No. of Printed Pages : 5 **MMTE–006**

M. SC. (MATHEMATICS WITH APPLICATION IN COMPUTER SCIENCE)

[M.SC. (MACS)]

Term-End Examination

December, 2025

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

Note : *(i) There are 6 questions in this paper and the 6th is compulsory.*

(ii) Do any four from questions 1 to 5.

(iii) Use of calculators is not allowed.

(iv) Show all relevant steps.

1. (a) Write the difference between stream ciphers and block ciphers. Give one example each of a stream cipher and a block cipher. 4

   (b) Write the names of modes of operations in block ciphers. Explain CBC Mode. 4

   (c) Explain the AKS algorithm. 2

2. (a) Consider a sequence of length $n = 80$ obtained by repeating the following sequence ten times :

   11010 00111 10101 11100 01010 11001 11000 00101.

   Test the sequence for randomness using frequency and serial test. You may find the following values useful : $\chi^2_{0.05,2} = 5.99146$, $\chi^2_{0.05,1} = 3.841146$.

   7

(b) What is primitive root of a finite field ? Check whether 5 is a primitive root of $\mathbf{Z}_{17}$. 3

3. (a) Construct the addition table for a finite field of order 8, i.e., $\mathbf{F}_{2^3}$. 4

(b) What is the length of the key in DES. How long is the actual key and what are the extra bits used for ? 3

(c) Find $17^6 \pmod{61}$ using the repeated squaring algorithm. 3

4. (a) Solve the equation $10^x = 52 \pmod{59}$ using the Baby-Step Giant-Step algorithm. 6

(b) Find the result of multiplying $f(x) = 1 + x + x^2 + x^4 + x^6$ with $g(x) = 1 + x + x^4$ mode $m(x) = 1 + x + x^3 + x^4 + x^8$ in $\mathbf{F}_2(x)$. 4

5. (a) Bano has published the public parameters (119, 11) for her signature using the RSA digital signature algorithm. Calculate her signature for the message M = 10. 7

   (b) Encrypt the string :

   ICAMEISAWICONQUERED

   using Vigenére cipher with keyword, 'VIGENERE'. 3

6. Which of the following statements are true and which are false ? Justify your answer :

   (a) AKS algorithm is a probabilistic algorithm. 2

   (b) Finding factors of composite 'n' is same as finding $\phi(n)$, given $n = pq$ (p & q are primes). 2

(c) CBC mode generates same ciphertext for same block of plaintext. 2

(d) If $\bar{a}$ and $\bar{b}$ are in $\mathbf{F}_p$, $0 \le a \le p^{-1}$, $0 \le b \le p^{-1}$ and g is a generator of $\mathbf{F}^*_p$, the discrete logarithm of $\bar{a}$ with respect to g is less than the discrete logarithm of $\bar{b}$ with respect to g if $a < b$. 2

(e) The RSA system is secure for all choices of modulus of encryption. 2

× × × × ×