# University of Ruhuna

## Bachelor of Science (General) Degree - Level III (Semester II) Examination - January 2018

**Subject: Applied/Industrial Mathematics**
**Course Unit: IMT321$\beta$ (Applied Algebra - Coding Theory)**
**Time: Two (02) Hours**

**Answer ALL Questions. Calculators will be provided.**

---

**1.** Explain what you mean by "one-way function" and "discrete logarithm".

Consider a communication network with $N$ users $A, B, C, \ldots$. Outline the main steps of the Diffie-Hellman public-key cryptosystem using this network of users.

For a particular **Diffie-Hellman public-key cryptosystem**, one chooses the prime number 23.

(a) Show that 3 is **not** but 5 is a possible generator.

(b) Now suppose that $A$ chooses 7 and $B$ chooses 13 as their private keys. Compute their public keys.

(c) If $A$ and $B$ decided to establish a common secret key, explain how they compute it giving detailed calculations.

---

**2.** Explain the

(i) key generation procedure,

(ii) encryption algorithm, and

(iii) decryption algorithm,

for **basic ElGamal public-key cryptosystem.**

(a) Suppose that Alice selects the prime number 2357 and a generator 2 of the multiplicative group $\mathbb{Z}_{2357}^*$. If Alice chooses 1751 as her private key, compute Alice's public key.

(b) Suppose Bob wants to send the plaintext $m = 2035$ to Alice. If Bob selects a random integer 1520, then show how he computes the ciphertext $c$.

Explain how Alice decrypts the ciphertext $c$ she received.

---

**3.** (a) Determine whether the string `0-1392-4101-4` is a valid ISBN (International Standard Book Number).

(b) Explain the following terms giving examples:

(i) Hamming weight $w(c)$ of a codeword $c$,



**Continued.**

(ii) Hamming distance $d(x, y)$ between two codewords $x, y$, and

(iii) Minimum (Hamming) distance $d(C)$ of a code $C$.

What is the minimum distance of the binary repetition code of length 5? Justify your answer.

(c) Explain clearly the meanings of the following:

(i) $C$ is a $t$-error detecting code,

(ii) $C$ is a $t$-error correcting code.

A binary linear code called Hamming code is given by [7,4,3]. Determine how many errors it can correct.

(d) State the sphere-packing bound for a $t$-error correcting $q$-ary code with $M$ codewords each of length $n$.

Suppose that we want a binary code to have 4 codewords and to be 2-error correcting. Check the above bound for codewords of length 3 and 7. Hence, show that we can have such a binary code if we use codewords of length 7 or more.

---

**4.** Consider a (5,2) binary linear code $C$ with the generator matrix

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

(a) Write down the code $C$.

(b) Find the cosets of $C$.

(c) Find the coset leader of each coset.

(d) Find a parity check matrix for $C$.

(e) Construct the Slepian standard array for this problem.

(f) Extend the standard array in part (c) by listing the syndromes of each coset leader in an extra column on the right.

(g) Suppose that the vector 01101 is received. Apply syndrome decoding algorithm to decode the received vector to obtain the transmitted codeword.

---