Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May	2019	MATH3401-WE01

Title: Cryptography and Codes

Time Allowed:	3 hours	
Additional Material provided:	None	
Materials Permitted:	None	
Calculators Permitted:	Yes	Models Permitted: Casio fx-83 GTPLUS or Casio fx-85 GTPLUS.
Visiting Students may use dictionaries: No		

Instructions to Candidates:	Credit will be given for: the best **FOUR** answers from Section A and the best **THREE** answers from Section B. Questions in Section B carry **TWICE** as many marks as those in Section A.

Revision:	

ED01/2019

University of Durham Copyright

SECTION A

1. 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 encrypts the plaintext "PLAY" using a Hill cipher with block length two and key matrix
$$\begin{pmatrix} 5 & 7 \\ 2 & 17 \end{pmatrix}.$$
   Find the ciphertext (in alphabetic form).

   (b) Using a Hill cipher with block length two and a different key matrix M, Alice encrypts the plaintext "MILK" and obtains the ciphertext "EFFI".
   Find the key matrix M.

2. Alice and Bob are using the Diffie–Hellman key exchange scheme. They choose the prime $p = 89$ and the primitive root $g = 7 \bmod p$. Alice's private key is α and her public key is 54. Bob's private key is β and his public key is 11.

   (a) Using the baby-step giant-step algorithm, or otherwise, find α.

   (b) Show that Alice and Bob's shared secret key is 57.

3. Let E be the elliptic curve defined by $y^2 = x^3 + 2x + 1$ over $\mathbb{Q}$. Let $P = (0, 1)$, a point on E.

   (a) Show that $[2]P = (1, -2)$.

   (b) Find $[3]P$.

   (c) Using the Nagell–Lutz theorem, show that P is not a torsion point.

   (d) Deduce that $E(\mathbb{Q})$ is infinite.

University of Durham Copyright

4. The code C is the image of the map $f_A : \mathbb{F}_5^4 \longrightarrow \mathbb{F}_5^5$, so $C = \{xA \mid x \in \mathbb{F}_5^4\}$, where

$$A = \begin{pmatrix} 1 & 0 & 2 & 1 & 1 \\ 1 & 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 & 1 \\ 4 & 0 & 3 & 3 & 2 \end{pmatrix}.$$

   (a) Find a generator-matrix G for C, and show that $k = \dim(C) = 3$.

   (b) Find a check-matrix H for C, and find $d = d(C)$.

   (c) Find parameters $[n_2, k_2, d_2]$ for $C^\perp$, the dual of C.

   (d) Use your matrix G to

      i. encode the message (4,2,0).

      ii. channel-decode the codeword (1,3,1,1,4).

5. Let C be an $[n, k, d]$ code with check-matrix H.

   (a) In lectures we proved that there exists a codeword $c \in C$ with $0 < w(c) \leq m$ if and only if H has m linearly dependent columns. Prove **one** direction of this result, either $\Rightarrow$ or $\Leftarrow$.

   For linear codes, the Singleton Bound says that $d \leq n - k + 1$. Prove this in three different ways:

   (b) by considering a map $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-(d-1)}$.

   (c) by considering the check-matrix H.

   (d) by considering a generator-matrix G in RREF (row-reduced echelon form).

6. Let $C \subseteq \mathbb{F}_2^5$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$.

   (a) Make a syndrome look-up table for this code, and use it to decode the received words $\mathbf{y}_1 = (1, 0, 1, 1, 0)$ $\mathbf{y}_2 = (1, 1, 0, 1, 1)$, and $\mathbf{y}_3 = (0, 1, 0, 1, 0,)$.

   (b) Which of these $\mathbf{y}_i$ has two nearest neighbours in C? Confirm your answer by listing the codewords in C.

   (c) The code is now sent over a binary symmetric channel with symbol-error probability p. Using your table, what is the probability that you will decode a received word correctly (that is, find the codeword that was sent)?

   (d) Let $\widehat{C}$ be the extended code of C. Write down a check-matrix $\widehat{H}$ and a generator-matrix $\widehat{G}$ for $\widehat{C}$.

   (e) If we extend a binary code repeatedly, $C, \widehat{C}, \widehat{\widehat{C}} \ldots$, what happens to the minimum distance? Explain.

University of Durham Copyright

SECTION B

7. Alice and Bob are exchanging messages using the RSA encryption scheme. Alice's public key is (N, e) where N is the public modulus, a product of two primes p and q, and e is the encryption exponent.

   (a) Bob wants to send the message m to Alice, where m is an integer modulo N. Explain how he encrypts m as an integer c modulo N.

   To obtain m from c, Alice uses the equation
   $$m \equiv c^d \mod N$$
   where d is the decryption exponent. Explain how Alice finds d. Your answer should point out where Alice uses information that is known only to her.

   (b) Suppose that Alice's public key is $(N, e) = (58033, 10007)$, and that the decryption exponent is $d = 53343$. Using this information, factorise N.

   You may use the congruence $5^{66725424} \equiv 13467 \mod N$.

   (c) Suppose now that Alice uses a different public key (N, e) and that $e = 3$. Show that
   $$d = \frac{2\phi(N) + 1}{3}.$$
   If, moreover, $p < q < 2p$, show that
   $$\left| d - \frac{2N + 1}{3} \right| < 2\sqrt{N}.$$

8. (a) Let $p = 53$ and let E be the elliptic curve $y^2 = x^3 + 3x + 32$ over $\mathbb{F}_p$. Let $P = (1, 6)$, which is a point of $E(\mathbb{F}_p)$.

   Given that $[3]P = (24, 28)$ and $[32]P = (9, 24)$, show that P has order 67.

   (b) Stating any theorems you use, show that $|E(\mathbb{F}_p)| < 70$. Deduce that $E(\mathbb{F}_p)$ is cyclic of order 67.

   (c) Alice is signing messages using the elliptic curve Elgamal signature scheme. Her public elliptic curve is the elliptic curve E above, and her public generator is the point P of order $n = 67$. Her secret key is an integer $1 \leq \alpha \leq n - 1$ and her public key is $Q = [\alpha]P = (43, 3)$.

   In this scheme, a valid signature on the message m is a pair (R, s) where $R = (x_R, y_R)$ is a point on $E(\mathbb{F}_p)$ with $0 \leq x_R \leq n - 1$, s is an integer with $0 \leq s \leq n - 1$, and the equation
   $$[x_R]Q \oplus [s]R = [m]P$$
   holds.

   Given that:

   - $((2, 29), 38)$ is a valid signature on the message $m = 2$; and
   - $((2, 29), 42)$ is a valid signature on the message $m = 3$,

   find α.

University of Durham Copyright

9. Let p be a prime.

   (a) Show that in $\mathbb{F}_p[x]$ we have $x^p - 1 = (x-1)^p$.

   (b) Determine how many cyclic codes there are in $\mathbf{R}_p = \mathbb{F}_p[x]/(x^p - 1)$.

   (c) Consider the nontrivial cyclic codes in $\mathbf{R}_5 = \mathbb{F}_5[x]/(x^5 - 1)$. (Nontrivial means that $1 < |C_i| < 5^5$.) For each code give the generator-polynomial $g_i(x)$ and a generator-matrix G_i.

   (d) Give the check-polynomial $h_i(x)$ and a check-matrix H_i for each code.

   (e) Show that these codes are dual in pairs.

   (f) Show in general that, if $p \geq 3$, then the cyclic codes in $\mathbf{R}_p$ are dual in pairs. (*Hint:* Pascal's triangle)

10. The Reed-Solomon code $\mathrm{RS}_k(\mathbf{a}, \mathbf{b})$ is the image of the linear map $\varphi_{\mathbf{a},\mathbf{b}} : \mathbb{F}_q[x]_{<k} \longrightarrow \mathbb{F}_q^n$, where $\varphi_{\mathbf{a},\mathbf{b}}(f(x)) = (b_1 f(a_1), \ldots, b_n f(a_n))$.

    (a) Explain briefly why a generator-matrix for $\mathrm{RS}_k(\mathbf{a}, \mathbf{b})$ is given by

$$G = \begin{pmatrix} - & \varphi_{\mathbf{a},\mathbf{b}}(1) & - \\ - & \varphi_{\mathbf{a},\mathbf{b}}(x) & - \\ & \vdots & \\ - & \varphi_{\mathbf{a},\mathbf{b}}(x^{k-1}) & - \end{pmatrix}.$$

    (b) By finding suitable vectors $\mathbf{a}$ and $\mathbf{b}$, show that the code in $\mathbb{F}_7^6$ with generator matrix

$$G_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 6 & 0 & 4 & 4 \end{pmatrix}$$

    is a Reed-Solomon code $\mathrm{RS}_2(\mathbf{a}, \mathbf{b})$. Write down the generator matrix G_3 for $\mathrm{RS}_3(\mathbf{a}, \mathbf{b})$.

    (c) By considering the weights of codewords, show that any $\mathrm{RS}_k(\mathbf{a}, \mathbf{b})$ has $d = n - k + 1$. Because of this we say that $\mathrm{RS}_k(\mathbf{a}, \mathbf{b})$ is *maximum distance separable*, or MDS.

    (d) What does it mean for a code to be *perfect*? Show that an $[11, 6, 5]$ code over $\mathbb{F}_3$ is perfect.

    It was stated in lectures that for $n \leq 1000$, $d \leq 1000$ and $q \leq 100$ the only possible parameters for a (nontrivial, linear) perfect code are:

    - the parameters of the odd binary repetition codes
    - the parameters of the Hamming codes
    - $[23, 12, 7]$ or $[90, 78, 5]$ over $\mathbb{F}_2$, or $[11, 6, 5]$ over $\mathbb{F}_3$.

    (e) Can any codes with these parameters also be MDS? Give the parameters for these perfect MDS codes, in terms of n or q as appropriate.

    (f) Can a Reed-Solomon code be perfect?

University of Durham Copyright