

B.Tech. VIII Semester (Back) Examination, April/May-2017**Computer Sc. and Engg.****8CS2(O) Information System Security****CS & IT**

rtuonline.com

Time : 3 Hours**Maximum Marks : 80****Min. Passing Marks : 26****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 suitable be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.

Unit-I

1. a) What do you mean by abelian group? Prove that a set of integer under addition $(\mathbb{Z}, +)$ is an abelian group? (10)
- b) What is key equivocation and unicity distance explain in detail? (6)

OR

1. What are the problem with the pseudoprimalitiy test and how can overcome these problem by using the miller rabin randomized primality test algorithm? (16)

Unit-II

2. a) What is cryptography? Draw and explain the model of conventional cryptography and it's components. (8)
- b) Explain S-box theory in detail. (8)

OR

2. a) What is the concept of IDEA? Explain the concept of round IDEA. (8)
- b) Explain the Lucifer algorithm in detail and what are the limitation of Lucifer algorithm. (8)

Unit-III

3. Describe the Diffie-hellman key exchange algorithm in detail. Also decuess "Non in the middle attack" problem associated with the algorithm. (16)

3. a) Perform incryption and decryption using RSA algorithm. (8)
 $P = 3$ $Q = 11$ E (public key) = 7
 M (plain text) = 5
- b) Differentiate between symmetric and asymmetric key cryptography. (8)

Unit-IV

4. a) Explain the concept of MAC and it's function. (8)
 b) What is the property of digital signature? Explain. (8)

OR

4. a) Explain MD5 message digest algorithm with its logic and compression function. (10)
 rtuonline.com
- b) Explain the model of authentication system. (6)

Unit-V

5. What is certificate revocation? Why we need certificate revocation and what is the Concept of Certificate Revocation List (CRL)? (16)

OR

5. Writs short note : rtuonline.com (4×4)
- a) PGP trust model
 b) R64 conversion
 c) Need of MIME
 d) Three way authentication

