The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2018–2019**

Codes and Cryptography **2 hours 30 minutes**

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

Please leave this exam paper on your desk
Do not remove it from the hall

Registration number from U-Card (9 digits)
to be completed by student

Blank

1 (i) Let $C \subseteq \mathbb{F}_2^6$ be the linear code over $\mathbb{F}_2$ generated by $(1,1,0,0,1,1)$, $(0,1,0,1,0,0)$, $(1,0,1,1,0,1)$ and $(1,0,0,1,1,1)$.

(a) Convert the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathrm{M}_{4\times 6}(\mathbb{F}_2)$$

into *reduced row echelon form*. Write down a generator matrix for C in *standard form* i.e. a matrix of the form $(I_k|*)$, and use that to determine if $(1,1,0,1,0,1)$ is a codeword in C. Finally, write down the dimension of C and the size of C. ***(6 marks)***

(b) Find a *parity check matrix* for C. ***(4 marks)***

(ii) Let C_1 and C_2 be codes over an alphabet set F, and let C be the code whose codewords are strings c_1c_2 for arbitrary $c_1 \in C_1$ and $c_2 \in C_2$. Suppose C_1, C_2 and C have parameters (n_1, M_1, d_1), (n_2, M_2, d_2) and (n, M, d) respectively.

(a) Write down expressions for n and M in terms of n_1, n_2 and M_1, M_2. Also, write down a relation between $d(x_1, y_1)$, $d(x_2, y_2)$ and $d(x_1x_2, y_1y_2)$ for $x_1, y_1 \in C_1$, $x_2, y_2 \in C_2$. ***(2 marks)***

(b) Prove that $d = d_1 + d_2$. Deduce that if both d_1 and d_2 are odd then $t = t_1 + t_2$ where t_1, t_2 and t are the error correcting indices of C_1, C_2 and C repectively. ***(3 marks)***

2 (i) Let F be an alphabet with q letters and let $n \geq 2$ be an integer.

(a) Show that if $c \in F^n$ and $0 \leq r \leq n$, then the Hamming sphere $S(c, r)$ contains

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

words. ***(2 marks)***

(b) Write down, without proof, the *Sphere Packing Bound* for an (n, M, d)-code C over F. When does equality hold? ***(2 marks)***

(c) Show that there does not exist a $[13, 8, 5]$-linear code over $\mathbb{F}_3$. ***(2 marks)***

(ii) Let C be the $[8, 4]$-linear code over $\mathbb{F}_2$ with generator matrix

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

Calculate GG^T where G^T is the transpose of G, and show that C is its own dual i.e. $C = C^{\perp}$. ***(4 marks)***

(iii) In this part $\mathbb{F}$ is the field of integers modulo some prime number. You can use basic results from linear algebra and the existence of a parity check matrix without proof.

Let M be an $m \times n$ matrix over $\mathbb{F}$ and let $V \subset \mathbb{F}^n$ be the null space of M. Assume that $m < n$. By considering the first $m + 1$ columns of M or otherwise, show that the minimum distance $d(V)$ of V satisfies the inequality $d(V) \leq m + 1$.

Hence, or otherwise, show that if C is an $[n, k, d]$-linear code over $\mathbb{F}$ with error-correcting index t then

$$t \leq \left\lfloor \frac{n-k}{2} \right\rfloor.$$

(5 marks)

3 (i) The *X-method* for encrypting messages proceeds as follows. Let $(a_1, a_2, \ldots, a_n)$ be the alphanumeric conversion of an n-letter word. Then the encrypted word has alphanumeric conversion $(b_1, b_2, \ldots, b_n)$ where $b_1 = 3a_1$ and

$$b_i = a_i + a_{i-1} \quad \text{when } i > 1.$$

The alphanumeric conversion modulo 26 is given below:

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

(a) Encrypt CODES. ***(1 mark)***

(b) A 6-letter word is encrypted using the *X-method* followed by a Vigenere encryption with key MAS. The encrypted word is

WAJ JFH.

The space is for ease of reading. Decrypt. ***(4 marks)***

(c) A two step encryption process is applied to 3-letter words by first applying the *X-method* followed by a Vigenere encryption with key MAS. Write down—no justification required!—matrices

$$\Lambda = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \quad \text{and} \quad \boldsymbol{\lambda} = \begin{pmatrix} * \\ * \\ * \end{pmatrix}$$

which express this two step encryption as a single affine transformation $f : \mathbb{Z}_{26}^3 \to \mathbb{Z}_{26}^3$ given by $f(\boldsymbol{x}) = \Lambda\boldsymbol{x} + \boldsymbol{\lambda}$. ***(2 marks)***

(ii) Alpha and Beta are members of a secret organisation who communicate using the *Massey-Omura/Shamir keyless cryptosystem* with an agreed large prime number p. Alpha wishes to send to Beta a message M which is a non-zero element of $\mathbb{F}_p$. Describe the three messages that pass between Alpha and Beta, and indicate how Beta decrypts. You do not have to justify why the process works but you must set out clearly any notation that is introduced. ***(3 marks)***

Let $p = 31$ be the agreed prime number. Snooper, a third member of the organisation, intercepts the following three messages between Alpha and Beta in *sequence*: 4; 4; 2.

(a) Write down the order of 4 in $\mathbb{F}_{31}^*$. ***(1 mark)***

(b) Suppose Beta's chosen key is b with $0 < b < 30$. Determine the possible values of b, and determine the message Alpha sent to Beta. ***(4 marks)***

4 Let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_{13}$.

(i) Compute x^2, x^3 and $x^3 + x + 1$ for all $x \in \mathbb{F}_{13}$. Hence find all the points on $\mathcal{E}$. (You should find that there are eighteen points including the point at infinity.) ***(6 marks)***

(ii) You should find that $(5, 1)$ and $(12, 8)$ are two points on $\mathcal{E}$. *By inspection* or otherwise, write down the equation of the line through $(5, 1)$ and $(12, 8)$ and write down the third point where this line intersects the elliptic curve $\mathcal{E}$. Hence calculate $(5, 1) + (12, 8)$. ***(3 marks)***

(iii) Calculate the point $2(0, 12)$ in $\mathcal{E}$. ***(3 marks)***

(iv) A secret organisation including Alpha and Beta uses the ElGamal cryptosystem with the elliptic curve $\mathcal{E}$ over $\mathbb{F}_{13}$ as above and a point $P \in \mathcal{E}$ of large order. Beta's private key is 2. He receives the message

$$\big((0, 12), (12, 5)\big) \in \mathcal{E} \times \mathcal{E}$$

from Alpha. Decrypt. The answers to parts (ii) and (iii) are particularly relevant. ***(3 marks)***

End of Question Paper