

8E5002

Roll No. _____

[Total No. of Pages : 2]

8E5002

B. Tech. VIII Semester (Main/Back) Examination-2014
Computer Science
8CS2 Information System and Securitics
(Common for 8 CS 2 & 8 IT 2)

Time : 3 Hours**Maximum Marks : 80****Min. Passing Marks : 24****Instructions to Candidates:**

Attempt any **five** questions, selecting **one** question from **each** unit. All questions carry **equal** marks. (Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.)

Unit - I

1. What do you mean by abelian group? Prove that a set of integer under addition $(\mathbb{Z}, +)$ is an abelian group? (16)

OR

1. Explain the following with example
- Fermat's little theorem.
 - Euler's Totient function.
 - Euler's theorem
 - Discrete logarithm
- (16)

Unit - II

2. What are the basic difference between passive and active attack? Explain the following cryptographic technique
- Substitution technique
 - Transposition technique.
- (16)

OR

2. What do you mean by link to link and end to end encryption. Explain the concept of confusion and diffusion in block cipher? (16)

Unit - III

3. Explain the concept of public key cryptography or asymmetric key cryptography with example? Differentiate between them? (16)

OR

3. Explain the role of RSA algorithm in public key Cryptography. Explain the RSA algorithm with example? Explain the Diffie Hellman key exchange algorithm with example. (16)

Unit - IV

4. Why we need Message authentication justify your answer. Explain the concept of MAC and its functions and what is Hash function? Explain it? (16)

OR

4. What is the Format of x.509 authentication certificate and the hierarchy of x.509 certificate? Explain various services provided by PGP. (16)

Unit - V

5. Why SSL is important? Explain the working of SSL using diagram what are the difference between SSL, SET and TSL. (16)

OR

5. Draw and explain the various field of authentication header. Also explain the position of authentication header in IPV4 and IPV6 packet format. (16)