The University Of Sheffield.

**SCHOOL OF MATHEMATICS AND STATISTICS** **Spring Semester 2016–2017**

**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) The Sheffield University Registration Number (SURN) is a code of length 9 over $\mathbb{Z}_{10} = \{0, 1, \ldots, 9\}$. The codewords are words $a_1a_2a_3 \ldots a_9$ where each $a_i \in \mathbb{Z}_{10}$ and

$$a_1 + 3a_2 + 7a_3 + 9a_4 + a_5 + 3a_6 + 7a_7 + 9a_8 + a_9 = 0.$$

(a) Find two SURNs of the form 14*abababa*. ***(3 marks)***

(b) Given two SURNs $a_1a_2 \ldots a_9$ and $b_1b_2 \ldots b_9$, and a letter $x \in \mathbb{Z}_{10}$, explain why the word $c_1c_2 \ldots c_9$ where

$$c_1 = a_1 + xb_1,\ c_2 = a_2 + xb_2,\ \ldots,\ c_9 = a_9 + xb_9$$

is a valid SURN. Identify the SURNs 00001111? and 12345678? with missing last digits, and write down five different SURNs of the form 1234????2. ***(7 marks)***

(ii) Let $C$ be the binary linear code of length 7 with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \in \mathrm{M}_{4\times 7}(\mathbb{F}_2).$$

(a) Find a parity check matrix for $C$ and determine the minimum distance of $C$. ***(12 marks)***

(b) A word in $C$ was transmitted and the word 1110111 was received with a possible error at one bit. Determine the correct codeword. ***(3 marks)***

**2** This question concerns binary words of length $n$ where $n \geq 2$ is a fixed integer.

(i) Briefly explain what is meant by the terms *Hamming distance* and *weight* for word(s) in $\mathbb{F}_2^n$, and describe how the two are related. State the triangle inequality for the Hamming distance and deduce that

$$\mathrm{wt}(x+y) \leq \mathrm{wt}(x) + \mathrm{wt}(y)$$

for all $x, y \in \mathbb{F}_2^n$ where wt denotes weight. ***(5 marks)***

(ii) Show that if $c \in \mathbb{F}_2^n$ and $0 \leq r \leq n$, then the Hamming sphere $S(c, r)$ contains $\displaystyle\sum_{j=0}^{r} \binom{n}{j}$ words. ***(3 marks)***

(iii) Write down, without proof, the *Sphere Packing Bound* for an $(n, M, d)$-code $C$ over $\mathbb{F}_2$. When does equality hold? Deduce that there is no $[12, 7, 5]$-linear code over $\mathbb{F}_2$. ***(5 marks)***

(iv) Let $C$ be an $[n, k, d]$ linear code over $\mathbb{F}_2$ and parity check matrix $H$. Write down, without proof, a relation between the columns of $H$ and the minimum distance $d$. Deduce that the error-correcting index $t$ of $C$ satisfies the inequality $t \leq \left\lfloor \dfrac{n-k}{2} \right\rfloor$. ***(4 marks)***

(v) Let $e = 10\ldots0 \in \mathbb{F}_2^n$ be the word with first letter 1 and remaining letters all 0. Determine the possible values of $\mathrm{wt}(x+e) - \mathrm{wt}(x)$ for $x \in \mathbb{F}_2^n$. ***(2 marks)***

Now let $d$ be an even positive integer, and assume that there exists a binary code of length $n$, size $M$ and minimum distance $d$. Show that there exists a binary $(n, M, d)$ code whose codewords all have even weight. ***(6 marks)***

**3** Secret agents Codes and Cryptography use the alphanumeric conversion modulo 26 given below and a variety of encryption techniques for exchanging secrets.

| 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 |

(i) Codes and Cryptography agree to meet up in a popular coffee shop. The location of the coffee shop is encrypted using a Vigenere encryption with key $GREEN$, followed by a second Vigenere encryption with key $TEA$. The process yields the word $AMSLDNSTP$. Identify the location.

***(4 marks)***

(ii) So that agent MAS345 does not find out, Codes and Cryptography encrypt the topic for discussion using an affine transformation $f : \mathbb{Z}_{26}^2 \to \mathbb{Z}_{26}^2$ given by $f(\boldsymbol{x}) = \Lambda\boldsymbol{x} + \boldsymbol{\lambda}$ where

$$\Lambda = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix} \quad \text{and} \quad \boldsymbol{\lambda} = \begin{pmatrix} 11 \\ 13 \end{pmatrix}.$$

The encrypted word is $KMVT$. Decrypt. ***(5 marks)***

(iii) Cryptography needs to tell Codes which bus to take from the city centre. They agree to use the *Massey-Omura/Shamir keyless cryptosystem* with the prime 101. Codes chooses 7 as her private key.

Codes receives a text from Cryptography with the number 16. Following Codes' reply, she gets a second text with the message 81. What was Codes' initial reply, and which bus must she take? ***(5 marks)***

(iv) The organisation of which Codes and Cryptography are part of uses the *Diffie-Hellman key exchange* system with prime 101 and generator 2.

Let Codes' public key be 59, and set $a$ to be Codes' private key. Thus $1 \leq a \leq 100$ and $2^a = 59$ in $\mathbb{Z}_{101}$.

(a) What must $59^{50} \in \mathbb{Z}_{101}$ be if $a$ is even? Calculate $59^{50}$ and determine if $a$ is even or odd. ***(3 marks)***

(b) Calculate $2^{a-1}$ and show that 4 must divide $a - 1$. ***(3 marks)***

(c) Show that $a - 4$ must be a multiple of 25. ***(3 marks)***

(d) What is Codes' private key? ***(2 marks)***

**4** Let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_{17}$.

(i) Compute $x^2$, $x^3$ and $x^3 + x + 1$ for all $x \in \mathbb{F}_{17}$. Hence find all the points on $\mathcal{E}$. (You should find that there are eighteen points including the point at infinity.) ***(10 marks)***

(ii) A secret organisation including Root and Stokes uses the ElGamal cryptosystem with the elliptic curve $\mathcal{E}$ over $\mathbb{F}_{17}$ as above and a point $P \in \mathcal{E}$ of order 18.

(a) Explain how Stokes would send a message $M \in \mathcal{E}$ to Root given that Root's public key is $P_R \in \mathcal{E}$. If Root's private key is $r$, how would he decipher the message? ***(5 marks)***

(b) Root's private key is 2. He receives the message

$$\big((6,6),(13,1)\big) \in \mathcal{E} \times \mathcal{E}$$

from Stokes. Decrypt. ***(10 marks)***

## End of Question Paper