C 41655 (Pages : 2) Name..............................

Reg. No..............................

EIGHTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION APRIL 2013

EC/PTEC 09 804 L11—CRYPTOGRAPHY AND NETWORK SECURITY

(2009 admissions)

Time : Three Hours Maximum : 70 Marks

Part A

Answer **all** *questions.*

1. What is denial of service ?
2. Why Elliptic curve cryptography is better than R.S.A. ?
3. What is weak collision resistance and strong collision resistance ?
4. What happens if a k value used in creating a D.S.A. signature is compromised ?
5. What is the purpose of Anti-replay window in IPSEC.

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*

6. Determine the cipper text for plain text using double transposition technique :

   Key : 4 3 1 2 5 6 7

   Plain text : Danger disperse

7. Explain the electronic code book mode.
8. For E_{11} (1, 6) consider the point G = (2, 7). Compute the multiples of G from 2G through 3G.
9. In an RSA, the public key of a given user is $e = 31$, $n = 3599$? What is the private key ?
10. Why brute-force attack on a MAC is difficult ? Explain.
11. In PGP the signature is generated before compression, explain why ?

(4 × 5 = 20 marks)

Part C

12. Explain in detail about DES.

Or

13. Discuss briefly the classical encryption techniques with suitable example.

14. Describe the operation of Diffie–Hellman key exchange.

Or

15. Discuss briefly about elliptic curve cryptography.

Turn over

16. Describe in detail the requirements and functions of Authentication.

Or

17. Explain in detail about Authentication protocol.

18. Explain the architecture of IP Sec

Or

19. Write briefly about design of firewalls.

(4 × 10 = 40 marks)