U.S.N.										

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

Autonomous Institute Affiliated to VTU

September / October 2022 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 | **Date: 26.09.2022**

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) Explain the attacks involved in modification of data stream and eavesdropping of transmissions. **10**

b) Apply hill cipher algorithm to decrypt the message "*SAKNOXAOJX*" using the following a key. $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$ **10**

UNIT - II

2 a) With a neat diagram, give the cipher technique used to encrypt block of plain text and digital data stream. **10**

b) Show that DES decryption is, in fact, the inverse of DES encryption **10**

UNIT - III

3 a) Show with proper math how the basic Diffie Hellman Key Agreement would happen between two endpoints A and B where the modulo prime chosen is 19 the generator is 3 A and B chose their secret numbers as 29 and 39 respectively **08**

b) Perform encryption and decryption using the RSA algorithm, for the following: $p = 7$; $q = 11$, $e = 17$; $M = 8$ **06**

c) How Hash Functions are used for Message Authentication. Explain the usage of hash functions in different scenarios. **06**

UNIT - IV

4 a) List the strength of any cryptographic system with the key distribution technique give an example with neat sketch. **10**

b) With a neat diagram. Explain the general scenario of Key Distribution system between the users A and B. **10**

OR

5 a) 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. **10**

	b)	Justify how protection against both active and passive attacks using the Secret key distribution with confidentially and authentications is performed.	**10**

UNIT - V

6	a)	Sketch the Simplified Depiction of Essential Elements of Digital Signature Process and explain it.	**10**
	b)	List the major security services provided by AH and ESP respectively defined by IETF. Give example for each.	**10**

OR

7	a)	Illustrate the procedure of NIST DSA to avoid modifications of data during communication.	**10**
	b)	Explain the mechanism used for authentication and confidentiality in IP security association	**10**

******