Printed Pages – 3 Roll No. : .....

322734(22)

B. E. (Seventh Semester) Examination, Nov.-Dec. 2021

(New Scheme)

(CSE, IT Engg. Branch)

CRYPTOGRAPHY and NETWORK SECURITY

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : *Attempt all questions. Part (a) of each question is compulsory and containing 2 marks. Attempt* ***two*** *parts from (b), (c) and (d) and each part carries 7 marks each.*

1. (a) Define cryptography, cryptology and cryptoanalysis.

(b) List the security attacks. Explain all types of security

attacks with example.

(c) Explain the principle of DES with its strength in cryptography standardization.

(d) Differentiate between symmetric and asymetric key cryptography.

2. (a) Define block and stream Cipher.

(b) Explain the working of AES in brief.

(c) Write and explain encryption algorithm for RC4.

(d) Write the properties of group, ring and field.

3. (a) Define Euler's Totient function.

(b) Explain RSA public key cryptography.

(c) Differentiate between conventional and public key encryption.

(d) Explain the key exchange problem in Public key and Private key cryptography.

4. (a) Define Hash function and its usage.

(b) What is digital signature? Explain the working mechanism of digital signature with suitable diagram.

(c) What are the requirement of message authentication? Explain it with functions.

(d) Explain H-MAC algorithm briefly.

5. (a) Define computer virus.

(b) Explain secure electronic transaction (SET) in detail.

(c) Explain the working of firewall architecture with its different types.

(d) What is web security? Explain in detail Secure Socket Layer. (SSL).