(c) Explain Diffie-Hellman scheme for exchange of secret key. How it is used for key exchange and vulnerable to man-in-the-middle-attack?

6. (a) Explain the full service of kerberos environment. What are the principle differences between version four and version five of kerberos?

(b) Why authentication and confidentiality are important in pretty good privacy (PGP)?

(c) Explain the following :

(i) Firewall

(ii) Secure socket layer protocols

⌘⌘⌘

S.No. : 205 BCS3702

No. of Printed Pages : 04

Following Paper ID and Roll No. to be filled in your Answer Book.

PAPER ID : 33231 Roll No. 1 2 2 0 4 4 0 0 3 8

B. Tech Examination 2025-26

Odd Semester

NETWORK SECURITY AND CRYPTOGRAPHY

Time : Three Hours] *[Maximum Marks : 60*

Note :– Attempt all questions.

SECTION – A

1. Attempt all parts of the following : $8 \times 1 = 8$

(a) What is Fermat's little theorem?

(b) What are the properties of digital signature?

(c) Differentiate between message integrity and message authentication.

(d) Differentiate between substitution and transposition cipher.

(e) What do you mean by cryptanalysis?

(f) Explain transport layer security.

(g) Find GCD (1970, 1066).

(h) Explain Shannon's confusion and diffusion.

SECTION – B

2. Attempt any two parts of the following : $2 \times 6 = 12$

(a) Differentiate between monoalphabetic and polyalphabetic cipher and give one example for each.

(b) In a public key system using RSA, you intercept the cipher text C=10 sent to a user whose public key is e=5, n=35. What is the plaintext?

(c) What is fermat's theorem? Explain it and prove 6^10 mod 11.

(d) Difference between secure socket layer (SSL) and transport layer security (TLS).

SECTION – C

Note:- Attempt all questions. Attempt any two parts from each question. $5 \times 8 = 40$

3. (a) Explain IP security architecture and define secure socket layer protocols.

(b) Draw general structure of DES and explain encryption and decryption process.

(c) Define Euler's totient function $\Phi(n)$. Calculate $\Phi(36)$ and $\Phi(100)$.

4. (a) Explain advanced encryption standard and its operations.

(b) Describe Brute force attacks and SHA.

(c) Why message authentication is required?

5. (a) Explain chinese remainder theorem. Explain its various applications.

(b) What is discrete logarithmic problem? Find all primitive roots of 25.

[P. T. O.