S.No. : 382 BCS3702

No. of Printed Pages : 03

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

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

B. Tech Examination 2023-24

(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 : $1 \times 8 = 8$

   (a) Distinguish between active and passive attacks.

   (b) Define padding in block cipher.

   (c) Write any two applications of RSA algorithm.

   (d) What do you understand by Diffie-Hellman Protocol?

   (e) What are the two categories of digital signature?

[P. T. O.

(f) Explain the difference between Hash function and Encryption?

(g) What is Kerberos?

(h) List any two applications of x.509 certificate.

SECTION – B

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

(a) Differentiate between block cipher and a stream cipher.

(b) Elaborate on Fermat's and Euler's theorem.

(c) Elucidate the digital signature standard.

(d) Describe the cryptographic algorithm used in S/MIME.

SECTION – C

Note:- Attempt any two parts from each question. Each part carry equal marks. $8 \times 5 = 40$

3. (a) Explain Cipher feedback mode.

(b) Compare the substitution and transposition Cipher techniques.

(c) Explain symmetric key encryption model with a neat diagram.

4. (a) What is primality test? Explain in brief.

(b) Describe the RSA algorithm.

(c) Discuss about the concept of key exchange using Deffie Hellman algorithm.

5. (a) List and explain the properties of Hash function.

(b) Explain the working of digital signature with the help of neat and clean diagram.

(c) Explain the four stages of AES algorithm.

6. (a) How does PGP (pretty good privacy) provide confidentiality and authentication service for e-mail? Explain.

(b) Briefly explain the architecture of SSL.

(c) Write short note on firewall.

⌘⌘⌘