



## EXAMINATION PAPER

<b>Examination Session:</b> May/June	<b>Year:</b> 2025	<b>Exam Code:</b> MATH3401-WE01
---	----------------------	------------------------------------

<b>Title:</b> Cryptography and Codes III (2023/24 Syllabus)
--

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

Instructions to Candidates:	<p>Answer all questions.</p> <p>Section A is worth 40% and Section B is worth 60%. Within each section, all questions carry equal marks.</p> <p>Write your answer in the white-covered answer booklet with barcodes.</p> <p>Begin your answer to each question on a new page.</p>
-----------------------------	---

<b>Revision:</b>	
------------------	--

## SECTION A

**Q1** We use the following convention to convert alphabetic messages into sequences of 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

You receive the ciphertext “JOPRMD”, encrypted using a Hill cipher with block length 2 and key matrix

$$K = \begin{pmatrix} 5 & 1 \\ 12 & 9 \end{pmatrix}.$$

Find the plaintext (as a word).

**Q2** Alice and Bob are using the Diffie–Hellmann key exchange scheme with  $p = 157$  and  $g = 5$ .

- (a) Alice sends  $g^\alpha = 124$  to Bob and Bob sends  $g^\beta = 108$  to Alice. Use the baby-step giant-step algorithm to find  $\alpha$ .
- (b) Find their shared secret key. *If you were unable to answer part (a), use the (incorrect) value  $\alpha = 19$ .*

**Q3** (a) Give a matrix  $H \in M_{2,4}(\mathbb{F}_3)$  such that the code defined by

$$C = \{\mathbf{x} \in \mathbb{F}_3^4 \mid \mathbf{x}H^t = \mathbf{0}\}$$

is a ternary Hamming code of redundancy 2.

- (b) Give the parameters of the code  $C$  (no proof is required).
- (c) Is the code  $C$  permutation equivalent to a cyclic code? Justify your answer. (Hint: Write generator-matrices for all ternary cyclic codes of block-length 4 and dimension 2.)

**Q4** Let  $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + x + 2)$ .

- (a) Show that  $x$  is primitive in  $\mathbb{F}_9$ .
- (b) Let  $C = \langle \{(0, x + 1, 2x + 1, x, 1), (1, 0, 0, 2, x), (2, 1, 0, x + 2, x)\} \rangle \subseteq \mathbb{F}_9^5$ . Find a generator- and a check-matrix for  $C$ , and its parameters  $[n, k, d]$ .

## SECTION B

**Q5** (a) Using the congruences

$$458^2 \equiv 2^3 \cdot 3^6 \cdot 5 \pmod{45151}$$

$$1327^2 \equiv 2^3 \cdot 5 \pmod{45151},$$

factorise 45151.

(b) Bob's RSA public key is  $(N, e) = (47941, 3)$ .

(i) Find the encryption of  $m = 149$ .

(ii) Another message  $m'$  has encryption 31163. Show that the encryption of  $149m'$  is 27.

(iii) Hence find  $m'$ . *You do not need to find the decryption exponent.*

**Q6** Let  $E$  be the curve defined by  $y^2 = x^3 + x^2 + x$  over  $\mathbb{F}_p$  where  $p > 3$  is prime. Although this is not an elliptic curve as defined in lectures, it is still possible to put a group law  $\oplus$  on the set of points

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + x^2 + x\} \cup \{\mathcal{O}\}$$

as follows. Define  $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$ . If  $P = (x_0, y_0)$  and  $Q = (x_1, y_1)$  are in  $E(\mathbb{F}_p)$  and  $y_0 = -y_1$ , define  $P \oplus Q = \mathcal{O}$ . Otherwise, define

$$P \oplus Q = (x_2, y_2)$$

where

$$x_2 = \lambda^2 - 1 - x_0 - x_1$$

and

$$y_2 = -(\lambda x_2 + \mu)$$

with

$$\lambda = \begin{cases} \frac{y_1 - y_0}{x_1 - x_0} & \text{if } x_1 \neq x_0 \\ \frac{3x_0^2 + 2x_0 + 1}{2y_0} & \text{if } x_1 = x_0 \text{ and } y_1 = y_0 \end{cases}$$

and

$$\mu = y_0 - \lambda x_0.$$

(a) Give a geometric interpretation, with justification, of the quantities  $\lambda$  and  $\mu$ .

(b) Suppose that  $p = 5$ . List the points of  $E(\mathbb{F}_5)$  and show that  $E(\mathbb{F}_5)$  is cyclic of order 8 with  $P = (2, 2)$  being a generator.

(c) Suppose that  $p = 7$ . List the points of  $E(\mathbb{F}_7)$  and show that  $|E(\mathbb{F}_7)| = 8$ . Is  $E(\mathbb{F}_7)$  cyclic?

- Q7** (a) Show that the only irreducible polynomials in  $\mathbb{F}_2[x]$  of degree three are  $x^3+x^2+1$  and  $x^3+x+1$ .
- (b) Using the fact that  $x^7-1=(x-1)(x^3+x^2+1)(x^3+x+1)$  in  $\mathbb{F}_2[x]$ , list the generator-polynomials of all binary cyclic codes of block length 7.
- (c) Give generator- and check-matrices for the binary cyclic codes of length 7 and dimension 4.
- (d) State the sphere packing bound for a  $q$ -ary  $(n, M, d)$  code and explain what it means for a code to be perfect. Find all (if any) binary cyclic codes of length 7 and dimension 4 which are perfect. Justify your answer.
- Q8** Let  $p$  be an odd prime, and let  $C_1, C_2 \subseteq \mathbb{F}_2^p$  be cyclic binary codes of block-length  $p$ . Write  $g_1(x)$  and  $g_2(x)$  for their generator-polynomials, and assume that  $x^p-1=(x-1)g_1(x)g_2(x)$ .
- (a) Let  $a(x) \in \langle g_1(x) \rangle$  and  $b(x) \in \langle g_2(x) \rangle$ . Show that  $a(x)b(x)$  is either zero or equal to  $1+x+\dots+x^{p-1}$  in  $\mathbf{R}_p = \mathbb{F}_2[x]/(x^p-1)$ .
- (b) Assume now that  $C_1$  and  $C_2$  are permutation equivalent and let  $a$  be a codeword of  $C_1$  of weight  $w$ . Show that there is a codeword  $b \in C_2$  of weight  $w$ .
- (c) With notation as above assume that  $w$  is odd. Show that  $w^2 \geq p$ .
- (d) Using the fact that

$$x^{31}-1=(x-1)(1+x^3+x^8+x^9+x^{13}+x^{14}+x^{15})(1+x+x^2+x^6+x^7+x^{12}+x^{15})$$

in  $\mathbb{F}_2[x]$ , show that every codeword of odd weight of the cyclic code  $\langle g(x) \rangle$ , with  $g(x) = 1+x^3+x^8+x^9+x^{13}+x^{14}+x^{15}$ , has weight at least 7.