BTICS504N

B.Tech.(CSE-ICS)

V Semester Examination, June-July 2024

Network Security and Cryptography

Choice Based Credit System (CBCS)

Time: 3 Hrs.

Maximum Marks: 60

Minimum Pass Marks: 24

Note: (1) *All questions carry equal marks, out of which part 'A' and 'B' carry 3 marks and part 'C' carries 6 marks.*
(2) *From each question, part 'A' and 'B' are compulsory and part 'C' has internal choice.*
(3) *Draw neat diagram, wherever necessary.*
(4) *Assume suitable data wherever necessary.*

Q.1.(A) Explain the principle of Security.   03

(B) What are some common threats that can compromise network security?   03

(C) Provide examples of methods that ensure strong authentication.   06

OR

Write short notes on (Any Two):

(a) Honeypots, (b) Access Controls, (c) Wired Equivalent Privacy.

Q.2.(A) What role do proxy servers and anonymizers play in internet browsing?   03

(B) Explain the concept of Key Range and Key Size.   03

(C) What are some methods hackers use to crack passwords?   06

OR

How do substitution techniques alter the original message in cryptography?

Q.3.(A) What is the main principle behind symmetric key cryptography?   03

(B) How does Double DES enhance security compared to single DES?   03

(C) How does IDEA differ from other encryption algorithms like DES or AES?   06

OR

How does the DES algorithm encrypt and decrypt data?

Q.4.(A) How does asymmetric key cryptography ensure secure communication?   03

(B) What is the purpose of the Diffie-Hellman Key Exchange?   03

(C) How does the RSA algorithm encrypt and decrypt data?   06

OR

How do symmetric and asymmetric key cryptography work together to secure data transmission?

Q.5.(A) What does authentication mean in computer security? 03

(B) How does SSL ensure secure communication over the internet? 03

(C) What are the limitations of steganography? 06

OR

How do PGP and S/MIME ensure the confidentiality and integrity of emails?

xxxxxxx