Paper / Subject Code: 37472 / Cryptography and System Security

Duration: 3hrs **[Max Marks:80]**

N.B. : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

1 Attempt **any FOUR** **[20]**

a Describe services and mechanisms.

b ECB and CBC block cipher.

c Why digital signature and digital certificates are required?

d What is keyed and keyless transposition ciphers?

e Explain clickjacking and session hijacking.

2 a Explain DES algorithm with reference to following points: **[10]**

1. Block size and key size
2. Need of expansion permutation
3. Role of S-box
4. Possible attacks on DES

b Use the playfair cipher with the keyword “example” to encipher “The algorithm name is playfair cipher” **[10]**

3 a What are properties of hash function? Compare MD-5 and SHA hash algorithm. **[10]**

b Explain Diffie hellman key exchange algorithm. **[10]**

4 a What do you understand by digital signatures and digital certificates? Explain digital signature scheme RSA. **[10]**

b Explain memory and address protection in detail. Write a note on file protection. **[10]**

5 a Enlist various functions of protocols of SSL. Explain the phases of handshake protocol. **[10]**

b Briefly explain database security. What do you understand by multilevel database security. **[10]**

6 Write short notes on **any four:** **[20]**

a Web browser attacks

b X.509

c Cross site request forgery

d DNS attack

e Email attacks.
