Data provided: Data Sheet

MAS345

The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS Spring Semester 2013–2014

Codes and Cryptography 2 hours 30 minutes

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

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

$$H_1 = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}$$

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

$$H_2 = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

(i) (a) Let $a = a_1a_2a_3a_4a_5a_6 \in C_1$. Show that a_6 is determined by the other five bits of a. Find $x, y \in \mathbb{F}_7$ such that $64331x \in C_1$ and $64331xy \in C_2$. ***(5 marks)***

(b) Let $u, v \in \mathbb{F}_7$ be such that $u \neq v$. Show that, for $a_1, a_2, a_3, a_4 \in \mathbb{F}_7$, $a_1a_2a_3a_4uv$ and $a_1a_2a_3a_4vu$ cannot both be codewords in C_1. ***(3 marks)***

(c) Show that if $a_1a_2a_3a_4a_5a_6 \in C_1$ then $a_2a_3a_4a_5a_6a_1 \in C_1$. ***(2 marks)***

(d) Show that no two columns of H_2 are linearly dependent and hence find the minimum distance of C_2. State clearly any result relating minimum distance to linear dependence of columns that you use. ***(5 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 $a = a_1a_2a_3 \ldots a_i \ldots a_n \in C$ and let $b = a_1a_2 \ldots b_i \ldots a_n$ be obtained from a by a single error which occurs in the ith bit. Show that $Hb^T = (b_i - a_i)h_i$. ***(3 marks)***

(iii) A codeword c from C_2 is transmitted, an error occurs in one bit and $r = 3104566$ is received. Use (ii) to identify c. ***(4 marks)***

Show also that if v is obtained from c by transposing the first two bits and also transposing the fourth and fifth bits then $v \in C_2$. Deduce that there exists $s \in \mathbb{F}_7^7$ such that s can be obtained from two different codewords in C_2 by transposing two digits. ***(3 marks)***

2 (i) Let F be an alphabet and $n \geq 2$ be an integer. Let r be an integer with $0 \leq r \leq n$ and let $c \in F^n$. Let j be an integer such that $0 \leq j \leq r$. Show that the number of elements in the Hamming sphere $S(c, r)$ of radius r centred at c is

$$\sum_{j=0}^{r} (q-1)^j \binom{n}{j}.$$

(3 marks)

(ii) Write down, without proof, the *Sphere-Packing Bound* for an (n, M, d)-code C over an alphabet F with q elements and explain what it means to say that C is *perfect*. ***(3 marks)***

(iii) Let

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

which is a parity check matrix for the special Hamming code Ham_3. Let D be the matrix obtained from H by interchanging the first and third rows of H. Thus D is in reduced row echelon form and is a generator matrix for the dual code $\mathrm{Ham}_3^{\perp}$.

(a) Write down, without proof, the dimension and minimum distance of Ham_3 and show that Ham_3 is perfect. ***(5 marks)***

(b) Write down, without proof, the dimension of $\mathrm{Ham}_3^{\perp}$. List all the non-zero elements of $\mathrm{Ham}_3^{\perp}$. Hence find the minimum distance of $\mathrm{Ham}_3^{\perp}$ and show that $\mathrm{Ham}_3^{\perp}$ is not perfect. ***(6 marks)***

(c) Using D as a generator matrix, find a matrix E that is a parity check matrix for $\mathrm{Ham}_3^{\perp}$ and a generator matrix of Ham_3. ***(5 marks)***

(d) Show that $\mathrm{Ham}_3^{\perp} \subseteq \mathrm{Ham}_3$ and find a codeword r of Ham_3 that does not belong to $\mathrm{Ham}_3^{\perp}$. ***(3 marks)***

3 (i) The title of a novel is encrypted using the one-time pad method modulo 31, using capital letters, five punctuation marks and the correspondence with $\mathbb{F}_{31}$ in the table on the provided data sheet. Spaces and any punctuation marks not shown in the table are deleted. The key is the passage beginning

I TURNS TO LENNIE AND SAYS : 'JUMP IN'

from page 39 of ISBN 0330241443. The encrypted title

: CAWUS : Z

is obtained. Decrypt the title. ***(3 marks)***

The title is further encrypted by encrypting : CAWUS : Z using the Vigenère method, modulo 31 and with the same correspondence as above, with key HILARY. Which letter appears three times in the final encrypted title? ***(3 marks)***

(ii) A pair of days in July 2014, the dth and the eth, is written as the column $(d\ e)^T$ and encrypted using 2-dimensional affine encryption modulo 31, with the transformation $f : \mathbb{F}_{31}^2 \to \mathbb{F}_{31}^2$ given by $f(V) = KV + L$, where

$$K = \begin{pmatrix} 4 & 1 \\ 7 & 10 \end{pmatrix} \text{ and } L = \begin{pmatrix} 25 \\ 21 \end{pmatrix}.$$

The result of the encryption is $(5\ 24)^T$. Find d and e. ***(5 marks)***

(iii) In its initial position, a drum in a simplified Enigma machine performs the permutation

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

Find the permutation $2 * \alpha$ performed by the drum after two rotations. ***(2 marks)***

(iv) Compute 64^{17} in $\mathbb{F}_{103}$ and write down the order of 64 in $\mathbb{F}_{103}^*$. You may use the squares in $\mathbb{F}_{103}$ shown on the data sheet. ***(3 marks)***

3 (continued)

(v) The secret society Cockatrice uses the keyless cryptosystem of Massey-Omura/Shamir to exchange messages that are expressed as elements of $\mathbb{F}_p$ for some prime p.

(a) Let $p = 103$. Explain why no member of Cockatrice has secret key 69. ***(1 mark)***

(b) Ermintrude and Florence are two members of Cockatrice with secret keys $e_E = 5$ and $e_F = 7$ respectively and $p = 103$. If Ermintrude wishes to send the message 64 to Florence what are the three messages that pass between them? You may use the inverses in $\mathbb{Z}_{102}$ shown on the data sheet. ***(4 marks)***

(c) Dylan and Zebedee are two members of Cockatrice with secret keys e_D and e_Z respectively. Dylan wishes to send the message M to Zebedee. Let r be the order of M in $\mathbb{F}_p^*$. Show that the middle of the three messages that pass between them is equal to M if and only if $e_D e_Z - 1$ is a multiple of r. ***(3 marks)***

Give an example where the middle message is M but e_D and e_Z are not inverses of each other modulo $p - 1$. ***(1 mark)***

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

It is given that 18 is a quadratic residue modulo 23. Evaluate 18^6, modulo 23, and hence find the two square roots of 18 in $\mathbb{F}_{23}$. ***(2 marks)***

(ii) Let $p = 23$, let $q = 103$ and let $n = pq = 2369$. Cockatrice and its rival Iguanodon are to hold a summit meeting and agree to decide on the venue by coin tossing by telephone using quadratic residues modulo products of two primes. Iguanodon sends 2369 to the Cockatrice and receives the quadratic residue 1858 in reply. Determine the pairs $\{\pm x_1\}$ and $\{\pm x_2\}$ of elements of $\mathbb{Z}_{2369}$ from which Iguanodon must then make a choice. ***(7 marks)***

You may find the following congruences helpful:

$$\begin{aligned} 1858 &\equiv 18 \bmod 23, \\ 1858 &\equiv 4 \bmod 103, \\ 103 \times 21 &\equiv 1 \bmod 23, \\ 23 \times 9 &\equiv 1 \bmod 103, \\ 16583 &\equiv 0 \bmod 2369. \end{aligned}$$

(iii) 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)***

(iv) Let $n = 29341 = 13 \times 37 \times 61$. Show that n is a Carmichael number, stating clearly any result that you use. ***(4 marks)***

It is given that $2^{14670} \equiv 29340 \bmod 29341$, $2^{7335} \equiv 26424 \bmod 29341$, $3^{14670} \equiv 1 \bmod 29341$ and $3^{7335} \equiv 22569 \bmod 29341$.

Is 29341 a strong pseudoprime to the base 2? Is 29341 a strong pseudoprime to the base 3? Justify your answers. ***(3 marks)***

End of Question Paper

MAS345 Codes and Cryptography 2013-14

DATA SHEET

Table for Q3(i)(a):

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 inverses in $\mathbb{Z}_{102}$.

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