The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2015–2016**

Codes and Cryptography **2 hours 30 minutes**

Attempt all the questions. The allocation of marks is shown in brackets.
There is no separate data sheet provided.

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 F be a finite alphabet set, and let n be a positive integer.

(a) Define the Hamming distance $d(x, y)$ between two words $x, y \in F^n$. Prove the *triangle inequality*: If $x, y, z \in F^n$ then

$$d(x, z) \leq d(x, y) + d(y, z).$$

(4 marks)

(b) What is the minimum distance of a code C of length n over F? State, without proof, the error detection and error correction properties of C if it has minimum distance d. ***(3 marks)***

(c) For each word $x \in F^n$, let $xx \in F^{2n}$ denote the word formed by repeating x. Thus if $x = x_1x_2 \dots x_n$, then

$$xx := x_1x_2 \dots x_nx_1x_2 \dots x_n.$$

Now let C be an (n, M, d)-code over F and let C' be the code

$$C' := \{xx \,:\, x \in C\}$$

of length $2n$ over F. Show that C' has error correcting index $d - 1$. ***(3 marks)***

(ii) Let C be the linear code over $\mathbb{F}_2$ of length 7 generated by the words $(1, 1, 0, 0, 1, 1, 0)$, $(0, 1, 1, 0, 0, 0, 1)$, $(0, 0, 0, 1, 1, 0, 1)$ and $(1, 0, 1, 1, 0, 1, 0)$.

(a) Show that the matrix

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

is a generator matrix of C. How many codewords are there in C? Find all codewords in C of even weight. ***(7 marks)***

(b) Find a parity check matrix for C. ***(8 marks)***

2 (i) Let F be an alphabet with q elements 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. ***(3 marks)***

(b) Write down, without proof, the *Sphere Packing Bound* for an (n, M, d)-code C over F. When does equality hold? ***(3 marks)***

(c) Show that there does not exist an $[11, 6, 5]$-linear code over $\mathbb{F}_2$. Is there a $[7, 4, 4]$-linear code over $\mathbb{F}_2$? Justify your answer. You may use general results proved in the lectures provided they are clearly stated. ***(5 marks)***

(ii) (a) How is the minimum distance of a linear code is related to weights of its codewords? State a result which relates the minimum distance of a linear code to linear dependence of columns of a parity check matrix. ***(3 marks)***

(b) Let $p \geq 5$ be a prime number and let a, b, c be three distinct elements of $\mathbb{F}_p$. Thus $b - a$, $c - b$ and $a - c$ are all invertible. Show that the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{pmatrix}$$

has rank 3. ***(4 marks)***

(c) Let C be the linear code over $\mathbb{F}_{11}$ with parity check matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 \end{pmatrix}.$$

Find a codeword of weight 4 and determine the minimum distance of C. ***(7 marks)***

3 (i) A team and a venue for a bat and ball game is drawn up and then encrypted using the alphanumeric conversion modulo 26 given below, and a variety of techniques.

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) Each name on the list is encrypted using a Caesar encryption with key F followed by a Vigenere encryption with key $LORDS$. The first encrypted name is $WTRIPATN$. Decrypt. ***(4 marks)***

(b) The venue, a four letter word, is encrypted using an affine transformation $f : \mathbb{Z}_{26}^4 \to \mathbb{Z}_{26}^4$ given by $f(\boldsymbol{x}) = K\boldsymbol{x} + L$ where

$$K = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 0 & 3 & 5 & 7 \\ 0 & 0 & 5 & 7 \\ 0 & 0 & 0 & 7 \end{pmatrix} \quad \text{and} \quad L = \begin{pmatrix} 1 \\ 3 \\ 5 \\ 7 \end{pmatrix}.$$

The encrypted word is $ZNEG$. Decrypt. ***(4 marks)***

(ii) Agnew and Boycott are members of a society who agree to use the ElGamal encryption method with the prime 17 and the generator 3. Boycott's secret key is 6.

(a) What is Boycott's public key? ***(2 marks)***

(b) Agnew sends a message, encrypting 7. The encrypted message has the form $(11, x)$ where $x \in \mathbb{F}_{17}$. Identify x. ***(5 marks)***

(c) Agnew sends a second encrypted message $(14, 6)$ to Boycott. Decrypt the message. ***(5 marks)***

(d) Agnew sends a third message m to Boycott and notices that the encrypted message is (m, m). Determine all possible m. ***(5 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.) ***(10 marks)***

(ii) Your list of points on $\mathcal{E}$ should include $(12, 8)$. Calculate the point $2(12, 8)$ on $\mathcal{E}$. ***(5 marks)***

(iii) A secret organisation including Guy and Fawkes uses the Menezes-Vanstone cryptosystem with the elliptic curve $\mathcal{E}$ over $\mathbb{F}_{13}$ as above and a generator, which you are not given, as the group key. Guy wants to set up a meeting with Fawkes on $d/m/2016$ i.e. the d-th day of the m-th month with $1 \leq d \leq 12$. (Guy refuses to work after the first twelve days of every month!) The message $(d, m) \in \mathbb{F}_{13}^2$ is then sent to Fawkes using Fawkes's public key.

Fawkes receives the message

$$\big((12, 8), (3, 9)\big) \in \mathcal{E} \times \mathbb{F}_{13}^2.$$

Fawkes's private key is 2. Determine the secret date. ***(6 marks)***

(iv) Let $P := (1, 4)$. You are given that $2P = (8, 12)$, $4P = (11, 11)$ and $8P = (4, 2)$. Show that P has order 18. ***(4 marks)***

End of Question Paper