

EXAMINATION PAPER

Examination Session: May/June

Year: 2022

Exam Code:

MATH3401-WE01

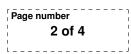
Title:

Codes and Cryptography III

Time:	3 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: Casio FX83 series or FX85 series.

Instructions to Candidates:	Answer all questions. Section A is worth 40% and Section B is worth 60%. Withi each section, all questions carry equal marks.						
	Students must use the mathematics specific answer book.						

Revision:



SECTION A

Q1 We use the following convention to convert alphabetic messages into integers modulo 26:

А	В	\mathbf{C}	D	Е	F	G	Η	Ι	J	Κ	L	Μ
1	2	3	4	5	6	$\overline{7}$	8	9	10	11	12	13
Ν	Ο	Р	Q	R	S	Т	U	V	W	Х	Y	Ζ
14	15	16	17	18	19	20	21	22	23	24	25	26

- **1.1** Suppose Alice is using $M = \begin{pmatrix} 3 & 4 \\ 1 & 8 \end{pmatrix}$ as an encryption matrix in a 2 × 2 Hill/Block cipher. Find two different plaintexts that encrypt to the same ciphertext. Using the encryption matrix M given above, can there be three different plaintexts which encrypt to the same ciphertext? If yes, give an example; if no, prove that it is impossible.
- **1.2** Suppose a one time pad was used to encrypt a message to obtain the following ciphertext:

TIUBSRBEWKTY.

Suppose you know that the first four letters in the plaintext are *SELL*. Then use this information to guess the keypad and further decipher the plaintext. Give rigorous reasoning.

- **Q2** Let $E: y^2 = x^3 + Ax + B$ be an elliptic curve defined over a finite field \mathbb{F}_p . Let \oplus denote the standard group operation on $E(\mathbb{F}_p)$.
 - **2.1** Now, let \odot be a different operation on $E(\mathbb{F}_p)$ defined by

$$P \odot Q = -(P \oplus Q), \tag{1}$$

for any $P, Q \in E(\mathbb{F}_p)$. Is this operation associative? Give rigorous reasoning.

- **2.2** Let $E: y^2 = x^3 x$ be defined over \mathbb{F}_3 . Prove that in this case, the operation \odot as defined in (1) indeed gives a group structure on $E(\mathbb{F}_3)$.
- **2.3** Let *E* be an elliptic curve over \mathbb{F}_p such that $E(\mathbb{F}_p)$ is a group under operation \odot defined in (1). Prove that the cardinality of $E(\mathbb{F}_p)$ is at most 4.
- **Q3** 3.1 Let $C \subseteq \mathbb{F}_7^6$ be the code generated by

$$G = \begin{pmatrix} 1 & 2 & 4 & 0 & 6 & 1 \\ 0 & 0 & 0 & 3 & 5 & 1 \\ 0 & 0 & 0 & 0 & 2 & 3 \end{pmatrix}.$$

Find a check matrix for C.

3.2 By considering the syndrome of $\boldsymbol{y} = (1, 2, 1, 4, 0, 1) \in \mathbb{F}_7^6$, determine whether \boldsymbol{y} is a codeword of C or not.



- **Q4** 4.1 Show that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, and is a primitive polynomial over \mathbb{F}_2 .
 - **4.2** Let $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2+x+1)$. Construct a decoding array for $C = \langle (x,1) \rangle \subseteq \mathbb{F}_4^2$, and use it to decode (x,0) and (x,x).
 - **4.3** Suppose that C is transmitted over a 4-ary symmetric channel with symbol error probability p. Find p such that the chance that a received word is decoded correctly is equal to 1/2.

SECTION B

Q5 5.1 Suppose Alice is sending a message $0 \le m < n$ to Bob using the RSA public key protocol with RSA modulus n = pq and public encryption key e. Bob receives Alice's corresponding ciphertext x, but instead of the standard decryption modulus d, he uses d' defined by

$$d'e \equiv 1 \bmod \lambda(n).$$

Here, given n = pq as above, we define $\lambda(n) = \text{l.c.m.}(p - 1, q - 1)$ where l.c.m. denotes the least common multiple function. Will Bob be able to recover m by computing $x^{d'} \mod n$? Give rigorous reasoning.

5.2 Let $p \equiv 3 \mod 4$ denote a large prime. Let 0 < m < p denote a message and let *h* denote a hash function

$$h(m) = m^2 \bmod p.$$

Prove that h is not pre-image resistant. Is it strongly collision free? Give thorough reasoning.

(Hint: you may use here that -1 is not a quadratic residue modulo p.)

5.3 Let E be an elliptic curve defined by the equation

$$y^2 = x^3 + 376x.$$

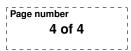
Determine the set of torsion points $E(\mathbb{Q})_{\text{tors}}$ explicitly. Give careful reasoning of each step.

(Hint: you may reduce the equation modulo suitable primes.)

- **Q6 6.1** Suppose Alice is using the ElGamal digital signature scheme with a prime p and a primitive root g modulo p to sign a message m. Suppose her random number generator machine is broken. Therefore, she instead chooses $k = \alpha$, where α is her secret key and computes the signature (r, s). Suppose Eve intercepts the signed message. Show how Eve can use this information to break this cryptosystem.
 - **6.2** For a in \mathbb{Z} , a > 0, let E_a be an elliptic curve defined over \mathbb{Q} by the equation

$$y^2 = x^3 + a$$

Find the values of a for which $E_a(\mathbb{Q})$ has torsion points of order 2, and specify these points. Do the same for order 3. Explain each step carefully.



- **Q7** 7.1 Let $C = \langle (2,1,0), (0,2,1) \rangle \subseteq \mathbb{F}_3^3$. Find a generator matrix and check-matrix for C, and state the parameters [n, k, d] for this code.
 - **7.2** Find a generator matrix and a check-matrix for C^{\perp} , and state the parameters [n', k', d'] for this code.
 - **7.3** Show that the permutation automorphism group of both C and C^{\perp} is S_3 . Hint: Recall that S_3 is generated by the two elements written in cycle form as (12) and (123).

7.4 Show that

$$|\mathrm{MAut}(C)| = 2|\mathrm{PAut}(C)|.$$

- Q8 8.1 Show that linear binary self-dual codes exist if and only if the block-length is even.
 - 8.2 Show that

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

is a generator matrix for $\widehat{Ham}_2(3)$, and state (without proof) the parameters [n, k, d] for this code.

8.3 For $x, y \in \mathbb{F}_2^n$, let $x \cap y$ denote the vector which has a 1 only in positions where both x and y have a 1, and is 0 elsewhere.

Show that $\boldsymbol{x} \cdot \boldsymbol{y} = 0$ if and only if $w(\boldsymbol{x} \cap \boldsymbol{y})$ is even.

8.4 We say that a code is *doubly-even* if the weight of any codeword is a multiple of four. Let C be a linear binary code with generator matrix G, such that every row of G has weight divisible by four, and any two distinct rows of G are orthogonal. Show that $C \subseteq C^{\perp}$, and that C is doubly-even.

Hint: You may use the fact that for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n$,

$$w(\boldsymbol{x} + \boldsymbol{y}) = w(\boldsymbol{x}) + w(\boldsymbol{y}) - 2w(\boldsymbol{x} \cap \boldsymbol{y}).$$

8.5 Show that the matrix defined in block form as

$$G_2 = \begin{pmatrix} G_1 & \hat{0} \\ \hat{0} & G_1 \end{pmatrix},$$

where $\hat{0}$ denotes a matrix of all zeros of the appropriate dimension, is the generator matrix for a binary doubly-even self-dual code.