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: VII**
Branch: ES – Cluster Elective **Duration: 3 hrs.**
Course Code: 19EC7CE2NC **Max Marks: 100**
Course: Networks Security and Cryptography **Date: 22.09.2023**

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) With diagram explain network security model. **05**

   b) Encrypt the plaintext paymoremoney using Hill cipher with the key **05**

$$\begin{pmatrix} 17 & 7 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

   c) Use double transposition cipher to encrypt the text "the purpose of our lives is to be happy" with the encryption key "21534" **05**

   d) Using play fair method, key *flag*, Encrypt: **05**
   "indiaismycountry".

UNIT - II

2. a) With diagram explain DSA Signing and verifying. **05**

   b) In S-DES Obtain the cipher text for the given 8 bit plain text **05**
   (1 0 1 0 0 1 0 1) , K1 = 10100100 and K2= 01000011 to generate cipher text, Consider IP= (2,6,3,1,4,8,5,7) , E/P =(4,1,2,3,2,3,4,1),
   P4 = (2,4,3,1) and IP^{-1} = (4,1,3,5,7,2,8,6).

$$S0= \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \qquad S1= \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

   c) Consider a Diffie – Hellman scheme with a common prime q = 97 and primitive root α = 13. If user A has private key X_A=36 and user B has private key X_B =58, compute the secret key of user A & user B. **05**

   d) Derive an expression for message authentication and confidentiality in which authentication is tied to plaintext with diagram. **05**

OR

3.	a)	Perform encryption and decryption using RSA algorithm for the following data; p=17, q=7, e=17, M=88.	**05**
	b)	With diagram explain key generation in DES.	**05**
	c)	Discuss the different modes of block Cipher operation.	**10**

UNIT - III

4.	a)	With relevant diagram explain PGP message generation.	**07**
	b)	Who are the participants of SET protocol and what are the sequence of events required for transaction?	**07**
	c)	With relevant diagram explain UNIX password scheme.	**06**

OR

5.	a)	With relevant diagram explain card holder purchase request.	**07**
	b)	With relevant diagram explain different types of firewalls.	**06**
	c)	Explain the phases of virus in its life time. Discuss various types of viruses.	**07**

UNIT - IV

6.	a)	Describe the various methods for extracting evidence from systems and provide examples of helpful and relevant tools.	**10**
	b)	How do you create a forensic backup in computer forensics?	**10**

UNIT - V

7.	a)	Describe the JAVA implementation of a realistic cryptographic solution.	**10**
	b)	Describe how to use Microsoft to create a viable cryptography implementation.	**10**

*****