COLLEGE OF ENGINEERING PUNE

(An Autonomous Institute of Govt. of Maharashtra)

END SEM- EXAM

(CT 403) Information Security

Program: **B.Tech. (Computer Engineering/Information Technology)**

Year: 2013-14 Semester VII

Duration: 3 hr. Max. Marks: 60

Instructions:

1. **All Questions are Compulsory.**
2. **Make appropriate assumptions wherever necessary.**
3. **Give examples and draw neat diagrams wherever necessary.**

Q1. **A.** Fill in the blanks and **Re-write** the complete sentence with correct answer: **(5)**

1. While creating a digital signature, we encrypt the _____ with the_____.
   a. message digest, sender's public key
   b. message digest, receiver's private key
   c. one-time session key, receiver's public key
   d. message digest, sender's private key
2. When the existing bits in a key in IDEA protocol are exhausted, _____.
   a. a new key is generated
   b. the existing bits are shifted
   c. the key is discarded
   d. the protocol asks for more key bits
3. We trust a digital signature because it proves that _____.
   a. the sender's public key is visible to all
   b. the sender's private key is safe and secure
   c. the sender has a digital certificate
   d. the sender has the private key

4. If the sender encrypts the message with the receiver's public key, it achieves the purpose of _____.
   a. Confidentiality
   b. Authentication
   c. Confidentiality but not authentication
   d. Confidentiality and authentication
5. To verify a digital certificate, we need the _____.
   a. CA's private key
   b. CA's public key
   c. certificate owner's private key
   d. certificate owner's public key

B. List the various attacks possible on DES? Explain the Linear Cryptanalysis and Differential Cryptanalysis attack with respect to DES in detail. **(5)**

Q.2. A. Describe IDS and list its types. Distinguish between IDS and Firewall **(4)**

B. In a public-key cryptosystem using RSA, you intercept the ciphertext C=284 sent to user whose public key is (e=223, n=713). What is the plaintext M? **(6)**

Q.3. A. Take "CHARLES" as a keyword for the Playfair Cipher and Encipher the following text using the same "meet me at the bridge tonight" **(6)**

B. Describe steganography and distinguish between steganography and digital watermarking. **(2)**

C. i. Solve $3^{50} \bmod 7$ by using Fermat's little Theorem. **(2)**

ii. Find all solutions to $6x \equiv 3 \bmod 15$

Q.4. A. Explain various services provided by IPSec. Distinguish between **(5)**

Transport and tunnel mode of IPSec.

B. What do you mean by Authentication? Describe various requirements and working of Kerberos. **(5)**

Q.5. A. Describe the following threats with example: **(4)**

a) Sniffing

b) Modification or Alteration

c) Repudiation of origin

d) Denial of Service

B. Consider *Plaintext= 123456ABCD132536 (in hex)* **(6)**

Key= AABB09182736CCDD (in hex), what is the Ciphertext after first round of DES. (use of data sheet is allowed)

Q.6. A. What are the steps involved in PGP (Pretty Good Privacy) for securing E-mails? Describe each step with an example. **(5)**

B. Describe the generalized structure of virus program and its various phases. List various types of malicious codes. **(5)**