Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May	2018	MATH3401-WE01

Title: Cryptography and Codes III

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:

SECTION A

1. (a) Let A be an alphabet, $|A| = q$. A code $C \subseteq A^n$ is sent over a q-ary symmetric channel with symbol-error probability p. For $c \in C$, $y \in A^n$, explain why

$$p(y \text{ received} \mid c \text{ sent}) = (\frac{p}{q-1})^{d(y,c)}(1-p)^{n-d(y,c)}.$$

(b) Let $A = \{1, 2, 3, 4\}$, and let $C = \{111, 222, 333, 444\} \subseteq A^3$. How many words in A^3 have a unique nearest neighbour in C? How many do not?

This (nonlinear) code C is sent over a 4-ary symmetric channel with symbol-error probability p, and the receivers consider two possible decoding plans:

- Plan A: Use nearest-neighbour decoding if and only if the received word y has a unique nearest neighbour in C. Otherwise do not decode.
- Plan B: Accept y if it is in C. Otherwise ask for retransmission, as often as necessary.

The word 111 is sent.

(c) For each plan, find in terms of p the probability of successfully decoding y back to 111. Explain your answers briefly. If $p = 0.1$, which plan gives a higher chance of eventual success?

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

(a) Find parameters $[n, k, d]$ for C.

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

(c) Show that for **one** of these $\mathbf{y}_i$, different tables could have produced different decodings. How many possible decodings are there for this $\mathbf{y}_i$? Explain briefly, in terms of $d(C)$, how this can happen.

(d) Show that C is **not** MDS (maximum difference separable).

(e) Show that any (non-trivial) binary MDS code must have $k = 1$.
(*Hint:* Consider a check-matrix in standard form $(I|A)$, and the weights of its columns.) What kind of code does this produce?

3. (a) For any prime q, the standard check-matrix for a $\mathrm{Ham}_q(2)$ code is $\begin{pmatrix} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & 2 & \cdots & q-1 \end{pmatrix}$. In terms of q, find parameters $[n, k, d]$ for the q-ary code with this check-matrix, and use them to show that it is perfect.

   (b) Let C_1 be the $\mathrm{Ham}_5(2)$ code with standard check-matrix H_1 as above, and let the 5-ary code C_2 have check-matrix $H_2 = \begin{pmatrix} 3 & 4 & 3 & 4 & 2 & 0 \\ 3 & 2 & 0 & 1 & 4 & 2 \end{pmatrix}$. Show that C_2 is also a $\mathrm{Ham}_5(2)$ code, and equivalent, but not equal, to C_1. Find generator-matrices G_1 for C_1 and G_2 for C_2.

   (c) The message-vector $(1, 2, 3, 4)$ is encoded, sent though the channel, decoded, and finally channel-decoded. Show each stage in this process

      i. using C_1, with received word $\mathbf{y}_1 = (0, 0, 1, 0, 3, 4)$.

      ii. using C_2, with received word $\mathbf{y}_2 = (1, 0, 1, 0, 3, 4)$.

4. Use the following convention to convert alphabetic messages into numbers.

$$\sqcup \to 0, \quad A \to 1, \quad \ldots, Z \to 26. \tag{1}$$

   (a) An affine cipher was used to produce the ciphertext "YFWJLQRFAJ". Suppose you know that the first two letters of the plaintext were "HO", then use this information to find the decryption key. Use this to find the full original plaintext.

   (b) In a chosen plaintext attack on a 2×2 block cipher, Eve finds out that the block cipher converts the message "$\sqcup$A" to "ET", and it converts the message "ZZ" into "AB". Use this information to find the encryption key.

5. (a) Describe Diffie-Hellman key exchange protocol using a prime p and a primitive root g modulo p.

   (b) A key k is exchanged using the Diffie-Hellman key exchange between Alice and Bob using using $p = 97, g = 10$. Suppose that Alice chose the number 35 and Bob choose 67, then find the key k as a number between 0 and 96 using this information.

6. Let $E : y^2 = x^3 - 34x + 37$ be an algebraic curve defined over $\mathbb{Q}$. Let $P = (1, 2)$ and $Q = (6, 7)$ be points over E.

   (a) Compute the discriminant of E and show that this curve is elliptic.

   (b) Compute $P \oplus Q$.

   (c) Compute $P \oplus Q$ mod 5. Using the addition law for $E(\mathbb{F}_5)$, compute $[2](1, 2)$ in $E(\mathbb{F}_5)$. Do both answers match?

SECTION B

7. (a) By considering possible factors, show that $x^3 + x^2 + 1$ is irreducible in $\mathbb{F}_2[x]$.

   (b) Working in the field $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x^2 + 1)$, complete the table below. You must give each x^i in the form $a_2x^2 + a_1x + a_0$, with the a_i in $\mathbb{F}_2$:

i	0	1	2	3	4	5	6	7
x^i	1	x	x^2	x^2+1				

   (c) Let $C = \langle\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}\rangle \subseteq \mathbb{F}_8^5$, where $\mathbf{u} = (1, 0, x, x^2 + x + 1, x + 1)$, $\mathbf{v} = (0, 1, x^2, x^2 + 1, x^2 + x)$, and $\mathbf{w} = (1, x, x^2 + x + 1, 0, x)$. Find a generator-matrix for C, and show that $\dim(C) = 2$.

   (d) Find a check-matrix for C, and show carefully that $d(C) = 3$. Thus there must exist a word $\mathbf{c} \in C$ with weight $w(\mathbf{c}) = 3$; find such a word, in terms of $\mathbf{u}$ and $\mathbf{v}$.

   (e) Consider the following statement, which is **false**: "If code C has a generator-matrix G in RREF, then one of G's rows has weight $d(C)$." Show that the code above is a counter-example to this statement, and find another code, over a different field, which is also a counter-example.

8. Let $C = \{000, 111, 222\} \subseteq \mathbb{F}_3^3$.

   (a) Give parameters $[n, k, d]$, a generator-matrix G and a check-matrix H for C.

   (b) Since C is cyclic, its codewords can also be regarded as polynomials in a certain ring $\mathbf{R}_n$. Specify this ring, and give the generator-polynomial $g(x)$ and check-polynomial $h(x)$ for $C \subseteq \mathbf{R}_n$.

   (c) Let $f_1(x) = 2 + 2x + 2x^2$ and $f_2(x) = x + x^2$ be polynomials in $\mathbf{R}_n$. Use $h(x)$ to check whether they are in C.

   (d) Now consider $C^\perp \subseteq \mathbb{F}_3^3$. List all its codewords; for full marks explain briefly how you do this.

   (e) By finding suitable vectors $\mathbf{a}$ and $\mathbf{b}$, show that C is also a Reed-Solomon code, $\mathrm{RS}_1(\mathbf{a}, \mathbf{b})$. Show that (in this case) we have $C^\perp = \mathrm{RS}_2(\mathbf{a}, \mathbf{b})$.

   (f) Now consider the extended code $\widehat{C}$. Write down a generator-matrix $\widehat{G}$, a check-matrix $\widehat{H}$, and parameters $[\hat{n}, \hat{k}, \hat{d}]$ for $\widehat{C}$.

   (g) Explaining briefly, show that:

   i. $\left(\widehat{C}\right)^\perp \neq \widehat{C^\perp}$

   ii. $\widehat{C}$ is not cyclic

   iii. $\widehat{C}$ is not an RS code.

9. (a) Show that if $x^2 \equiv y^2 \bmod n$, but $x \not\equiv \pm y \bmod n$, then $\gcd(x+y, n)$ cannot be 1 or n. In other words, prove that $\gcd(x+y, n)$ is a proper divisor of n.

   (b) Suppose you want to factor $n = 642401$. Suppose you discover that

   $$516107^2 \equiv 7 \bmod n, \qquad \text{and} \qquad 187722^2 \equiv 28 \bmod n,$$

   then use this information to factor n.

   (c) Suppose you know that

   $$3^6 \equiv 44 \bmod 137, \qquad 3^{10} \equiv 2 \bmod 137.$$

   Find a value of x with $0 < x < 135$ such that $3^x \equiv 11 \bmod 137$.

   (d) i. Explain how the RSA algorithm with public key (n, e) can be used to send a number x to Bob.

   ii. Naive Nelson uses RSA with public key (n, e) to receive a single ciphertext c, corresponding to the message m. Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Evil Eve knows the value of c and sends him the ciphertext $2^e c \bmod n$. Show how this allows Eve to find m.

10. (a) State Hasse's theorem.

    (b) Let E be an elliptic curve $y^2 = x^3 + 7x + 1$ defined over $\mathbb{F}_{101}$. Let $P = (0, 1)$.

    i. Prove that order of P in $E(\mathbb{F}_{101})$ is 116. You may use here that $[4]P = (96, 12), [26]P = (86, 64)$, $32[P] = (22, 81)$.

    ii. Prove that $E(\mathbb{F}_{101})$ is a cyclic group generated by P.
    (Hint: You may use Hasse's theorem here).

    (c) Consider the elliptic curve $E : y^2 = x^3 + 108x + 203$ defined over $\mathbb{Q}$. Prove that the torsion subgroup of E is trivial.
    (Hint: You may reduce this equation modulo primes.)

END