

EXAMINATION PAPER

Examination Session: May/June

2024

Year:

Exam Code:

MATH30120-WE01

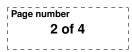
Title:

Cryptography and Codes V

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

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

Revision:



SECTION A

- Q1 In this question, messages are sequences of digits regarded as integers modulo 10.
 - (a) A 2×2 Hill cipher modulo 10 is used to encrypt the plaintext '1989'. The resulting ciphertext is '9532'. Find the encryption and decryption keys.
 - (b) A 3×3 Hill cipher modulo 10 is used to encrypt the plaintext '124'. The resulting ciphertext is '783'. Find the encryption of the plaintext '248'.

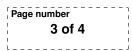
- **Q2** Let *E* be the elliptic curve $y^2 = x^3 + 2x$ over \mathbb{F}_7 .
 - (a) Find all 2-torsion points of $E(\mathbb{F}_7)$.
 - (b) Show that $(5,4) \in E(\mathbb{F}_7)$ has order 8.
 - (c) Is $E(\mathbb{F}_7)$ cyclic?

- $\mathbf{Q3}$ (a) How many ternary cyclic codes of block-length 4 are there? Justify your answer.
 - (b) For each such code give a generator-matrix, and the generator-polynomial.

- Q4 (a) Let C be a linear code in \mathbb{F}_q^n . Give the definition of its dual C^{\perp} . State, without proof, how the dimension of C is related to that of C^{\perp} . Do the same for their generator and check-matrices.
 - (b) Let now D be another linear code in \mathbb{F}_q^n and define

$$C+D := \{c+d \in \mathbb{F}_a^n \mid c \in C, \ d \in D\}.$$

Show that $(C + D)^{\perp} = C^{\perp} \cap D^{\perp}$. (Here you may assume without proof that C + D is a linear code in \mathbb{F}_q^n .)



SECTION B

- **Q5** Alice and Bob use the Diffie–Hellman key exchange protocol. They publicly agree on a large¹ prime p and primitive root $g \in \mathbb{F}_p^{\times}$. Alice chooses an integer $0 \leq \alpha and Bob chooses an integer <math>0 \leq \beta . They keep these secret and exchange the values of <math>g^{\alpha}$ and g^{β} over a public channel.
 - (a) What is their shared secret key? How can they each calculate it?

Now Alice and Bob generate secret sequences of integers $\alpha_1, \alpha_2, \ldots$ and β_1, β_2, \ldots by taking

$$\alpha_1 = \alpha$$

$$\beta_1 = \beta$$

$$\alpha_{n+1} = a\alpha_n + b \mod (p-1)$$

$$\beta_{n+1} = c\beta_n + d \mod (p-1)$$

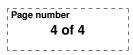
where a, b, c, d are publicly known integers with a and c coprime to p-1. They use these to obtain shared secrets $\kappa_1, \kappa_2, \ldots$ using the Diffie-Hellman protocol.

- (b) Suppose that Eve observes the messages sent between Alice and Bob and also obtains the value of κ_2 . Show that she can find κ_n for all $n \ge 2$.
- (c) Can Eve find κ_1 (in a reasonable amount of time)? Justify your answer.
- (d) Can Eve find α and β (in a reasonable amount of time)? Justify your answer.

Q6 Alice's RSA public key is (n, e) where n is a product of two primes.

- (a) Suppose that (n, e) = (399797, 3). Bob sends the message m to Alice. Its encryption is 8000. Find m.
- (b) Suppose that (n, e) = (18871, 17). Use Fermat's method to factorise n and hence find the decryption exponent d.
- (c) Suppose that n = 12449. Let P = (2,5) be a point on the elliptic curve $E: y^2 = x^3 + 17$ modulo n. By attempting to compute [4]P, factorise n.

¹Say, $p > 2^{2048}$.



- **Q7** Let g(x) be the generator-polynomial of a binary cyclic code C of length n > 1 and dimension at least one.
 - (a) Show that, if g(x) has x 1 as a factor then the code C contains no codewords of odd weight.
 - (b) Show that if x 1 is not a factor of g(x) then the code C contains the codeword consisting of all 1s.
 - (c) Assume that for any $m \in \mathbb{N}$ with m < n, g(x) does not divide $x^m 1$. Show that the code C has minimum distance at least 3.
 - (d) Suppose g(x) is such that the corresponding code C contains both even-weight and odd-weight codewords. Show that the polynomial (x-1)g(x) also generates a binary cyclic code C_1 of length n, and that $C_1 = \{c \in C \mid w(c) \text{ is even}\}$. That is, the code C_1 consists of the even-weight codewords of C.

- **Q8** (a) Let $q \ge n \ge k \ge 0$ be positive integers and $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, with the a_j all distinct and the b_j all non-zero. Give the definition of the Reed-Solomon Code $\mathrm{RS}_k(\mathbf{a}, \mathbf{b})$ as a q-ary [n, k] code. Furthermore give, without proof, the minimum distance of this code and the form of a generator-matrix.
 - (b) Consider the polynomial $x^2 + 1 \in \mathbb{F}_3[x]$. Show that it is irreducible. Is it primitive? Justify your answer.
 - (c) Consider the field $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$. Give a cyclic 9-ary [4, 2, 3] code by giving both a generator-matrix and its generator-polynomial.