D 41407 **(Pages : 2)** **Name..**

Reg. No...

EIGHTH SEMESTER B.TECH. (ENGINEERING) [2014 SCHEME] DEGREE EXAMINATION, APRIL 2018

Electronics and Communication Engineering

EC 14 805 C—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours Maximum : 100 Marks

Part A

Answer any **eight** *questions.*

1. With block diagram, explain the model of conventional cryptosystem.

2. Explain the simplified DES scheme.

3. What is a CTR mode of Block CIPHER ? List its advantages.

4. What is the principle of public key cryptosystem ? What are six ingredients of it ?

5. Explain the techniques for distribution of public keys.

6. State the axioms to be obeyed an abelian group G.

7. Enumerate and explain the attacks in the context of communication across a network.

8. What are the requirements for a digital signature ? Explain.

9. What are the contents of Trust Flag Byte ? Explain.

10. What are the types of Firewalls ? Explain.

(8 × 5 = 40 marks)

Part B

11. (a) With block diagram, explain the model for network security.

Or

(b) With the network illustration and decryption algorithm, explain the Fiestel Cipher.

12. (a) Discuss in detail about RSA algorithm, its computational aspects, encryption, decryption and key generation process.

Or

(b) Describe Diffie-Hellman key exchange algorithm.

Turn over

13. (a) Describe the basic uses of hash functions.

Or

(b) (i) What are the two classes of authentication protocols ? Explain.

(ii) Describe the steps of Digital Signature Algorithm (DSA).

14. (a) (i) Summarise the PGP services. (10 marks)

(ii) List the Tunnel mode and Transport mode functionality. (5 marks)

Or

(b) (i) List the design goals for a firewall. (5 marks)

(ii) How to achieve security against Trojan Horse attack ? Explain. (10 marks)

[4 × 15 = 60 marks]