U.S.N | | | | | | | | | | |

P.E.S. College of Engineering, Mandya - 571 401

(An Autonomous Institution affiliated to VTU, Belagavi)

Eighth Semester, B.E. - Computer Science and Engineering

Semester End Examination; May/ June - 2019

Cryptography and Network Security

Time: 3 hrs *Max. Marks: 100*

***Note**: Answer **FIVE** full questions, selecting **ONE** full question from each unit.*

UNIT - I

1	a.	Categorize Passive and Active attack and explain.	10
	b.	Briefly explain the security service and mechanisms defined under X800 standards.	10
2	a.	Explain the extended Euclidean algorithm.	10
	b.	What are the different transposition cipher techniques? Explain.	10

UNIT - II

3	a.	How meet in the middle attack is done in 2-DES?	5
	b.	Distinguish between diffusion and confusion.	5
	c.	Give the detailed description of key generation and encryption of IDEA algorithm.	10
4	a.	Give the structure of AES. Explain how Encryption /Decryption is done in AES?	10
	b.	Briefly explain the characteristics of AES to analyse.	10

UNIT - III

5	a.	Explain Sieve of Eratathenes method to find all primes less than *n* with example.	10
	b.	Describe Chinese remainders theorem and explain its applications.	10
6	a.	Explain RSA crypto system structure.	10
	b.	Explain ElGamal crypto system with example.	10

UNIT - IV

7	a.	Explain Needham-Schroeder protocol.	10
	b.	Discuss Diffie-Hellman Key Agreement.	10
8	a.	Describe the general structure of electronic-mail (e-mail) system.	10
	b.	Discuss the content of MIME / SMIME.	10

UNIT - V

9	a.	Discuss how to calculate master secret from pre-master secret in cryptographic generation?	10
	b.	Explain four protocols of SSL.	10
10	a.	What is transport mode and tunnel mode? Explain about the scope of AH and ESP in these modes.	10
	b.	For a Diffie-Hellman protocol, list some weakness and explain how to eliminate before it is suitable for IKE.	10

* * * *