

Total No. of Pages : 02

Roll No.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Total No. of Questions : 09

B.Tech. (IT) (Sem.-6)

CRYPTOGRAPHY AND NETWORK SECURITY

Subject Code : BTIT610-18

M.Code : 79629

Date of Examination : 01-12-2023

Max. Marks : 60

Time : 3 Hrs.

INSTRUCTIONS TO CANDIDATES :

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.
3. SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.

SECTION-A

1. Write briefly :
 - a) Define Cryptography.
 - b) Discuss CIA model.
 - c) What is Block Cipher?
 - d) What is the purpose of AES?
 - e) Discuss Kerberos.
 - f) Write about RSA Algorithm.
 - g) What are Digital signatures?
 - h) Define PGP.
 - i) Give concept of honeypots.
 - j) Write about IDS.

SECTION-B

2. What is Passive attack? Give an example of passive attack on network system.
3. How Euclidean algorithm is useful in Network Security applications?
4. Write the functioning and role of DES algorithm in cryptography.
5. Discuss the need of Hash Function and how they are implemented.
6. Write a short note on Network security controls.

SECTION-C

7. Explain the need of Math Background to implement the cryptography concepts.
8. What is the concept of MD5 and SHA Algorithm? How it is used in Cryptography?
9. Discuss about design and types of Firewalls. How they are used in securing the Computer Networks?

NOTE : Disclosure of Identity by writing Mobile No. or Making of passing request on a page of Answer Sheet will lead to UMC against the Student.