Course Code : CST 407 **ITSJ/RW – 17 / 1399**

Eighth Semester B. E. (Computer Science and Engineering) Examination

INFORMATION SECURITY

Time : 3 Hours] [Max. Marks : 60

Instructions to Candidates :—

(1) Q. No. **One** and Q. No. **Three** are compulsory. Read the internal choices specified for subsequent questions.
(2) All questions carry marks as indicated against them.
(3) Due credit will be given to neatness and adequate dimensions.
(4) Assume suitable data and illustrate answers with neat sketches wherever necessary.

1. (a) How would you classify the type of attacks with reference to X.800 security architecture ? 6 (CO 1)

(b) Recall and provide a definition for the following terms :

(i) Security threat

(ii) Security attack

(iii) Security mechanism

(iv) Security service. 4 (CO 1)

2. (a) How would you individually summarize and analyze the parameters required to design a Feistel Cipher ? 4 (CO 1)

Solve any **One** question from 2(b) and 2(c) :

(b) Can you demonstrate the use of Vigenere cipher with keyword "HEALTH" to encipher the message "Life is full of surprises" ? 3 (CO 1)

OR

(c) Investigate the information that you would use to support the view that the Round-key generator of S-DES creates two 8-bit keys out of a 10-bit cipher key. 3 (CO 1)

(d) Can you apply the encryption method suggested under the Playfair cipher technique to solve the information given below ?

"The house is being sold tonight" (Ignore the spaces between words) Use the following key square :

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

3 (CO 1)

3. (a) Discuss in detail the RSA algorithm, highlighting its computational aspect and security. 4 (CO 1, 2, 4)

(b) Explain briefly about Diffie-Hellman key exchange algorithm with its pros and cons. Compute the secret key for the given information : $p = 11$, $g = 2$, $X_A = 9$, $X_B = 4$. 6 (CO 1, 2, 4)

Solve any **One** question from Q 4(a) and Q 4(b) :

4. (a) What do you mean by a hash function ? Can you state the properties that a hash function H must possess, to be useful for message authentication? 4 (CO 3, 4)

OR

(b) Identify the use of a has function in the Birthday Attack. 4 (CO 3, 4)

(c) Describe Digital Signature Standard (DSS) Algorithm and show how signing and verification is done using DSS. 6 (CO 3, 4)

Solve any **Two** questions from Q 5(a), (b) and (c) :

5. (a) Describe the authentication dialogue used by Kerberos for obtaining services from another Realm. 5 (CO 4)

(b) Explain with help of an example how a user's certificate is obtained from another Certification Authority in X.509 scheme. 5 (CO 4)

(c) Classify and elaborate the IPSec documents overview. 5 (CO 4)

Solve any **One** question from Q 6(a) and Q 6(b) :

6. (a) Discuss the handshake protocol actions of Secure Socket Layer. 5 (CO 5)

OR

(b) Imagine the scenario given as follows : "A system administrator trusts the internal users of its system", examine and justify whether what type of Fire wall is to be used for the given situation ? 5 (CO 5)

(c) Can you write a brief outline about audit records ? 5 (CO 5)