M.Sc. (MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE)

M.Sc. (MACS)

Term-End Examination

June, 2021

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours | *Maximum Marks : 50*

(Weightage : 50%)

Note :

(i) Question no. ***1*** *is* ***compulsory****.*

(ii) Answer any ***four*** *questions from questions no. 2 to 6.*

(iii) The use of calculators is ***not*** *allowed.*

---

1. State whether the following statements are *True* or *False*. Give reasons for your answers. *10*

(i) $(Z_{16}, +, \cdot)$ is a field.

(ii) The main purpose of a cryptographic hash function is compression of messages.

(iii) RSA is a block cipher.

(iv) The Repeated Squaring Algorithm is a probabilistic algorithm.

(v) DES is a secure tool for encryption.

2. (a) Encrypt the message "PROTECT YOURSELF WITH A MASK" using the affine cipher $x \mapsto (7x + 5) \bmod 26$ and the encoding of characters

$$A \to 0, B \to 1, C \to 2, \ldots, Z \to 25.$$

What is the key space of the affine cipher defined over $\mathbb{Z}$? *4*

(b) Find the decryption key d of the RSA cryptosystem when the public key is $n = 77$ and $e = 43$. *3*

(c) Encrypt the message 1101 0011 1001 using the toy block cipher with the key 101 110 011. *3*

$$S_1 \begin{bmatrix} 101 & 010 & 001 & 110 & 011 & 100 & 111 & 000 \\ 001 & 100 & 110 & 010 & 000 & 111 & 101 & 011 \end{bmatrix}$$

$$S_2 \begin{bmatrix} 100 & 000 & 110 & 101 & 111 & 001 & 011 & 010 \\ 101 & 011 & 000 & 111 & 110 & 010 & 001 & 100 \end{bmatrix}$$

3. (a) Let $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. We represent the field $\mathbb{F}_2$ by $\mathbb{F}_2[x]/\langle f(x) \rangle$ and we write $\gamma = x + \langle f(x) \rangle$. Use the table given below and construct corresponding logarithm and antilogarithm tables :

i	γ^i	Vector	i	γ^i	Vector
0	1	(0,0,0,1)	8	$\gamma^2 + 1$	(0,1,0,1)
1	γ	(0,0,1,0)	9	$\gamma^3 + \gamma$	(1,0,1,0)
2	γ^2	(0,1,0,0)	10	$\gamma^2 + \gamma + 1$	(0,1,1,1)
3	γ^3	(1,0,0,0)	11	$\gamma^3 + \gamma^2 + \gamma$	(1,1,1,0)
4	$\gamma + 1$	(0,0,1,1)	12	$\gamma^3 + \gamma^2 + \gamma + 1$	(1,1,1,1)
5	$\gamma^2 + \gamma$	(0,1,1,0)	13	$\gamma^3 + \gamma^2 + 1$	(1,1,0,1)
6	$\gamma^3 + \gamma^2$	(1,1,0,0)	14	$\gamma^3 + 1$	(1,0,0,1)
7	$\gamma^3 + \gamma + 1$	(1,0,1,1)			

Compute $\dfrac{(\gamma^4 + \gamma^2 + 1) + (\gamma^3 + \gamma)}{(1 + \gamma + \gamma^3)(1 + \gamma^2 + \gamma^7)}$ using the logarithm and antilogarithm tables. *6*

(b) Suppose Lisa sets up an El Gamal cryptosystem with p = 19, 2 as the primitive root and secret value 5.

(i) What values should she make public ?

(ii) Balu uses the system and sends the pair (14, 17). Find the message. *4*

4. (a) Prove that if n has k distinct odd prime factors, then $2^k \mid n$. *3*

(b) Susheela wants to use the Digital Signature Algorithm for signing messages. She chooses q = 11, p = 23, g = 5, and the secret value 3. Alia wants to sign the message M = 7. For signing she chooses the value k = 2. Find the digital signature. *4*

(c) Give an advantage of the OFB mode of operation over the CFB mode. Also explain a disadvantage of the OFB mode. *3*

5. (a) Apply the poker test to test the randomness of the following sequence with level of significance $\alpha = 0{\cdot}05$. *5*

100110100001000010111101101110100101

101100100110

[You may find the following values useful : $\chi^2_{0\cdot05,\,1} = 3{\cdot}84146$, $\chi^2_{0\cdot05,\,3} = 7{\cdot}81473$,

$\chi^2_{0\cdot05,\,4} = 9{\cdot}48773$]

(b) Check whether the polynomial $x^6 + x^5 + 1 \in \mathbb{F}_2[x]$ is irreducible. *5*

6. (a) Solve the equation $5^x \equiv 3 \pmod{23}$ using the baby-step giant-step method. *5*

(b) Find a recurrence that generates the sequence 110110110110110. *5*