Exam.Code:0923
Sub. Code: 6848

2021
B.E. (Information Technology)
Fifth Semester
ITE-503: Network Security and Cryptography

Time allowed: 3 Hours Max. Marks: 50

NOTE: *Attempt five questions in all, including Question No. 1 which is compulsory and selecting two questions from each Unit.*

x-x-x

I. Attempt the following:-

a) What is discrete logarithm problem?

b) What is factorization problem?

c) What is the use of Format's theorem in security?

d) What do you mean by one-way property in hash functions?

e) What is a dictionary attack?

f) Draw model of network security including cryptal analysis.

g) What do you mean by security parameters negotiation?

h) What do you mean by primitive root?

i) What is avalanche effect?

j) What is collision resistance? (10x1)

UNIT – I

II. What do you mean by mutual authentication? Design two authentication protocols using a) Asymmetric b) Symmetric cryptography such that man/woman in the middle, and replay attacks could be avoided? (2+4+4)

III. "Design a secure mailing system for UIET. The proposed system should have confidentiality, integrity and non-repudiation of messages exchanged, 'the proposed system should be computationally efficient. Assume your first name as symmetric encryption function, your roll no as assumed symmetric key for secure exchange and encryption and decryption, your last name as hash function, PU as public key of mail server and your nickname as your private key. (10)

IV. What do mean by Triple AES? Explain working of AES in detail. (10)

P.T.O.

UNIT – II

V. Explain ElGamal encryption system for public-key cryptography. Why this system is able to thwart man-in-the middle attack? Give mathematical proof of this algorithm. (8+2)

VI. You are required to implement secure web access in your organisation. Which protocol will you use for the purpose? Explain secure connection establishment and protocol to encrypt messages in details with suitable diagrams. (5+5)

VII. You are required to implement secure online question paper transmission for Panjab University. Use various protocols of IPSec to implement the same. Illustrate with suitable diagrams.

x-x-x