14IT605

Hall Ticket Number:

III/IV B.Tech (Supplementary) DEGREE EXAMINATION

November,2019 **Information Technology**

Sixth Semester **Cyber Security**

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

Answer Question No.1 compulsorily. (1X12 = 12 Marks)

Answer ONE question from each unit. (4X12=48 Marks)

1 Answer all questions (1X12=12 Marks)

a) Define Authentication.
b) Categorize cryptographic systems based on various parameters.
c) List the design features of Feistel cipher.
d) Mention the four possible approaches for attaching the RSA algorithm.
e) Why discrete logarithms are preferred for private keys?
f) What are the ingredients of public key cryptosystems?
g) Describe the requirements of cryptographic hash function H.
h) Suggest any three situations in which MAC is used.
i) Why brute force attack on a MAC is more difficult?
j) What is a replay attack? Mention the counter measures.
k) Define Kerberos Realm.
l) Write the limitations of packet filter firewall.

UNIT I

2 a) List and explain various X.800 security attacks and services. 8M

b) Encrypt the message "Attack is postponed until tomorrow" with Playfair Cipher using the key "Cryptography". 4M

(OR)

3 a) With a neat sketch explain the operations in a single round of DES algorithm. What is the role of avalanche effect on DES strength? 6M

b) Explain the Triple DES algorithm and the Known-Plaintext attack on it. 6M

UNIT II

4 a) Differentiate conventional and public key encryption techniques. 4M

b) Perform encryption and decryption using the RSA algorithm on the following data 8M
i) p=11, q=13,e=11, M=7 ii) p=17, q=31, e=7, M=2.

(OR)

5 a) With a suitable example explain Diffie-Hellman key exchange algorithm. 6M

b) Illustrate the man-in-the-attack against Diffie-Hellman key exchange algorithm. 6M

UNIT III

6 a) Describe the step-wise procedure for generating message digest using SHA-512. 8M

b) Explain the hash functions based on cipher block chaining. 4M

(OR)

7 a) Discuss the HMAC design objectives and algorithm. 8M

b) What are the requirements of digital signature? 4M

UNIT IV

8 a) Explain the techniques used for distribution of public keys. Write the pros and cons for each technique. 6M

b) Draw the X.509 version1 and version2 certificate formats. 6M

(OR)

9 a) Describe public key infrastructure. 8M

b) How mutual trust is established using a chain of public key certificates. 4M