Printed Pages – 4 Roll No. : .....

328840(28)

APR-MAY 2022

B. E. (Eighth Semester) Examination, ~~2020~~

(New Scheme)

(ET & T Engg. Branch)

CRYPTOGRAPHY & SECURE COMMUNICATION

Time Allowed : Three hours

Maximum Marks : 80

Minimum Pass Marks : 28

Note : *Part (a) of each question is compulsory carry 2 marks. Attempt any two parts from (b), (c) and (d) each carries 7 marks.*

Unit-I

1. (a) List of all additive inverse pairs in modulas 20.

(b) Find the multiplicative inverse of each of the following integers in Z_{180} using the extended Euclidean algorithm.

(i) 38

(ii) 24

(c) Define greatest common divisor of two integers. Which algorithm can effectively find the greatest common divisor and how?

(d) Define discrete logarithms and explain their importance in solving logarithmic equation.

Unit-II

2. (a) Define active attacks and passive attacks.

(b) Encrypt the message "today is holiday" :

(i) Using Caesar cipher

(ii) Using playfair cipher with keyword 'CSVTU'

(c) Explain DES algorithm with respect following points :

(i) General structure

(ii) Initial permutation

(iii) Number of rounds and round function

(iv) Strengths of DES

(d) Consider a Deffie-Hellman scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$:

(i) Show that 2 is a primitive root of 11.

(ii) If user B has public key $Y_A = 9$, what is A's private key $X_A = ?$

(iii) If user B has public key $Y_B = 3$, what is the shared secret key K, shared with A?

Unit-III

3. (a) What is the role of compression function in Hash function?

(b) What basic arithmetical and logical functions are used in SHA?

(c) What is the difference between a message authentication code and a one-way hash function?

(d) What are some threats associated with a direct digital signature scheme?

Unit-IV

4. (a) What is the difference between transport mode and tunnel mode?

(b) What are the services provided by the IPSec? Discuss the IP security architecture?

(c) Explain the role of key management in IPSec.

(d) List and explain in brief the four techniques used by firewalls to control access and enforce a security policy.

Unit-V

5. (a) What protocols comprise SSL?

(b) What are services provided by the SSL record protocol? Differentiate SSL connection and SSL session.

(c) How does the dual signature provide linking between two messages that are intended for two different recipients? Explain.

(d) List and briefly define the principal categories of SET participants.