U.S.N | | | | | | | | | | |

P.E.S. College of Engineering, Mandya - 571 401

(An Autonomous Institution affiliated to VTU, Belagavi)

Eighth Semester, B.E. - Computer Science and Engineering

Semester End Examination; June - 2017

Cryptography and Network Security

Time: 3 hrs *Max. Marks: 100*

***Note**: Answer **FIVE** full questions, selecting **ONE** full question from each unit.*

UNIT - I

1. a. Briefly explain the Non-Cryptanalytic attacks. 7

   b. Use auto key cipher with initial key value = 12 and encrypt the message "attackistoday". 8

   c. Define transposition cipher. Discuss keyless transposition ciphers with an example. 5

2 a. Briefly explain the ITU-T (X.800) security mechanisms. 8

   b. Find the multiplicative inverse of 23 in Z_{100}. Using extended Euclidean algorithm. 5

   c. Use multiplicative cipher with key = 7 to encrypt the message "hello". Also calculate the inverse key that will be used for decryption. 7

UNIT - II

3 a. Explain the DES function in detail. 10

   b. Discuss the key expansion process of AES in detail. 10

4 a. Discuss the transformations involved in AES. 10

   b. Show how round-keys are generated in DES? 10

UNIT - III

5 a. State the two versions of Fermat's little theorem. Find the results of 6^{10} mod 11 and 3^{12} mod 11 using Fermat's little theorem. 5

   b. Explain plaintext attacks and attacks on implementation in RSA. 10

   c. Find the solution to the simultaneous equations :
   $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 2 \bmod 7$ using Chinese remainder theorem. 5

6. a Discuss the process of key generation in RSA. Give a simple example which shows the working of RSA algorithm. 10

   b. Write the algorithm for decryption of message in Rabin cryptosystem. 5

   c. Explain how modification detection code is used for message integrity? 5

UNIT - IV

7 a. Explain Diffie-Hellman key agreement with an example. 10

   b. Write the application of PGP. Draw the figures of encrypted message, signed message and certificate message in PGP. 10

Contd…2

8 a. Discuss the content-type header of MIME in detail. 10

b. Define web of trust. Briefly explain the public key ring table format of PGP. 10

UNIT - V

9 a. Explain the Authentication Header protocol of IPSec. 10

b. Explain Phase-I of SSL handshake protocol. 10

10a. Draw and briefly explain the ISAKMP general header. 10

b. Explain the two modes in which IPSec operates. 10

* * * *