No. of Printed Pages : 3

MMTE-006

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

M.Sc. (MACS)

00428

Term-End Examination

June, 2015

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Attempt any **five** out of six questions. Use of calculator is **not** allowed.*

1. (a) Check whether the polynomial $f(x) = 1 + x^3 + x^6 \in Z_2[x]$ is irreducible with the help of algorithm that checks the irreducibility of polynomials over finite fields. *4*

(b) Explain the working of RC4 Stream Cipher (KSA & PRGA). *6*

2. (a) Solve the equation $5^x \equiv 22 \bmod 97$ using the baby-step, giant-step algorithm. *4*

(b) Explain Rabin-Miller Test for testing whether a large odd positive integer N is probably prime or composite. Also apply this test and state steps to check whether

(i) N = 897 is composite,

(ii) N = 53 is probably prime. *6*

3. (a) Explain Davis-Mayer method for constructing hash function with the help of a diagram. *3*

(b) Encrypt the plaintext "WE ARE BRAVE MEN TO FIGHT WAR" :

(i) By using simple columnar transformation cipher of width 5. *2*

(ii) By using key 53124 to permute columnar transformation of width 5. *2*

(iii) By using the keyword "TOOTH" of length 5 with Vigenere Cipher represented as integer mod 26 in keyword and plaintext. *3*

4. (a) Construct a finite field F_{24} using the primitive polynomial $1 + x + x^4$ and taking α as the primitive element $x + < 1 + x + x^4 >$ over $\mathbf{Z}_2[X] / < 1 + x + x^4 >$. Find Logarithmic Table and Antilogarithmic Table. *4*

(b) Explain the Substitution Transformation and construction of the S-box of AES. *6*

5. (a) Calculate 5^9 mod 41 by repeated squaring algorithm for integers showing all steps. *4*

(b) Write Algorithm for ElGamal Signature Generation and Key Verification. Also explain Diffie-Hellman Key Exchange based on Discrete Log Problem. *6*

6. Briefly explain the following :

(a) Cryptographically secure pseudo-random bit generator *2*

(b) Counter mode of operation of block cipher (both encryption and decryption) *4*

(c) Computational Diffie-Hellman problem *2*

(d) Confusion and diffusion in the context of a cryptosystem *2*