CBCS SCHEME

USN

15TE71

Seventh Semester B.E. Degree Examination, July/August 2021
Cryptography and Network Security

Time: 3 hrs. Max. Marks: 80

Note: ***Answer any FIVE full questions.***

1	a.	Explain Euclidean algorithm. Give an example to find the GCD of two large numbers.	(08 Marks)
	b.	Define group, ring, field and cyclic group.	(08 Marks)
2	a.	State and prove Fermat's and Euler's theorem.	(08 Marks)
	b.	Explain substitution Ciphers.	(08 Marks)
3	a.	With a neat diagram, explain Feistel Cipher.	(08 Marks)
	b.	Explain the AES encryption and decryption process with a neat diagrams.	(08 Marks)
4	a.	Distinguish between conventional and public key crypto systems.	(04 Marks)
	b.	What requirement must a public key cryptosystem fulfill to be a secure algorithm?	(06 Marks)
	c.	Explain RSA algorithm.	(06 Marks)
5	a.	Explain N-Hash algorithm with a neat diagram.	(08 Marks)
	b.	Explain secure Hash algorithm.	(08 Marks)
6	a.	Explain digital signature algorithm.	(08 Marks)
	b.	Explain any four MAC.	(08 Marks)
7	a.	Explain the various phases of SSL handshake protocol action.	(08 Marks)
	b.	Explain the two SSL concepts with their prarameters.	(08 Marks)
8	a.	Explain SSH protocol stack.	(08 Marks)
	b.	Explain the different phases of operation in IEEE 802.11i Robust security network.	(08 Marks)
9	a.	Explain PGP message transmission and reception with a neat diagram.	(08 Marks)
	b.	Explain functions and cryptographic algorithms used in S/MIME functionality.	(08 Marks)
10	a.	With a neat diagram, explain an IP security scenario.	(08 Marks)
	b.	Explain the ESP packet format.	(08 Marks)

* * * * *

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.