Data provided: Data Sheet

MAS345

The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2010–2011**

Codes and Cryptography **2 hours 30 minutes**

Answer ***four*** *questions. If you answer more than four questions, only your best four will be counted.*

1 (i) Let C be the linear code over $\mathbb{F}_2$ with generator matrix

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

Find a parity check matrix for C. ***(6 marks)***

How many codewords has C and how many codewords has $C^\perp$? ***(2 marks)***

How many codewords of even weight has C and how many codewords of even weight has $C^\perp$? ***(4 marks)***

(ii) A message of nine characters, each of which is a capital letter or one of five punctuation marks, is encoded in $\mathbb{F}_{31}$, 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 not shown in the table, working modulo 31 and using the passage

$$CODESANDCRYPTOGRAPHY$$

as key. The encrypted message

$$E!PIZOZHPAP$$

is obtained. Decrypt the message. ***(4 marks)***

(iii) A message is sent using 1-dimensional affine encryption modulo 31, with the transformation f given by $f(v) = kv + \ell$ for some $k, \ell \in \mathbb{F}_{31}$ and with the same correspondence between characters and $\mathbb{F}_{31}$ as in (ii). If E is encrypted as ! and T is encrypted as O identify k and ℓ and decrypt the message $FTJOB!COY$. ***(7 marks)***

(Inverses in $\mathbb{F}_{31}$ are shown on the data sheet.)

(iv) In its initial position, a disc in a simplified Enigma machine performs the permutation

$$\alpha := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 9 & 1 & 8 & 4 & 7 & 5 & 3 & 0 \end{pmatrix}.$$

Find the permutation $3 * \alpha$ performed by the disc after three rotations. ***(2 marks)***

2 Let C be an (n, M)-code over an alphabet F and let q be the number of distinct elements in F.

(i) Define the *Hamming distance* $d(x, y)$ between two elements $x, y \in F^n$ and the *minimum distance* $d(C)$ of C. ***(3 marks)***

Show that if C is linear then $d(C)$ is equal to the minimum value m of $\mathrm{wt}(c)$ taken over the non-zero codewords c of C. ***(3 marks)***

Hence find $d(C)$ when C is the $[4, 2]$-linear code over $\mathbb{F}_3$ with generator matrix

$$\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

(3 marks)

Let D be the non-linear code over $\mathbb{F}_3$ consisting of all elements of $\mathbb{F}_3^4$ of weight 3 or weight 0. Show that $d(D)$ is not equal to the minimum value m of $\mathrm{wt}(c)$ taken over the non-zero codewords c of D. ***(2 marks)***

(ii) Let $r \geq 0$ be an integer and let $c \in F^n$. Let i be an integer such that $0 \leq i \leq r$. Show that there are $(q-1)^i \binom{n}{i}$ elements v of F^n such that $d(c, v) = i$ and derive a formula for the number of elements in the Hamming sphere $S(c, r)$ of radius r centred at c. ***(4 marks)***

Find the number of codewords in the code D in part (i). ***(2 marks)***

(iii) Write down, without proof, the *Sphere-Packing Bound* for C. ***(2 marks)***

Show that there is no $[8, 4, 5]$-linear code over the field $\mathbb{F}_2$ and find the smallest prime number p such that the Sphere-Packing Bound admits the existence of an $[8, 4, 5]$-linear code over the field $\mathbb{F}_p$. ***(6 marks)***

3 Let C_1 be the $[6,5]$-linear code over the field $\mathbb{F}_7$ with parity check matrix

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

and let C_2 be the $[7,5]$-linear code over the field $\mathbb{F}_7$ with parity check matrix

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

(i) Given that $235\lambda03$ is a codeword in C_1 for some $\lambda \in \mathbb{F}_7$, identify λ and find $\mu \in \mathbb{F}_7$ such that $235\lambda03\mu$ is a codeword in C_2. ***(4 marks)***

(ii) Let $x_1x_2x_3x_4x_5x_6$ be a codeword in C_1 with $x_2 \neq x_5$. Show that $x_1x_5x_3x_4x_2x_6$ is not a codeword in C_1. ***(4 marks)***

Find $\sigma, \tau \in \mathbb{F}_7$ such that $0100\sigma\tau$ and $0\sigma00\tau1$ are codewords in C_1. Is $0\tau001\sigma$ also a codeword in C_1? ***(4 marks)***

(iii) Show that C_2 has minimum distance 3 and error-correcting index 1. ***(4 marks)***

For $1 \leq i \leq 7$, let h_i denote the ith column of H. Show that if an element $b = b_1b_2b_3b_4b_5b_6b_7$ of $\mathbb{F}_7^7$ is obtained by an error in the ith bit of a codeword $a = a_1a_2a_3a_4a_5a_6a_7 \in C_2$ then $Hb^T = (b_i - a_i)h_i$. ***(3 marks)***

(iv) An insurance company specialising in winter sports assigns a codeword from C_2 to each of its ski mountaineering policies. A holder of such a policy writes to the company quoting policy number 1411302. Show that the policy holder has made at least one error and, assuming that there is only one error, identify the policy number. ***(6 marks)***

4 (i) (a) Let p be a prime number. Show that, in the field $\mathbb{F}_p$, there is a generator of $\mathbb{F}_p^*$. If φ denotes Euler's φ-function, you may assume that, for every $n \in \mathbb{N}$, $\sum_{d|n} \varphi(d) = n$. ***(5 marks)***

(b) Use the squares on the data sheet to calculate 2^{20} and 2^{50} in $\mathbb{F}_{101}$. Deduce that 2 is a generator of $\mathbb{F}_{101}^*$. ***(5 marks)***

(ii) Ada, Boris, Calista and Dirk are members of a group who use the ElGamal encryption method with $p = 101$ and the generator $g = 2$ of $\mathbb{F}_{101}$. Boris's public key is 83 and Calista's public key is 10. Ada wishes to send the message 42 to both Boris and Calista using different values for the parameter k. Which ordered pair of elements of $\mathbb{F}_{101}$ does Ada send to Boris if she uses $k = 9$? Deduce from your calculations that Boris's secret key a_B must be the inverse of 9 modulo 100. ***(5 marks)***

Which ordered pair of elements of $\mathbb{F}_{101}$ does Ada send to Calista if she uses $k = 8$? Deduce from your calculations that Calista's secret key a_C must be a multiple of 25. ***(5 marks)***

Ada, whose secret key is 90, receives the message $(11, 31)$ from Dirk. Decrypt this message. ***(5 marks)***

5 (i) State, without proof, a necessary and sufficient condition on the prime factorization of n for a positive integer n to be a Carmichael number. ***(2 marks)***

Given that the prime factorization of 1001 is $7 \times 11 \times 13$, show that 41041 is a Carmichael number. ***(4 marks)***

(ii) Let n be a positive integer of the form $2^4 s + 1$ where s is odd and let $1 \leq a < n$. Write down, in terms of a and s, the Miller-Rabin test sequence that you would use to test whether n is a strong pseudoprime to the base a. ***(2 marks)***

How would you interpret a test sequence of the form $1, 1, 1, 1, 1$? If the test sequence is not of this form, how does the first term that is not 1 determine whether n is a strong pseudoprime to the base a? ***(3 marks)***

It is given that -1 is not a quadratic residue modulo 41041. Show that if 41041 is a strong pseudoprime to the base a then the test sequence is $1, 1, 1, 1, 1$ or $1, 1, 1, 1, -1$. ***(2 marks)***

(iii) The superincreasing 5-tuple $(v_1 = 1, v_2 = 5, v_3, v_4, v_5)$ is chosen in such a way that each v_i is the minimal value of v_i such that $v_i \equiv 1 \bmod 4$. Identify v_3, v_4 and v_5. ***(2 marks)***

(iv) An organisation, to which Xavier, Yolande and Zac belong, uses Merkle-Hellman knapsack encryption, with superincreasing 5-tuples, to encrypt messages that can be expressed involving the 31 letters and symbols in Question 1(ii), encoded as on the data sheet, but with A encoded as 26 and ? as 31. In choosing her key, Yolande first chooses the superincreasing 5-tuple from (iii). Her choice for an integer $M > \sum_{i=1}^{5} v_i$ is 80 and her choice for an integer a, with $0 < a < M$ and $(a, M) = 1$, is 27.

(a) What key does Yolande publish? How should Xavier encrypt the message UM for transmission to Yolande? ***(5 marks)***

(b) Yolande receives the encrypted message 3, 89, 82 from Zac. Which three-letter word was Zac's message? (Any inverses you need can be found by factorising 81.) ***(5 marks)***

End of Question Paper

DATA SHEET

Table for Q1(ii,iii) and Q5(iv):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X	Y	Z	?	.	!	,	:	
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	

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

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

The list below shows the inverses in $\mathbb{F}_{31}$.

$1^{-1} = 1$, $2^{-1} = 16$, $3^{-1} = 21$, $4^{-1} = 8$, $5^{-1} = 25$, $6^{-1} = 26$,
$7^{-1} = 9$, $8^{-1} = 4$, $9^{-1} = 7$, $10^{-1} = 28$, $11^{-1} = 17$, $12^{-1} = 13$,
$13^{-1} = 12$, $14^{-1} = 20$, $15^{-1} = 29$, $16^{-1} = 2$, $17^{-1} = 11$, $18^{-1} = 19$,
$19^{-1} = 18$, $20^{-1} = 14$, $21^{-1} = 3$, $22^{-1} = 24$, $23^{-1} = 27$, $24^{-1} = 22$,
$25^{-1} = 5$, $26^{-1} = 6$, $27^{-1} = 23$, $28^{-1} = 10$, $29^{-1} = 15$, $30^{-1} = 30$.