IT010 802 **Reg. No _______________**

Name _________________

B.TECH DEGREE EXAMINATION, MAY 2014

Eight Semester

Branch: Information Technology

IT010 802 CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours **Max. Marks: 100**

PART A

Answer all questions

Each carries 3 marks

1. Using Fermat's Little theorem find the multiplicative inverse of 8 in Z_{17}
2. Write down the difference between public key and private key cryptosystems
3. List out the parameters of AES
4. List out the functionality of S/MIME
5. What is an Intruder? Name three different classes of intruders

PART B

Answer all questions

Each carries 5 marks

6. Explain any two methods for testing prime numbers.
7. Using play fair cipher algorithm encrypt the message using the key "MONARCHY" and explain
8. Describe about Hash functions
9. Write short notes on PGP
10. Explain about Distributed Denial of Service attacks

PART C

Answer all questions

Each carries 12 marks

Module I

11. Explain about Chinese Remainder theorem and Euler's theorem with suitable examples.

OR

12. (a) Solve the set of following three equations:

$$3x+5y+7z \equiv 3 \pmod{16}$$
$$x+4y+13z \equiv 5 \pmod{16}$$
$$2x+7y+3z \equiv 4 \pmod{16}$$

(b) What is the remainder after dividing 3^{50} by 7?

Module II

13. Explain the Key Generation, Encryption and Decryption of DES algorithm in detail.

OR

14. Discuss the classical cryptosystems.

Module III

15. Discuss discrete logarithms and explain briefly about Diffie Hellman key exchange algorithm with its pros and cons.

OR

16. (a) Write a detailed note on Digital signatures.

(b)Write the notes on ECC encryption, decryption and security.

Module IV

17. Explain X.509 Authentication service.

OR

18. Explain Kerberos.

Module V

19. Explain in detail about definition, characteristics, types and limitations of firewalls.

OR

20. Explain in detail types and countermeasures related to viruses.