7E7032

Roll No. _____ [Total No. of Pages : 3

7E7032

B.Tech. VII Semester (Main) Examination, Dec. - 2015

Computer Science & Engineering

7CS2A Information System Security

CS, IT

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. a) What is cryptography? Explain Block and stream ciphers in detail. **(8)**

   b) What are the non-linear components used in DES encryption & description **(8)**

OR

1. a) Differentiate amongst cryptology, cryptography and cryptanalysis **(8)**

   b) What are the difference between active and passive attack? Determine the security services required to counter these attack. **(8)**

Unit - II

2. What is AES? What are the major parameters used in AES? Explain the processing of plain text with a suitable diagram. **(16)**

OR

2. a) What is the purpose of the S-Boxes is DES? What is the criteria to design S-Boxes? **(10)**

   b) Explain RC6 in detail. **(6)**

Unit - III

3. a) What is the strength of RSA? What are the different kinds of attacks possible against RSA? **(8)**

   b) What is X.509 certificate? Differentiate between X.509 client certificate and a normal SSL certificate. **(8)**

OR

3. Explain diffie Hellman key Exchange Algorithm in detail what are "Clogging attack" and "Man in the middle attack" on Diffie Hellman algorithm? **(16)**

Unit - IV

4. a) Differentiate between MAC and Hash value What are the characteristics of a good hash function? **(8)**

   b) Explain SHA in detail. **(8)**

OR

4. a) Explain Birthday attack on digital signature. Does it involve breaking of strong collision resistance or weak collision resistance? Justify your answer **(8)**

   b) What are the difference between source authentication and source Non-repudiation? Also explain the MD5 in detail **(8)**

Unit - V

5. a) What are the services provided by PGP? What is Radix -64 Transformation? Why it is required in PGP? **(10)**

   b) Define IP Security Architecture. **(6)**

OR

5. Write short note on(any 2)

   a) Lamport's Hash

   b) Transport and Tunnel mode

   c) Authentication Header **(8×2=16)**