Name : ....

Roll No. : ....

Invigilator's Signature : ....

CS/M.Tech (ECE)/SEM-2/MCE-204A/2011

2011

CRYPTOGRAPHY AND NETWORK SECURITY

Time Allotted : 3 Hours Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

GROUP – A

(Multiple Choice Type Questions)

1. Choose the correct alternatives for the following : 10 × 1 = 10

i) A cryptanalysis refers to

a) Cracking encryption algorithms

b) Security mechanisms

c) Encryption mechanism

d) Protocol designers.

ii) Polyalphabetic cipher belongs to the category of

a) Polygraphic b) Transposition

c) Substitution d) None of these.

iii) DES is which of the following cipher types ?

a) Block b) Stream

c) Transposition d) None of these.

iv) In the context of cryptography, Enigma implementation implies

a) Hacking b) Decryption

c) Linguistics d) Encryption.

v) In a disrupted transposition cipher, certain position of grid are filled with

a) Arbitrary characters b) Blanks

c) Ones d) Zeroes.

vi) The only unbreakable cipher is

a) LOKI 97 b) One-time pad

c) SEAL d) None of these.

vii) Passive attack in cryptography refers to

a) Release of Message b) Traffic analysis

c) None of these d) Both (a) and (b).

viii) A back door is a feature programmers use for

a) to fix bugs

b) to store additional information

c) to erase unwanted data

d) none of these.

ix) The fixed Data Encryption Standard uses a plaintext of *N* bits, where *N* is

a) 64 b) 128

c) 256 d) None of these.

x) The Hashed Message Authentication Code (HMAC) are based on

a) Single Hash Function

b) Two Hash Functions

c) Several Hash Functions

d) Keyless Hash functions.

GROUP – B
(Short Answer Type Questions)

Answer any *three* of the following. 3 × 5 = 15

2. State a few applications of cryptography. Encrypt the following message :

   ATTACK BEGINS AT DAWN HOLD TIGHT using a Rail-Fence cipher using three rails.

3. Explain with an example the meaning of Anagram. What is meant by columnar transposition ?

4. Discuss the security of Caesar Cipher. How is it related to ROT-13 algorithm ?

5. What are the differences between Cryptography and Steganography ? Compare between Substitution ciphers and Transposition Ciphers.

6. Explain the role of cryptography in network security.

GROUP – C

(Long Answer Type Questions)

Answer any *three* of the following. 3 × 15 = 45

7. Explain with an example the Double transposition cipher and distinguish it from the Myszkowski Transposition cipher. How is cryptanalysis performed in case of transposition ciphers ? What is the key in ROT-13 algorithm ?

8. What is the Vigenere cipher ? Give an example of Vigenere cipher. Explain the security of Vigenere cipher. What are the variants of Vigenere cipher ?

9. Elaborate the key principles of security. What are the Security Attacks and Security Mechanisms as defined by the OSI Security Architecture ? What is Replay attack ?

10. Explain in details the operation of Date encryption, Standard encryption and decryption process. What is meant by Triple DES ?

11. Discuss the authentication requirements and authentication functions. Explain the operations of Secure Hash algorithm.

12. Write short notes on any *two* of the following :

    a) Man-In-The-Middle Attack

    b) Bijective Function

    c) Advance applications of Network Security

    d) Electronic Code Book.