BE/BTECH DEGREE EXAMINATION MAY/JUNE 2012

IT2352-CRYPTOGRAPHY AND NETWORK SECURITY

PART –A(10X2=20 MARKS) **MAXIMUM :100 MARKS**

1. Define LFSR sequence.
2. Define finite filed
3. What do you mean by differential cryptanalysis?
4 define factoring.
5. Distinguish between differential and linear cryptanalysis
6. Write down the difference between the public key and private key cryptosystems
7. Define TLS
8. What do you mean by S/MIME?
9. Write down the system security standards.
10. Define intrusion

PART-B(5X16=80)

11 A) Explain about chinese remainder theorem.

OR

B) Explain Any Two Types Of Cipher Technique In Detail

12 A) Explain About Triple DES With An Example

OR

B) Explain About RC4 Algorithm

13A) WRITE NOTES ON BIRTHDAY ATTACK

OR

WRITE THE ALGORITHM OF MD5 AND EXPLAIN

14A) DESCRIBE ABOUT IP SECURITY

OR

B) LIST OUT THE PARTICIPANTS OF SET SYSTEM AND EXPLAIN IN DETAIL

15A) EXPLAIN THE VARIOUS TYPES OF FIREWALLS.

OR

B) EXPLAIN ABOUT THE MALICIOUS SOFTWARE.