Program/Sem:	**T.Y.B.Sc CS – Sem - V**	**Course:**	**Information and Network Security**
Program Code:	**1S00195**	**Course Code:**	**USCS502**

Duration: **2 ½ Hour** 0 4 NOV 2025 **Max. Marks:** **75**

Instructions:

1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Draw neat diagrams wherever necessary.

Q. 1 Attempt ANY FOUR from the following: **[20]**

a) Describe the main components of a simple symmetric cipher model. Explain with a suitable diagram.

b) Differentiate between substitution and transposition techniques in cryptography.

c) Using a simple columnar transposition cipher, encrypt the given plaintext message. Plaintext: CYBERSECURITY , Key: GERMAN

d) Explain any two types of active attacks with suitable illustrations.

e) Explain in detail the Feistel network structure used for both encryption and decryption operations.

f) What are the various types of security mechanisms employed to protect information systems?

Q. 2 Attempt ANY FOUR from the following: **[20]**

a) Describe the structure and components of an X.509 digital certificate.

b) Discuss in detail the Kerberos authentication process, including its message exchanges and ticketing mechanism.

c) Explain the working of the HMAC (Hash-based Message Authentication Code) algorithm.

d) Write a note on the public key cryptosystem and its significance.

e) Define a digital signature and explain its purpose in data integrity and authentication.

f) John and Sara want to communicate securely using the Diffie-Hellman Key Exchange method. Given the following parameters:
Prime number p=11, Generator g =2, John's private key = 4, Sara's private key = 3
Calculate John's public key, Sara's public key. Using the public keys, compute the shared secret key.

Q. 3 Attempt ANY FOUR from the following: **[20]**

a) Define S/MIME (Secure/Multipurpose Internet Mail Extensions) and highlight its key features.

b) Write a brief note on S/MIME and its role in secure email communication.

c) Explain the concept and functioning of Secure Electronic Transaction (SET) protocol.

d) Explain the architecture of IP security (IPSec).

e) Describe the structure of Pretty Good Privacy (PGP) encryption.

f) List and describe any five types of computer viruses.

Q. 4 Attempt ANY FIVE from the following: **[15]**

a) Explain the working principle of the Cipher Feedback (CFB) encryption mode.

b) Define a Message Authentication Code (MAC) and its purpose.

c) List and describe any three important features of cryptographic hash functions.

d) Define the rail fence cipher and its basic operation.

e) Describe the life cycle of a computer virus, highlighting its main stages.

f) Using Caesar cipher with key size = 4, encrypt the message:
"secure the network immediately"

--X--X--