Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2023	MATH30120-WE01

Title: Codes and Cryptography V

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%. Within each section, all questions carry equal marks. Students must use the mathematics specific answer book.

Revision:	

SECTION A

Q1 (a) 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 the plaintext "FROM" to Bob. Suppose that the corresponding ciphertext is "NLSO". Use this information to compute the encryption and decryption keys.

(ii) Alice uses a one-time pad to send a message to Bob. You intercept the ciphertext

ZQXVXKJZNDTEFOUU.

Suppose you know that the first four letters of the plaintext are YOUR. Using this information, can you guess what the one time pad is? What is the full plaintext? Give careful reasoning.

Q2 (a) Using the Chinese remainder theorem or otherwise, determine whether the group $(\mathbb{Z}/55)^\times$ is isomorphic to $(\mathbb{Z}/100)^\times$.

(b) State and explain how the ElGamal digital signature scheme works.

Q3 Let $C \subseteq \mathbb{F}_3^3$, given by

$$C = \{(222), (101), (010), (111), (121), (020)\}$$

be sent over a ternary symmetric channel with symbol-error probability p.

3.1 Calculate $\mathbb{P}((120) \text{ received} \mid (111) \text{ sent})$.

3.2 Calculate $\mathbb{P}((111) \text{ sent} \mid (120) \text{ received})$, assuming all codewords are equally likely to be sent. Fully simplify your answer.

3.3 What are the parameters $[n, k, d]_q$ of $\langle C \rangle$?

Q4 Let $\mathcal{G}_{11}$ be the ternary $[11, 6, 5]$ code generated by

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 \end{pmatrix}.$$

4.1 Show that $\mathcal{G}_{11}$ is a perfect code.

4.2 Give a generator matrix for $\mathcal{G}_{11}^\perp$.

4.3 Show that $\mathbf{c} = (1\,2\,0\,1\,1\,0\,1\,2\,0\,0\,0) \in \mathcal{G}_{11}^\perp$.

SECTION B

Q5 (a) Let $N = 227179$. Suppose you are given

$$477^2 \equiv 350 \bmod N,$$
$$482^2 \equiv 5145 \bmod N,$$
$$493^2 \equiv 15870 \bmod N.$$

Use this information to factor N as a product of two primes.

(b) Let $p \equiv 3 \bmod 4$ be a large prime and let g be a primitive root modulo p.

(i) Let z be a quadratic residue modulo p. Then prove that $z^{(p-1)/2} \equiv 1 \bmod p$.

(ii) Show that the Computational Diffie-Hellman problem, namely:

given $g^x \bmod p$ and $g^y \bmod p$, compute $g^{xy} \bmod p$,

is equivalent to solving the following problem:

given $g^x \bmod p$, compute $g^{x^2} \bmod p$.

(Hint: You may use that $(x+y)^2 = x^2 + y^2 + 2xy$.)

Q6 (a) Alice submits a bid to an auction, and so that other bidders cannot see her bid, she encrypts it under the public key of the auction service. Suppose that the auction service provides a public key for an RSA encryption scheme, with a modulus $n = pq$ and the encryption exponent e. Assume that bids are encoded simply as integers between 0 and n. Suppose it is also well known that Alice never bids above $n/2$ and that she always submits a rounded bid, namely that her bid is a multiple of 100. Show how Eve can submit an encryption of a bid that exceeds Alices bid by 10%, without even knowing what Alice's bid is.

(b) Let $E : y^2 = x^3 - 43x + 166$ be an alliptic curve defined over $\mathbb{Q}$. Let $P = (3, 8)$ be a point on the elliptic curve E.

(i) Compute the points $[3]P$ and $[4]P$ in $E(\mathbb{Q})$.

(ii) Compute the group structure of the reduction of E modulo 5, namely, of the group $E(\mathbb{F}_5)$.

(iii) Compute the group structure of the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$.

Q7 **7.1** Let $R_n = \mathbb{F}_q[x]/(x^n - 1)$, and let $g(x) \in R_n$. Show that $\langle g(x) \rangle$ is a cyclic code.

7.2 How many ternary cyclic codes of block-length 6 and dimension 3 exist?

7.3 Now let $R_6 = \mathbb{F}_3[x]/(x^6 - 1)$. Find the parameters $[n, k, d]$ of the code $C \subseteq R_6$ with generator-polynomial $g(x) = x^3 + x^2 + 2x + 2$.

Q8 Let $C_6 \subseteq \mathbb{F}_4^6$ be the code generated by

$$G_6 = \begin{pmatrix} 1 & 0 & 0 & 1 & x & x \\ 0 & 1 & 0 & x & 1 & x \\ 0 & 0 & 1 & x & x & 1 \end{pmatrix}.$$

8.1 By considering its syndrome, decode $\mathbf{x} = (x\,1\,1\,x^2\,1\,x^2) \in \mathbb{F}_4^6$ to a codeword of C_6. You do not need to explicitly give the syndrome table for C_6.

8.2 For $\lambda \in \mathbb{F}_4$, we define $\overline{\lambda}$ by $\overline{0} = 0$, $\overline{1} = 1$, $\overline{x} = x^2$, and $\overline{x^2} = x$. We extend this map to $\mathbb{F}_4^n$ by

$$\overline{\mathbf{x}} = (\overline{x_1}\,\overline{x_2}\,\ldots\,\overline{x_n}), \quad \text{where } \mathbf{x} = (x_1\,x_2\,\ldots\,x_n) \in \mathbb{F}_4^n.$$

Using this map, for a linear code $C \subseteq \mathbb{F}_4^n$ we define

$$\overline{C} = \{\overline{\mathbf{c}} \mid \mathbf{c} \in C\},$$
$$C^* = \{\mathbf{x} \in \mathbb{F}_4^n \mid \mathbf{x} \cdot \overline{\mathbf{c}} = 0 \;\forall\, \mathbf{c} \in C\}.$$

Prove that if $C \subseteq \mathbb{F}_4^n$ is a linear code, $C^* = (\overline{C})^{\perp}$.

8.3 Prove that C_6 satisfies $C_6^* = C_6$.