{101}$ shown on the data sheet. ***(4 marks)***

(ii) The superincreasing 5-tuple $(v_1 = 1, v_2 = 6, v_3, v_4, v_5)$ is chosen in such a way that each v_i is the minimal value of v_i such that $v_i \equiv 1 \bmod 5$. Identify v_3, v_4 and v_5. ***(2 marks)***

(iii) An organisation, to which Yvette belongs, uses Merkle-Hellman knapsack encryption, with superincreasing 5-tuples, to encrypt messages that can be expressed using the 26 letters A–Z, encoded as on the data sheet but with A encoded as 26, and five punctuation marks that are encoded as 27–31. In choosing her key, Yvette first chooses the superincreasing 5-tuple from (ii). Her choice for an integer $M > \sum_{i=1}^{5} v_i$ is 100 and her choice for an integer a, with $0 < a < M$ and $(a, M) = 1$, is 27 which, modulo 100, has inverse 63. She receives an encrypted message which, modulo 100, reduces to 53, 56, 4, 69. Identify the four-letter word that was encrypted. ***(6 marks)***

(iv) Let $p_1, p_2, \dots, p_k$ be distinct prime numbers and let $n = p_1 p_2 \dots p_k$. State, without proof, a necessary and sufficient condition for n to be a *Carmichael number*. ***(2 marks)***

Let $m > 2$ be an odd positive integer such that $6m$ divides 90 and $6m+1$ is prime. Show that $7 \times 13 \times (6m+1)$ is a Carmichael number. Hence find two Carmichael numbers that are divisible by 91. ***(6 marks)***

End of Question Paper

MAS345 Codes and Cryptography 2012-13

DATA SHEET

Table for Q3(i) and Q4(iii).

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

$*$ In Q4(iii), A is encoded as 26.

The list below shows the nonzero squares in $\mathbb{F}_{101}$.

$1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$, $8^2 = 64$,
$9^2 = 81$, $10^2 = 100$, $11^2 = 20$, $12^2 = 43$, $13^2 = 68$, $14^2 = 95$, $15^2 = 23$, $16^2 = 54$,
$17^2 = 87$, $18^2 = 21$, $19^2 = 58$, $20^2 = 97$, $21^2 = 37$, $22^2 = 80$, $23^2 = 24$, $24^2 = 71$,
$25^2 = 19$, $26^2 = 70$, $27^2 = 22$, $28^2 = 77$, $29^2 = 33$, $30^2 = 92$, $31^2 = 52$, $32^2 = 14$,
$33^2 = 79$, $34^2 = 45$, $35^2 = 13$, $36^2 = 84$, $37^2 = 56$, $38^2 = 30$, $39^2 = 6$, $40^2 = 85$,
$41^2 = 65$, $42^2 = 47$, $43^2 = 31$, $44^2 = 17$, $45^2 = 5$, $46^2 = 96$, $47^2 = 88$, $48^2 = 82$,
$49^2 = 78$, $50^2 = 76$, $51^2 = 76$, $52^2 = 78$, $53^2 = 82$, $54^2 = 88$, $55^2 = 96$, $56^2 = 5$,
$57^2 = 17$, $58^2 = 31$, $59^2 = 47$, $60^2 = 65$, $61^2 = 85$, $62^2 = 6$, $63^2 = 30$, $64^2 = 56$,
$65^2 = 84$, $66^2 = 13$, $67^2 = 45$, $68^2 = 79$, $69^2 = 14$, $70^2 = 52$, $71^2 = 92$, $72^2 = 33$,
$73^2 = 77$, $74^2 = 22$, $75^2 = 70$, $76^2 = 19$, $77^2 = 71$, $78^2 = 24$, $79^2 = 80$, $80^2 = 37$,
$81^2 = 97$, $82^2 = 58$, $83^2 = 21$, $84^2 = 87$, $85^2 = 54$, $86^2 = 23$, $87^2 = 95$, $88^2 = 68$,
$89^2 = 43$, $90^2 = 20$, $91^2 = 100$, $92^2 = 81$, $93^2 = 64$, $94^2 = 49$, $95^2 = 36$, $96^2 = 25$,
$97^2 = 16$, $98^2 = 9$, $99^2 = 4$, $100^2 = 1$.