The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2017–2018**

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 In this question $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ is the field of integers modulo 7.

(i) The Seven Hills University Registration Number (SHURN) is a code of length 6 over $\mathbb{F}_7$ with codewords $a_1a_2a_3 \dots a_6$ satisfying the relation

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 = 0.$$

You may assume that SHURN is a linear code.

(a) Write down, without proof, the dimension of SHURN and the number of valid SHURNs. ***(2 marks)***

(b) Find $a, b, c, d, e \in \mathbb{F}_7$ so that

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & 0 & 0 & b \\ 0 & 0 & 1 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & d \\ 0 & 0 & 0 & 0 & 1 & e \end{pmatrix}$$

is a generator matrix for SHURN. ***(2 marks)***

(c) State, without proof, a relation between weights of non-zero codewords and the minimum distance of a linear code. Hence, or otherwise, determine the minimum distance of SHURN. ***(3 marks)***

(ii) Let C be the linear code of length 5 over $\mathbb{F}_7$ with generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \in \mathrm{M}_{3\times 5}(\mathbb{F}_7).$$

(a) Convert G into *row reduced echelon form.* ***(2 marks)***

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

(c) Determine the minimum distance of C. ***(2 marks)***

2 (i) The name of an event happening in June–July 2018 is encrypted using a Vigenere encryption with key US and then using an affine encryption $m \to 9m$. The alphanumeric conversion modulo 26 given below is used in the encryption process.

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) The process yields the word $OCVBZYWL$. Identify the event. ***(2 marks)***

(b) Determine matrices

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

such that the above two step encryption process (applied to blocks of length 2) can be expressed as a single affine transformation $f : \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2$ given by $f(\boldsymbol{x}) = \Lambda\boldsymbol{x} + \boldsymbol{\lambda}$. ***(2 marks)***

(ii) Ant and Dec are members of an organisation that uses the *El-Gamal encryption method* with prime 101 and generator 3. Dec's secret key is 8.

(a) What is Dec's public key? ***(1 mark)***

(b) Ant wishes to send the message 11 to Dec choosing the supplementary key 9. What is the encrypted message? ***(2 marks)***

(c) Dec receives a second message $(17, 18)$ from Ant. Decrypt. ***(3 marks)***

(d) Ant and Dec are planning a surprise party. Dec, who is in charge of the guest list, encrypts the number of guests and sends the message $(2, 2)$ to Ant. Unfortunately, Ant has forgotten his secret key and asks Dec to be more helpful. Dec replies by sending the encrypted message $(61, 61)$. Show that if Ant's secret key is a then

$$\left(\frac{61}{2}\right)^{a-1} = 1.$$

Determine Ant's secret key given that it is known to be in the range between 10 and 50. ***(5 marks)***

3 Throughout this question $\mathbb{F}$ denotes the field of integers modulo 11 and $\mathcal{E}$ is the elliptic curve $y^2 = x^3 + 2x + 4$ over $\mathbb{F}$.

(i) Compute x^2, x^3 and $x^3 + 2x + 4$ for all $x \in \mathbb{F}$. Hence find all the points on $\mathcal{E}$. (You should find that there are seventeen points including the point at infinity.) ***(5 marks)***

(ii) A secret organisation including Messi and Ronaldo uses the Menezes–Vanstone cryptosystem with the elliptic curve $\mathcal{E}$ over $\mathbb{F}$ as above and the generator $(7, 3)$.

(a) Messi's secret key is 3. He receives the message

$$\big((3, 2), (5, 4)\big) \in \mathcal{E} \times \mathbb{F}^2$$

from Ronaldo. Decrypt. ***(7 marks)***

(b) Ronaldo sends the encrypted message

$$\big((3, 2), (7, 8)\big) \in \mathcal{E} \times \mathbb{F}^2$$

to Pogba, a third member of the organisation. Messi, who had finished decrypting his own message from Ronaldo, sees the encrypted message meant for Pogba. Explain how Messi can figure out—in a matter of minutes—that the supplementary key used was $k = 6$. If Pogba's public key is $(9, 5)$ and given that $6(9, 5) = (6, 10)$, decrypt Ronaldo's message to Pogba. ***(3 marks)***

End of Question Paper