11. (a) Discuss about SSL Record Protocol in detail. 6

(b) Write about Web Security Requirements. 3

(c) Write a short note on SET Protocol. 4

OR

12. Write short notes on (Solve any **three**) :

(a) Firewall design principles

(b) Viruses and Worms

(c) Trusted System

(d) SNMP. 13

NTK/KW/15/7585

Faculty of Engineering & Technology
Seventh Semester B.E. (Infor. Tech.) (C.B.S.) Examination
COMPUTER SYSTEM SECURITY

Time—Three Hours] [Maximum Marks—80

INSTRUCTIONS TO CANDIDATES

(1) All questions carry marks as indicated.

(2) Solve Question No. **1 OR** Question No. **2**.

(3) Solve Question No. **3 OR** Question No. **4**.

(4) Solve Question No. **5 OR** Question No. **6**.

(5) Solve Question No. **7 OR** Question No. **8**.

(6) Solve Question No. **9 OR** Question No. **10**.

(7) Solve Question No. **11 OR** Question No. **12**.

(8) Due credit will be given to neatness and adequate dimensions.

(9) Assume suitable data wherever necessary.

(10) Illustrate your answers wherever necessary with the help of neat sketches.

1. (a) Explain Active and Passive Attacks in detail. 7

(b) Explain S-DES Encryption and Decryption with an example. 6

OR

2. (a) Explain Play-fair substitution technique, convert the following text to cipher text using "MONARCHY" as a keyword. "It was disclosed yesterday". 5

(b) Explain substitute bytes, MFX Column and Add round key stages in AES Encryption process with neat diagram. 8

3. (a) Explain IDEA Cipher in detail with neat diagram. 8

(b) Write characteristics of advanced symmetric block ciphers. 6

OR

4. (a) Explain subkey, S-Box generation and round structure of Blow fish-with neat diagram. 6

(b) Write about ANSI X9.17 Pseudo random number generator. 4

(c) Explain differential and linear cryptanalysis. 4

5. (a) Explain RSA algorithm. Perform Encryption and Decryption using RSA algorithm for the following :

$p = 3 ; q = 11 ; d = 7 ; N = 5.$ 8

(b) Explain different schemes for distribution of public keys. 5

OR

6. (a) Explain cryptography with Elliptic curves. 6

(b) Draw and explain MD-5 Hash algorithm in detail. 7

7. (a) Describe SHA-1 with neat sketches. 8

(b) Explain Digital Signature Standard. 5

OR

8. (a) Explain the difference between kerberos version 4 and version 5. 4

(b) What is the purpose of X.509 authentication service ? Describe the format of X.509 certificate and certificate revocation. 9

9. (a) Explain PGP in detail. 8

(b) Discuss about ESP header of IPSec in both the modes. 6

OR

10. (a) Explain S/MIME functions in detail. 6

(b) Explain ISAKMP in detail. 8