

TCS-606/TIT-606

B. TECH. (CS/IT) (SIXTH SEMESTER) END SEMESTER EXAMINATION, 2018

NETWORK AND CYBER SECURITY

Time : Three Hours

Maximum Marks : 100

Note : (i) This question paper contains five questions with alternative choice.

(ii) All questions are compulsory.

(iii) Instructions on how to attempt a question are mentioned against it.

(iv) Each part carries ten marks. Total marks assigned to each question are **twenty**.

1. Attempt any *two* questions of choice from (a), (b) and (c). (2×10=20 Marks)

(a) Explain various types of Active attacks and Passive attacks.

(b) Encrypt the following message :

(i) "secure" using playfair cipher with key money

(2) TCS-606/TIT-606

(ii) "enemy attacks tonight" using double transposition cipher

with key $k_1 = [3 \ 1 \ 4 \ 5 \ 2]$ and $k_2 = [4 \ 5 \ 1 \ 2 \ 3]$

(c) Explain Data Encryption Standard with its round description.

2. Attempt any *two* questions of choice from (a), (b) and (c). (2×10=20 Marks)

(a) Explain how key is exchanged using Diffie-Hellman Algorithm.

Suppose prime no $p = 13$ and its primitive root $g = 6$, alice chooses $a = 3$ as his private key and bob chooses $b = 10$ as his secret key, now find the secret key generated for both of them using Diffie-Hellman Algorithm.

(b) Explain how public and private keys are generated using RSA. Find public and private key when $p = 17$, $q = 11$ and $e = 7$.

(c) Find least residue using Fermat little theorem :

(i) $4^{532} \% 11$

(ii) $2^{50} \% 17$

(3)

3. Attempt any *two* questions of choice from (a), (b) and (c). (2×10=20 Marks)

(a) Explain Message authentication code and its requirement in Cyber security.

(b) Explain Message Digest Algorithm.

(c) Explain how hash code is generated to authenticate a message using Secure Hash Algorithm.

4. Attempt any *two* questions of choice from (a), (b) and (c). (2×10=20 Marks)

(a) What is PGP ? Discuss the operational description services provided by PGP.

(b) Explain secure socket layer services with encryption and decryption techniques used in SSL.

(c) Write the function of S/MIME.

5. Attempt any *two* questions of choice from (a), (b) and (c). (2×10=20 Marks)

(a) Explain different kinds of buffer overflow attacks.

(b) Write Digital Signature Algorithm to generate digital signature for message authentication.

(c) Explain various internal attacks.

TCS-606/TIT-606

420