U.S.N.										

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

Autonomous Institute Affiliated to VTU

September / October 2023 Supplementary 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

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

UNIT - I

1 a) Illustrate Passive attacks and Active attacks by taking two examples for each attack **06**

b) Using the Playfair cipher, Encrypt the plaintext "needsecurity" with the key "MTECH". **06**

c) Encrypt the message "safe messages" using the key "ciphering" using Hill Cipher. **08**

UNIT - II

2 a) Justify how DES operates on 64-bit blocks using key size of 56 bits. **06**

b) Identify which cipher technique is used for RSA algorithm RC4 algorithm. Differentiate the technique based on complexity, number of bits used and algorithm modes. **06**

c) Perform Key generation and Encryption using S-DES. Details are given below, assume input 10-bit key, K is: 1010000010 **08**
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) Perform encryption and decryption using RSA Algorithm. for the following: P=5; q=11; e=3; M=9. **06**

	b)	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged?	**06**
	c)	With a neat diagram, give the steps associated with SHA-512 Logic.	**08**

UNIT - IV

4	a)	Discuss different ways of distributing public keys.	**06**
	b)	If 'A' is the initiator and 'B' is the responder, With a neat diagram, explain the general scenario of key distribution.	**08**
	c)	Define Alert protocol. List and explain any five fatal alerts.	**06**

OR

5	a)	List the parameters of TLS Session and Connection. Give the functionalities of the same.	**06**
	b)	Given a scenario where the user A browses www.google.com on his web browser. Illustrate the process of http connection establishment and connection closure.	**08**
	c)	Illustrate how Symmetric key is distributed with Confidentiality and Authentication.	**06**

UNIT - V

6	a)	Distinguish between Transport-Mode and Tunnel-Mode techniques in IPsec ESP service.	**06**
	b)	List the applications and illustrate the benefits of IPSec during the communication between the user and the public network.	**06**
	c)	Examine the forgery attacks while sharing the document between different users.	**08**

OR

7	a)	Illustrate the DSA approach with neat sketch for signing and verification.	**06**
	b)	With a neat diagram, explain the ESP packet format	**06**
	c)	Explain the Header and Payload formats of Internet Key Exchange in a transport protocol.	**08**

******