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 - 2018

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.	Discuss the security services and mechanisms.	8
	b.	Differentiate between substitution cipher and transposition cipher.	5
	c.	Find Cipher text for "HELLO" using additive cipher (Key = 15).	7
2	a.	Explain additive and multiplicative inverse of an integer with example.	10
	b.	Explain different types of attacks threatening confidentiality, integrity and availability.	10

UNIT - II

3	a.	Discuss the DES structure in detail.	10
	b.	Explain Criteria, Rounds and Data units with respect to AES.	10
4	a.	What are the key-expansion mechanisms in AES that are designed to provide several features that thwart the crypt analyst?	10
	b.	Explain the design criteria and properties of DES analysis.	10

UNIT - III

5	a.	Explain trial division factorization method with pseudocode.	10
	b.	Explain RSA crypto system with an example.	10
6	a.	Discuss i) Euler's Phi-function ii) Chinese Remainder problem.	10
	b.	Discuss message authentication code with diagram.	6
	c.	Explain Rabin crypto system for encryption.	4

UNIT - IV

7	a.	Explain Needham-Schroeder protocol with diagram.	10
	b.	Explain different scenarios of PGP with message format.	10
8	a.	Explain private and public ring table with example.	10
	b.	Discuss MIME in detail.	10

UNIT - V

9	a.	Explain SSL services and key exchange algorithms.	10
	b.	Discuss Two security protocols of IPsec : i) Authentication header ii) Encapsulating Security Payload (ESP)	10
10	a.	Explain Phase-III and Phase-IV of handshake protocol.	10
	b.	Explain any five payloads along with payload format diagram of ISAKMP.	10

* * * *