The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2019–2020**

Codes and Cryptography **1 hour**

This is an open book exam.
Answer ***all*** *questions. 40 marks total.*
The submission deadline is 10 am (BST), twenty-four hours after it is released. Late submission will not be considered without extenuating circumstances. It is expected that you will be able to complete this exam in approximately one hour and it is recommended that you submit the work within four hours. You will not be penalised for taking longer, however.
Unless it is explicitly stated otherwise, it is intended that calculations are performed by hand (possibly with the aid of a calculator). To gain full marks, you will need to show your working. You will not get full marks if you simply write down output from a computer package.
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 The following variant of the Polybius square is used to substitute for each letter of the alphabet an ordered pair of elements of the finite field $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. For example, R gets replaced by $(3, 1)$, also written as 31. To convert a text into a string of elements of $\mathbb{F}_5$, all punctuation, including spaces, is omitted.

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I/J	K
2	L	M	N	O	P
3	Q	R	S	T	U
4	V	W	X	Y	Z

Let C be a $[6, 4]$ linear code over $\mathbb{F}_5$, with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 4 & 3 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{pmatrix}.$$

(i) Convert the text "MOBY DICK" into a string of elements of $\mathbb{F}_5$. Further, divide this string into blocks of length 4, and use G to encode each of these blocks $\mathbf{w}$ into a codeword $\mathbf{w}G$. Thus replace the original string of elements of $\mathbb{F}_5$ by a longer one, which we may refer to as the encoded version of "MOBY DICK". ***(3 marks)***

(ii) Give an example of a codeword of weight 4 in C. ***(1 mark)***

(iii) Find a parity check matrix H for C. You might like to check your answer by verifying that $H\mathbf{x}^T = 0$ for each row $\mathbf{x}$ of G. What are the minimum distance d and error-correcting index t for the code C? Give a brief justification of your answers. ***(7 marks)***

(iv) Does C attain the Singleton bound? Is C a perfect code? ***(5 marks)***

(v) The encoded version of a certain piece of text is put into storage, but subjected to errors, so that the retrieved string is different. Assuming no more than t errors per codeword, if the retrieved string is 201224001141, what was the original text? ***(5 marks)***

2 The alphanumeric conversion modulo 29 is given below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	Q	R	S	T	U	V	W	X	Y	Z		?	!	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

(i) Prove that 10 is a primitive root modulo 29, i.e. that the congruence class of 10 is a generator of the multiplicative group $\mathbb{F}_{29}^*$. ***(3 marks)***

(ii) Alice and Bob want to share a key using Diffie-Hellman key exchange. They work modulo $p = 29$, and use the generator $g = 10$ of $\mathbb{F}_{29}^*$. If Alice's secret key is 5 and Bob's public key is 17, what is their shared key? Alice uses this as the key for a Caesar cipher, and sends Bob an encrypted message YV!!COSCSQ. Decrypt this. Why would Bob's secret key be unsuitable for use in the Massey-Omura/Shamir system? ***(6 marks)***

(iii) Bob now wishes to send a message P to Alice, encrypted using her public key and ElGamal encryption. He generates a supplementary key $k = 3$, and sends her the pair $(14, 6)$. What is the decrypted message P? (You do not need to compute Alice's public key to find this.) ***(4 marks)***

(iv) Suppose now that Alice and Bob wish to communicate using 2-dimensional affine encryption, $\mathbf{v} \mapsto K\mathbf{v} + L$, where K is an invertible 2-by-2 matrix with entries in $\mathbb{F}_{29}$ and $\mathbf{v}, L$ are column vectors of length 2 with entries in $\mathbb{F}_{29}$. Here $\mathbf{v}$ represents a block of plaintext (after alphanumeric conversion), while K and L together constitute the key. Given that, under this encryption algorithm, AB becomes HK, CD becomes NY and EG becomes VN, find K and L. Why did I tell you the destination of EG, rather than of EF? ***(6 marks)***

End of Question Paper