U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

August 2022 Semester End Main Examinations

Programme: B.E | **Semester: VI**
Branch: Information Science and Engineering | **Duration: 3 hrs.**
Course Code: 20IS6PCCNS | **Max Marks: 100**
Course: Cryptography and Network Security | **Date: 10.08.2022**

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

PImportant Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

UNIT - I

1 a) Using Playfair cipher, encrypt the following PT: "The Key is hidden under the door" with Key: domestic. **06**

b) For the given Ciphertext "gzscxnzeukadoahdryfslv" apply Hill Cipher and decrypt the message using the following Key = [5 17 4 15]. Apply Column wise technique of solving Hill Cipher. **08**

c) Using Double transposition technique decrypt the message **06**
"EXMEEEXAFHSEEHOLTISARLBTTTSRSM" applying the key: 413256

UNIT - II

2 a) Explain in detail Feistel Cipher Structure with its design principles and parameters. **10**

b) Perform Key generation and Encryption using S-DES. Details are given below, assume input 10-bit key, K is: 1010000010 **10**
Plaintext : 01110010

IP							
2	6	3	1	4	8	5	7

E/P							
4	1	2	3	2	3	4	1

P10 = [3, 5, 2, 7, 4, 10, 1, 9, 8, 6] P8 = [6, 3, 7, 4, 8, 5, 10, 9]
P4 = [2, 4, 3, 1] IP^{-1} =[4, 1, 3, 5, 7, 2, 8, 6]

S0 =

	c0	c1	c2	c3
r0	1	0	3	2
r1	3	2	1	0
r2	0	2	1	3
r3	3	1	3	2

S1 =

	c0	c1	c2	c3
r0	0	1	2	3
r1	2	0	1	3
r2	3	0	1	0
r3	2	1	0	3

UNIT - III

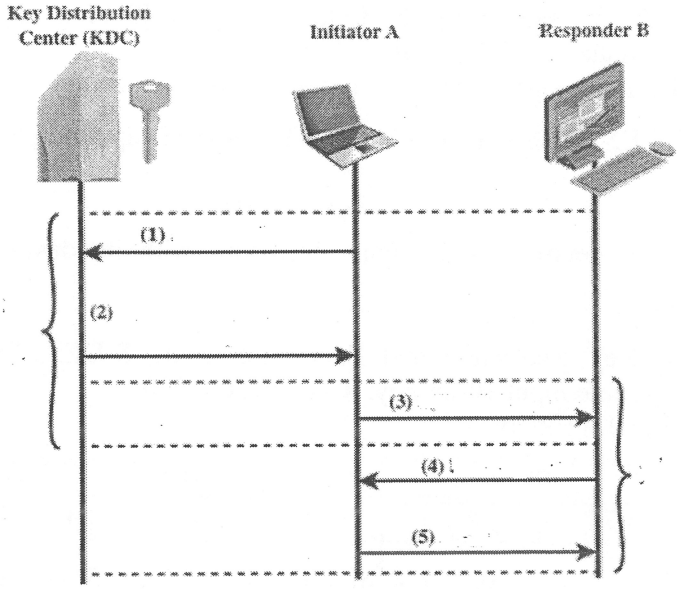
3 a) Applying RSA cryptosystem, Sita uses two prime numbers p = 13 and q =17 to generate her public and private keys. Given the public key of Sita is 35 and calculate the private key of Sita. Assume the message Sita sends is the codeword 10 to Rama in the encrypted format and Rama decrypts the message after receiving and identifies the codeword what sita have sent. **10**

b) Suppose that two parties A and B wish to setup a common secret key between themselves using the Diffie-Hellman Key exchange technique. They agree on 7 as the prime number and 3 as the primitive root. Party A chooses 2 and Party B chooses 5 as their respective secrets and calculate the Diffie Hellman Key at A and B. **06**

c) Mahesh wants to send a message to his friend Rahul which should be authenticated. Mahesh wants to maintain secrecy in the message transmission following a cryptosystem which addresses his requirements. Identify the cryptosystem and Illustrate with a neat diagram the scenario. **04**

UNIT - IV

4 a) Analyze the given figure and complete the steps from 1 to 5 and name the stages and explain the process of key distribution in detail. **10**



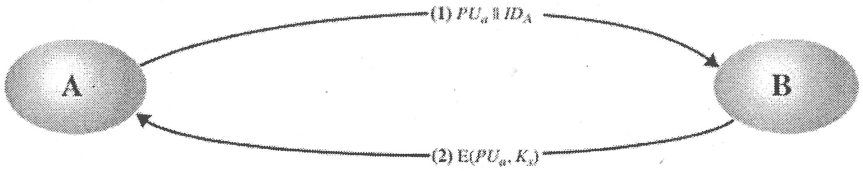
b) List and Explain some alerts that are fatal in Alert Protocol **05**

c) Compare between Publicly available directory and Exchange of Public-Key Certificate key distribution techniques. **05**

OR

5 a) Explain the process of establishing a secure session by using TLS Handshake protocol with neat diagram. **10**

b) Identify the key distribution technique followed in the below mentioned figure. Analyze the scenario where the adversary(attacker) is trying to intercept the messages sent from A to B and then relay the intercepted message or substitute another message what type of attack is possible in this scenario. Describe the attack in detail with diagrammatic representation. **10**



UNIT - V

6 a) Distinguish between Transport-Mode and Tunnel-Mode techniques in IPsec ESP service. **10**

b) Describe the process of IP Traffic Processing with Outband Packets. **10**

OR

7 a) Elaborate the SCHNORR algorithm to provide authentication of data. **08**

b) Explain the process of NIST DSA to avoid modifications of data during communications. **06**

c) Identify the IPSec document categorization groups with RFC standard 4301, security architecture for internet the protocol. **06**

******