Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2026	MATH3401-WE01

Title: Cryptography and Codes III

Time:	3 hours	
Additional Material provided:	None	
Materials Permitted:	None	
Calculators Permitted:	Yes	Models Permitted: Casio FX83 series or FX85 series.

Instructions to Candidates:	Answer all questions. The indicative marks shown in brackets for the main parts of each question are given as a guide to the weighting the markers expect to apply. Write your answer in the white-covered answer booklet with barcodes. Begin your answer to each question on a new page.

Revision:	

ED01/2026

SECTION A

1. Let C be a q-ary linear $[n, k, d]$ code.

(a) State the Singleton bound for C. **[2]**

(b) State the Sphere Packing bound for C. **[2]**

(c) Give an example of a perfect binary linear code of dimension 4 and minimum distance 3 by giving a generator-matrix of the code. Justify your answer. **[6]**

---

2. Let $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$.

(a) Make a table expressing each $x^i,\ 0 \leq i \leq 7$, in the form $a_2x^2 + a_1x + a_0$ with $a_0, a_1, a_2 \in \mathbb{F}_2$. **[4]**

(b) Let $C = \langle\{(x^2,\ x{+}1,\ x^2{+}x{+}1,\ 1), (0,\ 0,\ x^2,\ x), (x{+}1,\ x^2{+}x,\ 0,\ x^2{+}1)\}\rangle \subseteq \mathbb{F}_8^4$. Find a generator- and a check-matrix for C, and find the parameters $[n, k, d]$ of C. Justify your answer. **[6]**

---

3. 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

(a) Alice uses a one time pad with entries $(15, 20, 5, 17, 4, 22, 1, 4, 10)$ to encrypt the message $HELP\ ME$. Compute the ciphertext. **[3]**

(b) Alice uses a Hill cipher with the encryption key $\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$ to produce the ciphertext $UXVV$. Compute the decryption key and compute the plaintext. **[7]**

---

4. (a) Explain how the Diffie-Hellman key exchange protocol can be used to agree upon a key between Alice and Bob. **[3]**

(b) Alice and Bob use Diffie-Hellman key exchange with prime $p = 23$ and primitive root $g = 7$. Suppose Alice chooses a random number $n = 10$ and Bob chooses $m = 5$. What are the actual numbers exchanged between Alice and Bob? Which key $0 \leq \kappa \leq 22$ do they agree upon? Show your working. **[3]**

(c) Using Fermat's factorisation method, factor the integer 33673. **[4]**

SECTION B

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

(a) Let $\mathbf{a} = (0, 1, 2, x, 2x, x + 1) \in \mathbb{F}_9^6$ and $\mathbf{b} = (1, 2, 1, 2, 1, 2) \in \mathbb{F}_9^6$. Give a generator-matrix for the 9-ary Reed-Solomon Code $\mathrm{RS}_3(\mathbf{a}, \mathbf{b})$. Write the entries of the matrix in the form $cx + d$ with $c, d \in \mathbb{F}_3$. What are the parameters $[n, k, d]$ of $\mathrm{RS}_3(\mathbf{a}, \mathbf{b})$? **[4]**

(b) Assume that $\mathbf{c} = (c_1, c_2, c_3, c_4, c_5, c_6) \in \mathrm{RS}_3(\mathbf{a}, \mathbf{b})$ and we know that $c_1 = 1$ and $c_3 = c_5 = 0$. Find the entries c_2, c_4 and c_6 in the form $cx + d$ with $c, d \in \mathbb{F}_3$. Justify your answer. **[6]**

(c) Consider vectors $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6)$, $\mathbf{a}' = (a'_1, a'_2, a'_3, a'_4, a'_5, a'_6)$ and $\mathbf{b} = (b_1, b_2, b_3, b_4, b_5, b_6)$ in $\mathbb{F}_9^6$ such that $a'_i = \alpha a_i + \beta$, for $1 \leq i \leq 6$ and some $0 \neq \alpha \in \mathbb{F}_9$ and $\beta \in \mathbb{F}_9$. Show that $\mathrm{RS}_k(\mathbf{a}', \mathbf{b}) = \mathrm{RS}_k(\mathbf{a}, \mathbf{b})$ for all $k = 0, 1, \ldots, 6$. (Here we take all a_i pairwise distinct and all b_i non-zero.) **[5]**

---

6. Let $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$.

(a) Give an example of a perfect linear code over $\mathbb{F}_4$ with parameters $[5, 3, 3]$ by writing a check-matrix. Justify your answer. **[5]**

(b) Consider the polynomials $f_1(y) = y^2 + xy + 1 \in \mathbb{F}_4[y]$ and $f_2(y) = y^2 + (x + 1)y + 1 \in \mathbb{F}_4[y]$. Show that

$$y^4 + y^3 + y^2 + y + 1 = f_1(y) f_2(y),$$

as polynomials in $\mathbb{F}_4[y]$. **[2]**

(c) How many cyclic codes of length 5 over $\mathbb{F}_4$ are there? Justify your answer. **[4]**

(d) By writing a check-matrix, find a cyclic code of length 5 and dimension 3 over $\mathbb{F}_4$ which is perfect. Justify your answer. **[4]**

---

7. (a) Explain how the Elgamal digital signature scheme works. **[3]**

(b) Alice uses the Elgamal digital signature scheme with prime $p = 23$ and $g = 5$ to sign message m. Suppose her public verification key is $y = 9$.

(i) Compute Alice's secret key α directly from the above information. Justify your answer. **[2]**

(ii) Alice uses the same value of k to sign two messages $m_1 = 11$ and $m_2 = 16$. Suppose her signatures for m_1 and m_2 are $(10, 7)$ and $(10, 16)$ respectively. Show how one can also deduce Alice's secret key α directly from this information. For this part, do not compute any discrete logarithms directly. **[4]**

(c) 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 tries 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). **[6]**

---

8. Let E be the elliptic curve $y^2 = x^3 + 3x - 3$ over $\mathbb{F}_{23}$ and let $P = (1, 1)$ be a point on E. Let n be the order of the elliptic curve $E(\mathbb{F}_{23})$.

(a) Given that $[8]P = (18, 8)$, find $[16]P$ and hence find the order of P. **[5]**

(b) Show that $|E(\mathbb{F}_{23})| < 34$. Use this to show that $E(\mathbb{F}_{23})$ is a cyclic group. **[3]**

(c) Alice thinks of a secret integer $0 < \alpha < n$ and sends Bob the point $Q = [\alpha]P$. For what values of α would we have $[16]Q = \mathcal{O}$? Give thorough justification. **[3]**

(d) You now observe that $Q = (6, 1)$. Calculate $Q \oplus (-P)$ and hence find α. What is the order of $Q = (6, 1)$? **[4]**
