No. of Printed Pages : 3

MMTE-006

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

M.Sc. (MACS)

00612

Term-End Examination

December, 2014

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Attempt any **five** out of **6** questions. Use of calculators is **not** allowed.*

1. (a) Check whether the polynomial $f(x) = 1 + x + x^2 + x^5 + x^6 \in Z_2[x]$ is irreducible with the help of an algorithm that checks the irreducibility of polynomials over finite fields. *4*

(b) Given the sequence 111111000111111000..., find the recurrence that generates it. *6*

2. (a) Using Extended Euclidean Algorithm find gcd (f(x), g(x)), where

$$f(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^8$$

$$g(x) = 1 + x + x^2 + x^5.$$

Also find polynomials a(x), b(x) and d(x) in $Z_2[x]$ such that $d(x) = a(x) f(x) + b(x) g(x)$. *6*

(b) What are the monoalphabetic and polyalphabetic substitution ciphers ? Compare them from the point of view of method for cryptanalysis. *4*

3. (a) Use the keyword 'GATE' to encrypt the plaintext 'I STOOD FIRM TO FIGHT WAR' by Vigenère Cipher. *3*

(b) Assuming a block size of 64-bits and that each character is represented by 8-bits, what will be the string you get by applying Merkle-Damgard strengthening to the string "tobeatornottobeat" ? *3*

(c) Explain the four basic steps in the round function of AES. *4*

4. (a) In a long string of ciphertext, which was encrypted by means of an affine map on single-letter message units in the 26-letter alphabets, the most frequent letters are "K" and "H". Assuming that these ciphertext message units are encryption of "T" and "S", respectively, decrypt the ciphertext "DHKVVOUDEHKIKMIHK". *6*

(b) In a field with 2^8 elements and generator polynomial $p(x) = 1 + x + x^3 + x^4 + x^8$, find the product of the bytes $a = 10011011$ and $b = 00010100$ considered as elements of the field. *4*

5. (a) Define Cryptographic Hash Function and Keyed Hash Function. What are the advantages of using Keyed Hash Function ? *5*

(b) Consider ElGamal Scheme with common prime n = 19 and primitive root $\alpha = 10$. Bob has public key $y_B = 3$ and Alice chooses a random integer k = 6. What is the ciphertext of message M = 17 ? *5*

6. (a) Define pseudo prime, strong pseudo prime and Carmichael number. Prove that Carmichael number has at least three distinct prime factors. *5*

(b) In a RSA public key cryptosystem the ciphertext sent to a user with public key e = 13, n = 33 is intercepted. If the intercepted ciphertext is c = 8, what is the plaintext M ? *5*