

(Following Paper ID and Roll No. to be filled in your Answer Books)

Paper ID : 2289951

Roll No.

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

B.TECH.

Regular Theory Examination (Odd Sem - VII), 2016-17

CRYPTOGRAPHIC AND NETWORK SECURITY

Time : 3 Hours

Max. Marks : 100

Note : Attempt all Sections. If required any missing data; then choose suitably.

SECTION - A

1. Attempt all questions in brief. (10×2=20)
- What are the different security attacks
 - Explain field with example
 - What is message authentication code
 - Explain Intrusion detection.
 - Differentiate between virus and firewalls
 - Explain email security
 - Differentiate between public key and private key
 - What are the different security mechanism
 - What is Kerberos
 - What is IP security.

SECTION - B

2. Attempt any three of the following : (3×10=30)
- a) i) What is Ideal Block Cipher
 - ii) Explain Shannon Principle of confusion and Diffusion
 - b) Explain Chinese remainder theorem with example
 - c) Discuss the basic use of Message authentication code with suitable diagrams.
 - d) Explain Diffie - Hellman key Exchange
 - e) What are the different security threats. What is Firewall

SECTION - C

3. Attempt any one part of the following : (1×10=10)
- a) Explain DES with diagram.
 - b) Explain different block cipher mode of operation
4. Attempt any one part of the following : (1×10=10)
- a) State and prove Euler theorem.
 - b) Explain RSA using example
5. Attempt any one part of the following : (1×10=10)
- a) Write the objective of HMAC. Describe the HMAC algorithm.
 - b) Explain Elgamal Digital signature scheme.

6. Attempt any one part of the following : (1×10=10)
- a) Explain PGP and S/MIME
 - b) Explain X.509 in detail.
7. Attempt any one part of the following : (1×10=10)
- a) Explain the ESP format. What is anti replay service.
 - b) Discuss Secure Electronic Transaction (SET)