University of Ruhuna

Bachelor of Science General Degree
Level III (Semester II) Examination - January 2022

Subject: Industrial Mathematics
Course Unit: IMT 321β (Algebraic Data Encryption & Decryption Methods)
Time: Two (02) hours

Answer All questions
Calculators provided by the university are allowed.

---

1. a) What are the meanings of following terms in Cryptography:
   (i) Plaintext
   (ii) Ciphertext
   (iii) Encryption
   (iv) Decryption

[Marks(20)]

b) In RSA public key cryptosystem,

(i) Describe the steps of generating the public and private keys.

(ii) Let p and q be primes such that $p = 7$ and $q = 17$ respectively. If Alice chose the encryption key as 5 then show that Bob's private key is $(119, 77)$.

(iii) Alice wants to send a message $P = 19$ to Bob. If she encrypts the message using the public key $(119, 5)$, then determine the ciphertext.

[Marks(50)]

c) Alice and Bob agreed to use the prime number 17 and base 3 in the Diffie-Hellman key exchange. If Alice and Bob choose secret values as 5 and 12 respectively, then compute the shared secret key.

[Marks(30)]

---

2. a) (i) Write down the elements of $GF[2^3]$ in binary form.

(ii) Consider two polynomials $f_1(x)$ and $f_2(x)$ such that $f_1(x) = 1 + x^2 + x^3$ and $f_2(x) = 1 + x^2 + x^4$. Find the product and sum of these two polynomials over $GF(2)$.

[Marks(30)]

b) (i) What are the meanings of reducible polynomial and irreducible polynomial over a field? Explain each term by giving an example.

Continued...

(ii) Suppose that $R = \mathbb{Z}_3[x]$ and $q(x) = x^2 + 1$. Show that the ring R/qR is a field, and determine the number of elements in the field R/qR.

(iii) Find the generators of the cyclic multiplicative group $\mathbb{Z}_3^*$.

[Marks(40)]

c) Determine the greatest common divisor of the following pair of polynomials over $GF(11)$ by using the Euclidean algorithm

$$x^3 - 5x^2 + 10x - 8 \quad \text{and} \quad x^3 - 4x^2 + 7x - 6.$$

[Marks(30)]

---

3. a) (i) Explain clearly what are the types of errors in transmission of digital information over a channel.

(ii) Explain the concept of Parity check error detection method.

[Marks(30)]

b) In the Cyclic Redundancy Check (CRC) method in $\mathbb{F}_2$, assume that given message for transmission is 1100 and the generator polynomial is $g(x) = x^3 + x + 1$.

(i) What is the transmitted message after implementing CRC encoder?

(ii) Write down the transmitted message in polynomial form.

(iii) Determine whether the received message 1100110 with the generator 1011 has detectable errors or not in CRC method. State clearly the steps you use.

[Marks(50)]

c) Determine the 8−bit check sum for the 32− bit message block given below and write down the message as it would be transmitted.

10001001 00011001 10101001 00100100

[Marks(20)]

---

4. a) Explain the procedure of $[7, 4]$ Hamming code creation proposed by R.W. Hamming.

[Marks(20)]

b) A $[7, 4]$ linear block code C over $GF(2)$ is defined by the following parity check matrix,

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

Continued...

(i) Find the generator matrix of C.

(ii) Construct the equations for obtaining the parity bits.

(iii) Find the encoded codeword of the message 1010.

[Marks(45)]

c) Let some of the codewords in binary [5, 4] code are given by

$$c_0 = (00000), \quad c_1 = (10110), \quad c_2 = (01011), \quad c_3 = (11101).$$

Discuss the Linearity property of the above [5, 4] code.

Calculate the rate and error correcting capacity of the code.

[Marks(35)]
