Data provided: Data Sheet

The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2011–2012**

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) This part of the question concerns the pre-2007 version of the International Standard Book Number (ISBN).

(a) Find $a \in \mathbb{F}_{11}$ such that $345a345345$ is a valid ISBN number. ***(3 marks)***

(b) Let $a, b \in \mathbb{F}_{11}$. Show that $ababababab$ is a valid ISBN if and only if $a = b$. ***(4 marks)***

(c) Show that if $a, b, c, d, e, f, g, h \in \mathbb{F}_{11}$ are such that $abcd44efgh$ is a valid ISBN then, for all $j \in \mathbb{F}_{11}$, $abcdjjefgh$ is a valid ISBN. ***(3 marks)***

(d) Show that if $a, b, c, d, e, f, g, h \in \mathbb{F}_{11}$ are such that $abc44defgh$ is a valid ISBN then, for all $j \in \mathbb{F}_{11}$ such that $j \neq 4$, $abcjjdefgh$ is not a valid ISBN. ***(3 marks)***

(ii) A message of sixteen 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 a poem beginning

$$ON\ RAGLAN\ ROAD\ ON\ AN\ AUTUMN\ DAY$$

(with spaces removed) as key. The encrypted message

$$R?:OZASRY!TZOBE:$$

is obtained. Decrypt the message. ***(5 marks)***

(iii) Let K and L be the following matrices over $\mathbb{F}_{31}$:

$$K = \begin{pmatrix} 2 & 17 \\ 27 & 13 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{F}_{31}), \quad L = \begin{pmatrix} 30 \\ 15 \end{pmatrix} \in \mathrm{Mat}_{2\times 1}(\mathbb{F}_{31}).$$

Let $f : \mathrm{Mat}_{2\times 1}(\mathbb{F}_{31}) \to \mathrm{Mat}_{2\times 1}(\mathbb{F}_{31})$ be the affine transformation given by $f(V) = KV + L$. A message is sent using 2-dimensional affine encryption, as determined by f, with the same correspondence between characters and the field $\mathbb{F}_{31}$ as in (ii). Spaces and characters not in the table are ignored and the message is divided into blocks of length 2. One block in the message is encrypted as EE. Identify the two characters in this block. ***(7 marks)***

2 (i) Let $\mathbb{F} = \mathbb{F}_p$ for a prime number p. Let C be an $[n, k]$-linear code over $\mathbb{F}$ and let $C^\perp$ be the dual code

$$C^\perp = \{v \in \mathbb{F}^n : vx^T = 0 \text{ for all } x \in C\} = \{v \in \mathbb{F}^n : xv^T = 0 \text{ for all } x \in C\}.$$

Let G be a generator matrix for C.

(a) Use the second of the descriptions above to show that $C^\perp$ is an $[n, n-k]$-linear code over $\mathbb{F}$ and G is a parity check matrix for $C^\perp$. ***(7 marks)***

(b) Show that $C \subseteq (C^\perp)^\perp$ and use dimension to deduce that $(C^\perp)^\perp = C$. ***(4 marks)***

(c) Show that C has a parity check matrix. ***(2 marks)***

(ii) Find a parity check matrix H for the $[8, 5]$ linear code C over $\mathbb{F}_2$ that has generator matrix

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

(7 marks)

Find a non-zero word $v \in C^\perp \cap C$, and express v as a linear combination of the rows of G. ***(5 marks)***

3 Let

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

a parity check matrix for the special Hamming code Ham_3 over $\mathbb{F}_2$.

(i) Show that the minimum distance of Ham_3 is 3, stating clearly any result on linearly dependence of columns of parity check matrices that you use. Use the Sphere-Packing Bound to show that Ham_3 is a perfect code. ***(8 marks)***

(ii) A codeword c in Ham_3 is transmitted and 1000010 is received. Explain why at least one error must have occurred. Describe a general method, involving a single matrix multiplication, for the correction of single errors in special Hamming codewords and, on the assumption that a single error has occurred, use this method to identify the codeword c. ***(4 marks)***

(iii) Let $a = 1111111 \in \mathbb{F}_2^7$. Show that $a \in \mathrm{Ham}_3$ and deduce that if $v \in \mathrm{Ham}_3$ has weight d then $v - a \in \mathrm{Ham}_3$ and has weight $7 - d$. ***(3 marks)***

For $d = 0, 1, 2, 3, 4, 5, 6, 7$, let $f(d)$ denote the number of codewords in Ham_3 with weight d. Show that $f(d) = f(7 - d)$ for each d. Determine the value of $f(d)$ for each d. ***(6 marks)***

(iv) Let $c \in \mathrm{Ham}_3$ be of weight 3. How many elements of $\mathbb{F}_2^7$ are there in the Hamming sphere of radius 1 centred on c? How many of these have weight 2 and how many have weight 4? Justify your answer. ***(4 marks)***

4 (i) Let p be a prime number and let $g \in \mathbb{F}_p^*$. Explain what is meant by the *order* of g. Explain what it means to say that g is a *generator* of $\mathbb{F}_p^*$.

(3 marks)

Use the powers of 11 modulo 103 on the data sheet to determine the discrete logarithm of 57 to the base 11 modulo 103. Compute 57^6 in $\mathbb{F}_{103}$ and deduce that 57 is not a generator of $\mathbb{F}_{103}^*$. ***(4 marks)***

(ii) Hermia and Lysander use the keyless cryptosystem of Massey-Omura/Shamir with the prime 103 to exchange messages that can be expressed as elements of $\mathbb{F}_{103}$. Hermia chooses the private key $e_H = 11$ and Lysander chooses the private key $e_L = 13$. Hermia wishes to send a message m to Lysander.

(a) Identify the three integers i, j, k such that $1 \leq i, j, k \leq 102$ and m^i, m^j, m^k are, in order, the three messages transmitted between them. ***(5 marks)***

(b) Use the squares on the data sheet to calculate the three transmitted messages in the case where $m = 10$. ***(4 marks)***

(c) Show that if $b = m^j$ is the second of the three messages transmitted then $b^5 = m$. ***(2 marks)***

(iii) Explain what it means to say that a positive integer is a *Carmichael number*.

(2 marks)

Let $p_1, p_2, \ldots, p_k$ be distinct prime numbers and let $n = p_1 p_2 \ldots p_k$. Show that if $p_i - 1$ divides $n - 1$ for each i then n is a Carmichael number.

(5 marks)

5 (i) (a) Show that if p is a prime of the form $4k-1$ and y is a quadratic residue modulo p, then, in $\mathbb{F}_p$, $y = (y^k)^2$. ***(4 marks)***

Given that 5 is a quadratic residue modulo 19, evaluate 5^k for an appropriate value of k and hence find the two square roots of 5 in $\mathbb{F}_{19}$. ***(3 marks)***

(b) Identify the integers c and d such that $860 \equiv c \bmod 19$, $0 \leq c \leq 18$, $860 \equiv d \bmod 103$ and $0 \leq d \leq 102$. Write down a square root a of c in $\mathbb{F}_{19}$ and a square root b of d in $\mathbb{F}_{103}$. ***(3 marks)***

(c) Let $p = 19$ and let $q = 103$. Use the squares on the data sheet to show that $2p^2 \equiv 1 \bmod q$ and hence find the inverse of 19 modulo 103. Calculate $12q$ modulo p and hence find the inverse of 103 modulo 19. ***(3 marks)***

(d) In the final of a national literary quiz competition for pubs, the Blue Baboon is to play the Orient Calf. The team captains agree to decide on the venue for the final by coin tossing by telephone using quadratic residues modulo pq. The captain of the Blue Baboon team sends 1957 to the Orient Calf and receives the quadratic residue 860 in reply. Determine the pairs $\{\pm x_1\}$ and $\{\pm x_2\}$ of elements of $\mathbb{Z}_{1957}$ from which she must then make a choice. ***(7 marks)***

(ii) Let p and q be prime, let $x_1, x_2 \in \mathbb{Z}$ be such that $0 < x_1, x_2 < pq$ and let h be the highest common factor of $x_1 + x_2$ and pq. Show that if, in $\mathbb{Z}_{pq}$, $x_2 \neq \pm x_1$ and $x_2^2 = x_1^2$ then $h = p$ or $h = q$. ***(5 marks)***

End of Question Paper

MAS345 Codes and Cryptography 2011-12

DATA SHEET

Table for Q1(ii):

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 $\mathbb{F}_{103}$.

$1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$, $8^2 = 64$,
$9^2 = 81$, $10^2 = 100$, $11^2 = 18$, $12^2 = 41$, $13^2 = 66$, $14^2 = 93$, $15^2 = 19$, $16^2 = 50$,
$17^2 = 83$, $18^2 = 15$, $19^2 = 52$, $20^2 = 91$, $21^2 = 29$, $22^2 = 72$, $23^2 = 14$, $24^2 = 61$,
$25^2 = 7$, $26^2 = 58$, $27^2 = 8$, $28^2 = 63$, $29^2 = 17$, $30^2 = 76$, $31^2 = 34$, $32^2 = 97$,
$33^2 = 59$, $34^2 = 23$, $35^2 = 92$, $36^2 = 60$, $37^2 = 30$, $38^2 = 2$, $39^2 = 79$, $40^2 = 55$,
$41^2 = 33$, $42^2 = 13$, $43^2 = 98$, $44^2 = 82$, $45^2 = 68$, $46^2 = 56$, $47^2 = 46$, $48^2 = 38$,
$49^2 = 32$, $50^2 = 28$, $51^2 = 26$, $52^2 = 26$, $53^2 = 28$, $54^2 = 32$, $55^2 = 38$, $56^2 = 46$,
$57^2 = 56$, $58^2 = 68$, $59^2 = 82$, $60^2 = 98$, $61^2 = 13$, $62^2 = 33$, $63^2 = 55$, $64^2 = 79$,
$65^2 = 2$, $66^2 = 30$, $67^2 = 60$, $68^2 = 92$, $69^2 = 23$, $70^2 = 59$, $71^2 = 97$, $72^2 = 34$,
$73^2 = 76$, $74^2 = 17$, $75^2 = 63$, $76^2 = 8$, $77^2 = 58$, $78^2 = 7$, $79^2 = 61$, $80^2 = 14$,
$81^2 = 72$, $82^2 = 29$, $83^2 = 91$, $84^2 = 52$, $85^2 = 15$, $86^2 = 83$, $87^2 = 50$, $88^2 = 19$,
$89^2 = 93$, $90^2 = 66$, $91^2 = 41$, $92^2 = 18$, $93^2 = 100$, $94^2 = 81$, $95^2 = 64$, $96^2 = 49$,
$97^2 = 36$, $98^2 = 25$, $99^2 = 16$, $100^2 = 9$, $101^2 = 4$, $102^2 = 1$.

The list below shows the powers of 11 in $\mathbb{F}_{103}$.

$11^1 = 11$, $11^2 = 18$, $11^3 = 95$, $11^4 = 15$, $11^5 = 62$, $11^6 = 64$, $11^7 = 86$,
$11^8 = 19$, $11^9 = 3$, $11^{10} = 33$, $11^{11} = 54$, $11^{12} = 79$, $11^{13} = 45$, $11^{14} = 83$,
$11^{15} = 89$, $11^{16} = 52$, $11^{17} = 57$, $11^{18} = 9$, $11^{19} = 99$, $11^{20} = 59$, $11^{21} = 31$,
$11^{22} = 32$, $11^{23} = 43$, $11^{24} = 61$, $11^{25} = 53$, $11^{26} = 68$, $11^{27} = 27$, $11^{28} = 91$,
$11^{29} = 74$, $11^{30} = 93$, $11^{31} = 96$, $11^{32} = 26$, $11^{33} = 80$, $11^{34} = 56$, $11^{35} = 101$,
$11^{36} = 81$, $11^{37} = 67$, $11^{38} = 16$, $11^{39} = 73$, $11^{40} = 82$, $11^{41} = 78$, $11^{42} = 34$,
$11^{43} = 65$, $11^{44} = 97$, $11^{45} = 37$, $11^{46} = 98$, $11^{47} = 48$, $11^{48} = 13$, $11^{49} = 40$,
$11^{50} = 28$, $11^{51} = 102$, $11^{52} = 92$, $11^{53} = 85$, $11^{54} = 8$, $11^{55} = 88$, $11^{56} = 41$,
$11^{57} = 39$, $11^{58} = 17$, $11^{59} = 84$, $11^{60} = 100$, $11^{61} = 70$, $11^{62} = 49$, $11^{63} = 24$,
$11^{64} = 58$, $11^{65} = 20$, $11^{66} = 14$, $11^{67} = 51$, $11^{68} = 46$, $11^{69} = 94$, $11^{70} = 4$,
$11^{71} = 44$, $11^{72} = 72$, $11^{73} = 71$, $11^{74} = 60$, $11^{75} = 42$, $11^{76} = 50$, $11^{77} = 35$,
$11^{78} = 76$, $11^{79} = 12$, $11^{80} = 29$, $11^{81} = 10$, $11^{82} = 7$, $11^{83} = 77$, $11^{84} = 23$,
$11^{85} = 47$, $11^{86} = 2$, $11^{87} = 22$, $11^{88} = 36$, $11^{89} = 87$, $11^{90} = 30$, $11^{91} = 21$,
$11^{92} = 25$, $11^{93} = 69$, $11^{94} = 38$, $11^{95} = 6$, $11^{96} = 66$, $11^{97} = 5$, $11^{98} = 55$,
$11^{99} = 90$, $11^{100} = 63$, $11^{101} = 75$, $11^{102} = 1$.

TURN OVER

The list below shows the inverses in $\mathbb{Z}_{102}$.

$1^{-1} = 1,$	$5^{-1} = 41,$	$7^{-1} = 73,$	$11^{-1} = 65,$	$13^{-1} = 55,$	$19^{-1} = 43,$
$23^{-1} = 71,$	$25^{-1} = 49,$	$29^{-1} = 95,$	$31^{-1} = 79,$	$35^{-1} = 35,$	$37^{-1} = 91,$
$41^{-1} = 5,$	$43^{-1} = 19,$	$47^{-1} = 89,$	$49^{-1} = 25,$	$53^{-1} = 77,$	$55^{-1} = 13,$
$59^{-1} = 83,$	$61^{-1} = 97,$	$65^{-1} = 11,$	$67^{-1} = 67,$	$71^{-1} = 23,$	$73^{-1} = 7,$
$77^{-1} = 53,$	$79^{-1} = 31,$	$83^{-1} = 59,$	$89^{-1} = 47,$	$91^{-1} = 37,$	$95^{-1} = 29,$
$97^{-1} = 61,$	$101^{-1} = 101.$				