The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2020–2021**

Codes and Cryptography

This is an open book exam.

Answer all questions. 40 marks total.

You can work on the exam during the 24 hour period starting from 10am (BST), and you must submit your work within 3 hours of accessing the exam paper or by the end of the 24 hour period (whichever is earlier).

Late submission will not be considered without extenuating circumstances. *Calculations should be performed by hand. A university-approved calculator may be used. The use of any other calculational device, software or service is not permitted. To gain full marks, you will need to show your working.*

By uploading your solutions you declare that your submission consists entirely of your own work, that any use of sources or tools other than material provided for this module is cited and acknowledged, and that no unfair means have been used.

1 Let C be a linear code over $\mathbb{F}_{11}$, with parity check matrix

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

(Recall that X stands for 10 (mod 11).)

(i) What is the minimum distance of C? Justify your answer, and produce a codeword of minimum non-zero weight. ***(3 marks)***

(ii) Suppose that $12a358bX10$ belongs to C. Find a and b, hence write down this codeword. ***(4 marks)***

(iii) Suppose that $\mathbf{y} = 1231231231$ is Hamming distance 1 from a codeword $\mathbf{c} \in C$. Find $\mathbf{c}$. ***(4 marks)***

(iv) What is the dimension of C? How many codewords does C contain? Find a generator matrix G for C. ***(4 marks)***

(v) How many ISBN-10 codewords do not belong to C? If $\mathbf{w}$ is such a word, show that for any $\mathbf{c} \in C$, $d(\mathbf{c}, \mathbf{w}) > 1$. Hence or otherwise, show that C is not a perfect code. ***(5 marks)***

2 (i) 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

Caesar encryption has been used to produce a ciphertext

RQXYNHXDURTNCQNNGJV.

Recover the plaintext, then use it as a one time pad to encrypt the message

SHEFFIELDUNIVERSITY. ***(4 marks)***

(ii) In 1952 it was discovered that $p = 2^{607} - 1$ is prime. Alice and Bob decide to use this prime for Diffie-Hellman key exchange. They also need a generator g for $\mathbb{F}_p^*$, but you should not attempt to find one! If Alice has secret key $a = 2^{303} - 1$ and Bob has secret key $b = 2^{303} + 1$ (possibly not a good idea), what is their shared key? ***(4 marks)***

(iii) Let $\mathcal{E} : y^2 = x^3 - x$, an elliptic curve over the field $\mathbb{F}_{19}$.

(a) Without actually finding all the points on $\mathcal{E}$, explain why the number of points $|\mathcal{E}| \leq 39$. ***(2 marks)***

(b) Write down all the points P on $\mathcal{E}$ such that $2P = \mathcal{O}$, not forgetting $\mathcal{O}$ itself. For later, you may assume that they form a subgroup of $\mathcal{E}$, and Lagrange's theorem that the size of a finite group is divisible by the size of any subgroup. ***(1 mark)***

(c) Find a point $Q = (x, y)$ on $\mathcal{E}$ such that $x = 5$. By repeated doubling, check that $4Q = -Q$. ***(5 marks)***

(d) Again without actually finding all the points, deduce from (a),(b) and (c) an exact value for $|\mathcal{E}|$. ***(4 marks)***

End of Question Paper