

C 80578

(Pages : 2)

Name
Reg



**EIGHTH SEMESTER B.TECH. (09 SCHEME) (ENGINEERING DEGREE)
EXAMINATION, APRIL 2015**

EC/PTEC 09 804 L11—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours

Maximum : 70 Marks

Part A

Answer **all** questions.

1. Modification in an attack on what ?
2. What is trapdoor one way function ?
3. What is Repudiation ?
4. What is meant by computation resistance ?
5. In PGP how 128 bit random numbers are generated ?

(5 × 2 = 10 marks)

Part B

Answer any **four** questions.

6. Explain about ceaser cipher.
7. How sessionkey lifetime is selected ?
8. State any five properties of Hash functions.
9. Explain about reference monitor concept.
10. What is tunnel model AH ? Explain.
11. Explain the DSS approach of digital signatures.

(4 × 5 = 20 marks)

Part C

Answer **all** questions.

12. (a) Discuss the operation of DES algorithm.

Or

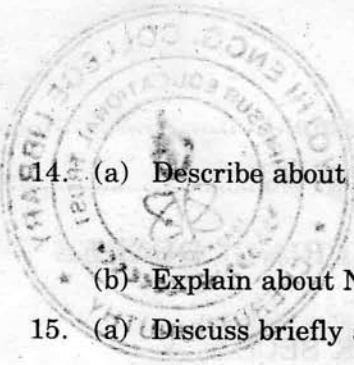
- (b) Explain about model of network security and transposition techniques.

13. (a) Explain the Diffie-Hellman keyexchange algorithm.

Or

- (b) With an example, explain RSA algorithm and key crypto systems.

Turn over



14. (a) Describe about Digital Signature standard and Authentication function.

Or

(b) Explain about Needham/Schroeder protocol and block chaining technique.

15. (a) Discuss briefly about S/MIME.

Or

(b) Describe the security architecture of IP.

(4 × 10 = 40 marks)