Total number of printed pages–4

53 (IT 811) CPNS

2018

CRYPTOGRAPHY AND NETWORK SECURITY

Paper : IT 811

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

*Answer **any five** questions.*

1. *(a)* What is Cryptography? What is Cryptanalysis?

   (b) Explain the significance of a network security model.

   (c) What are the CFB and OFB modes?

   5+7+8=20

2. *(a)* Explain the complete process of DES.

Contd.

(b) Using S-DES decrypt the string (10100010) using the key (0111111101) by hand. Show intermediate results after each function (IP, Fk, SW, FK, IP^{-1}). Then decode the first 4-bits of the plaintext string to a letter and the second 4-bits to another letter where we encode A through *P* in base 2. (i.e *A* = 0000, *B* = 0001, ..., *P* = 1111). Use the following data :

*P*10 = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6}

*P*8 = {6, 3, 7, 4, 8, 5, 10, 9}

E/P = {4, 1, 2, 3, 2, 3, 4, 1}

*P*4 = {2, 4, 3, 1}

*S*0 =

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

*S*1 =

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

IP = {2, 6, 3, 1, 4, 8, 5, 7}

IP^{-1} = {4, 1, 3, 5, 7, 2, 8, 5}

8+12=20

3. *(a)* Explain a single round of DES with block diagram.

(b) What is Firewall? How does it resolve the security issues? 10+10=20

4. *(a)* Compare between symmetric and asymmetric key cryptography.

(b) Explain RSA algorithm in brief.

(c) Given $p = 19$, $q = 29$, $N = p \times q$ and public key $e = 17$, compute the private key d corresponding to the RSA system. 5+7+8=20

5. Describe Diffie-Hellman Symmetric Key Exchange algorithm with an example. Explain how this process might become vulnerable. 20

6. *(a)* Outline the broad level steps in SET. 10

(b) Explain with figure, how SSL is accommodated in TCP/IP protocol suite. 10

7. Write short notes on ***any four*** of the following: 5×4=20

(a) Stream Cipher and Block Cipher

(b) CBC mode

(c) Kerbers

(d) Digital signature

(e) IPSec services

(f) Virtual Private Network.
