G 1675 (Pages : 2) Reg. No.....

Name.....

B.TECH. DEGREE EXAMINATION, MAY 2015

Eighth Semester

Branch : Electronics and Communication Engineering

EC 010 804 L 03—SECURE COMMUNICATION [Elective—III] (EC)

(New Scheme—2010 Admission Onwards)

[Regular/Supplementary]

Time : Three Hours Maximum : 100 Marks

Part A

Answer **all** *questions.*
Each question carries 3 *marks.*

1. Evaluate $(4 \times 3 - 1) / 2$ with respect to the finite field $\mathrm{GF}(5) = \{0, 1, 2, 3, 4\}$.
2. Bring out the consequences of using a one-time pad in 'depth' (use an example).
3. Explain the double transposition cipher with the help of an example.
4. What information must a public key certificate contain ?
5. Why is it a good idea to hash passwords that are to be stored in a file ? What is a 'salt' and why should 'salt' be used whenever passwords are hashed ?

(5 × 3 = 15 marks)

Part B

Answer **all** *questions.*
Each question carries 5 *marks.*

6. Define a *field*. What is a *Galois field* ? Let a, b and c be any three elements in a field. Then prove that for $a \neq 0$, $a.b = a.c$ implies that $b = c$.
7. Define the terms *Confidentiality, Integrity* and *Availability.*
8. Differentiate between differential and linear crypt analysis.
9. Distinguish between public key and private key cryptography.
10. Give short notes on Honey pot.

(5 × 5 = 25 marks)

Turn over

Part C

Answer **all** *questions.*
Each question carries 12 *marks.*

11. Let $p(x) = 1 + x + x^4$ is a primitive polynomial over GF(2). Then construct the extended field GF(2^4). If α is one of the roots of the given primitive polynomial within the field GF(2^4), evaluate the following :

    (a) α^{12} / α^5.

    (b) $1 + \alpha^5 + \alpha^{10}$.

Or

12. What is a primitive polynomial ? Determine whether the polynomial $p(x) = x^3 + x^2 + 1$ over GF (2) is primitive.

13. With suitable example clearly explain Hill cipher.

Or

14. Describe how a Playfair cipher differs from a simple substitution cipher with the help of an example. What are its major advantages ?

15. Discuss the shift row and mix column transformation techniques in Advanced Encryption Standard.

Or

16. Discuss about DES encryption.

17. Why is it a bad idea to use the same RSA key pair for both signing and encryption ?

Or

18. Discuss about the Public Key Infrastructure (PKI).

19. Explain rule based and anomaly based intrusion detection systems.

Or

20. Discuss about Intrusion Detection System and compare it with firewall.

(5 × 12 = 60 marks)