Durham University

EXAMINATION PAPER

Examination Session: May/June	**Year:** 2020	**Exam Code:** MATH3401-WE01

Title:	Cryptography and Codes III

Time (for guidance only):	3 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: There is no restriction on the model of calculator which may be used.

Instructions to Candidates:	Credit will be given for your answers to all questions. All questions carry the same marks. Please start each question on a new page. Please write your CIS username at the top of each page. Show your working and explain your reasoning.

Revision:	

ED01/2020

Q1 **1.1** Alice is sending messages to Bob, using the code $C \subseteq \mathbb{F}_5^5$ with generator-matrix $G = \begin{pmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \end{pmatrix}$.

(i) Find the parameters $[n, k, d]$ and a check-matrix H for this code.

(ii) Alice encodes message $\mathbf{m}_1$ as $\mathbf{c}_1$, and sends it to Bob.
In the channel it suffers one symbol-error, and Bob receives the word $\mathbf{y}_1 = (1, 2, 4, 2, 0)$. Show how, *without* making a whole syndrome table, Bob can use $S(\mathbf{y}_1)$ to find $\mathbf{c}_1$ and then $\mathbf{m}_1$.
How does he know that $\mathbf{c}_1$ is the *unique* nearest neighbour of $\mathbf{y}_1$?

(iii) Next, Bob receives the word $\mathbf{y}_2 = (2, 2, 1, 3, 4)$. Show how, while trying to use the same method, Bob discovers that at least two symbol-errors have occurred. Find the two nearest neighbours, $\mathbf{c}_2$ and $\mathbf{c}_3$, of $\mathbf{y}_2$.

1.2 Let the code $C \subseteq \mathbb{F}_3^4$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$.

(i) Find the parameters $[n, k, d]$ of C, and show that C is MDS (maximum distance separable).

(ii) Show that C is self dual - that is, $C = C^{\perp}$.

(iii) What does it mean to say that a code is *perfect*? Show that C is perfect.

(iv) In a *simplex* code, the Hamming distance $d(\mathbf{c}_1, \mathbf{c}_2)$ between any two distinct codewords is the same. Show that C is a simplex code.

Q2 In this question we use $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$.
To construct our code we also use some polynomials $\phi(y) = ay^2 + by + c$ over $\mathbb{F}_4$. (So the coefficients a, b, c are from $\mathbb{F}_4$, and we write y for the variable to avoid confusion. We can then 'plug in' elements of $\mathbb{F}_4$ for y.)

The hexacode $C \subseteq \mathbb{F}_4^6$ is given by

$$C = \{(\, a,\, b,\, c,\, \phi(1),\, \phi(x),\, \phi(x^2)\,) \mid \phi(y) = ay^2 + by + c \text{ with } a, b, c, \in \mathbb{F}_4\}$$

2.1 How many words are in this code?

2.2 Show that $G = \begin{pmatrix} 1 & 0 & 0 & 1 & x^2 & x \\ 0 & 1 & 0 & 1 & x & x^2 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ is a generator-matrix for C.

2.3 Find a check-matrix H for C, and show that $C^{\perp} \neq C$, but $C^{\perp}$ is equivalent to C.

2.4 By puncturing C at the 6th and 3rd position respectively, we make new codes C_6 and C_3. Show that these are equivalent, and are Hamming codes.

2.5 Consider the extended code $\widehat{C_6}$. Is it equal, or equivalent, to C? You may use the fact that $d(C) = 4$. (*Hint:* First show that $(x^2, x, 1, 0, 0) \in C_6$.)

Q3 **3.1** (i) Consider the polynomials $f_1(x) = x^2 + x + 1$ and $f_2(x) = x^2 + 2x + 2$ in $\mathbb{F}_3[x]$. Show that one of them is reducible and one is irreducible.

(ii) Complete the following table of powers of x in $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 2x + 2)$, giving each x^i in the form $a_1x + a_0$, with the a_i in $\mathbb{F}_3$.

i	0	1	2	3	4	5	6	7	8
x^i	1	x	$x+1$						

Use your table to calculate $x^2 + x^7$ and $(2x + 1)(2x + 2)$ in $\mathbb{F}_9$.

(iii) Ternary cyclic codes of block length 3 can be regarded as lying in the ring $\mathbf{R}_3 = \mathbb{F}_3[x]/(x^3 - 1)$. For each nontrivial such code (that is, with $0 < \dim(C) < 3$) give the generator-polynomial and a generator-matrix.

(iv) For the code of dimension 2, pick any nonzero codeword (written in $\mathbb{F}_3^3$), and show directly that all its cyclic shifts are in the code.

3.2 We use the following convention to convert alphabetic messages into integers modulo 26:

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

(i) Alice uses an affine cipher to send a message, which is either "ARMY" or "TEMP", to Bob. You intercept the ciphertext "FIWL". Find the message, and the key.

(ii) Alice uses a one-time pad to send the message "FILMSTAR" to Bob. You know the plaintext, and you intercept the ciphertext "PRIMARKS". Bob now re-uses the same one-time pad to send a message to Alice, and you intercept the ciphertext "QNOMILI". Find the plaintext of the message Bob sent to Alice.

Q4 **4.1** Suppose $n = 19291$ and $\phi(n) = 19000$. Here $\phi(n)$ denotes the Euler totient function. Use this information to factor n as a product of two primes.

4.2 Let $p = 71$ be a prime, let $g = 31$ be a primitive root modulo p. Then use the baby step, giant step algorithm to compute the index $I(6)$.

4.3 Bob has an RSA public key of the form $(n, 3)$, i.e. $e = 3$. When Alice wants to send a number $0 \leq x < n$ to Bob, she encrypts it using Bob's public key. For some reason, Bob fails to receive the message correctly, he informs Alice on the matter, and she retries to send the message again. However, this time, to prevent repeating the same message, Alice encrypts $x+1$ instead and sends it to Bob. Suppose that Eve has intercepted both encrypted messages successfully and she knows that the second time Alice encrypted $x + 1$ and sent it to Bob. Show how Eve can exploit this information to easily obtain x.
(Hint: First try to compute $x^2 + x$ from this information).

4.4 Alice is signing messages using the Elgamal signature scheme with a public prime p and a primitive root g. Her public verification key is $y \equiv g^{\alpha} \bmod p$. Suppose that she signs two different messages m_1 and m_2 with signatures (r, s_1) and (r, s_2) respectively. Here you may assume that $0 < m_1, m_2 < p - 1$ and $\gcd(s_1 - s_2, p - 1) = \gcd(r, p - 1) = 1$. Show how this information can be used to find Alice's private key α.

Q5 **5.1** Consider the following elliptic curve E defined over the field $\mathbb{F}_7$

$$E \ : \ Y^2 = X^3 + 2.$$

(i) Let $A, B \in E(\mathbb{F}_7)$ given by $A = (3, 1), B = (5, -1)$. Calculate the points $-A$ and $A \oplus B$.

(ii) Find all points $P \in E(\mathbb{F}_7)$ that satisfy that $[5]P = \mathcal{O}$. Here $\mathcal{O}$ denotes the identity element in $E(\mathbb{F}_7)$.

5.2 Alice and Bob are using an Elliptic curve Diffie-Hellman key exchange to agree on a key, using an elliptic curve E defined over a finite field $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$. Suppose Eve is able to intercept messages between Alice and Bob and is able to alter them before sending them forward. Devise an attack by Eve that will make sure that

- both Alice and Bob think that they have exchanged a key.
- Eve is able to decrypt all further ciphertexts Alice and Bob send to each other using their corresponding keys. You may assume here that Alice and Bob are using an encryption method in which the knowledge of the encryption key is enough to deduce the decryption key.

5.3 Let $p = 149$ and let $E : Y^2 = X^3 + 111X + 50$ be an elliptic curve over $\mathbb{F}_p$. Let $P = (7, 53)$ be a point on $E(\mathbb{F}_p)$. Suppose you know that $[39]P = (12, 117)$.

(i) Calculate the point $[78]P$ on $E(\mathbb{F}_p)$. Please show all your work.

(ii) Prove that $E(\mathbb{F}_p)$ is a cyclic group. What is the order of this group, i.e., how many elements does it have? Carefully justify each step in your answer.