(d) What will be minimum positive integer p such that 3^p modulo 17 = 1 ?

(e) Define Cipher text.

(f) What is PKI ?

(g) What is Malicious Code ?

(h) Define Product Cipher.

(i) Mention the stengths of DES algorithm.

(j) Differentiate MAC and Hash function.

8 mod 26 ?

Roll No. ..... Total Pages : 04

Jan-21-R-124

B. Tech. EXAMINATION, Jan. 2021

Semester VII (CBCS)

INFORMATION SECURITY

CS-703

Time : 3 Hours *Maximum Marks : 60*

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note : Attempt *Five* questions in all, selecting *one* question from each Sections A, B, C and D. Q. No. 9 is compulsory.

Section A

1. (a) What is Encryption ? Write the benefits of encryption. **5**

(b) Discuss the various types of threats to information. **5**

2. (a) Explain Kirchhoff principle. 5

(b) What is the need for information security ? 5

Section B

3. Why is it important to study the Feistel cipher ? Explain, how block cipher different from stream cipher ? **10**

4. (a) Compare Substitution and Transposition techniques. **5**

(b) Briefly explain the design principles of block cipher. **5**

Section C

5. Give short note on RSA algorithm. Also, encrypt the message "This is encrypted text" using the values $p = 7$ and $q = 17$. **10**

6. (a) Explain the public key cryptography with the help of suitable examples. **5**

(b) Briefly explain Deffie-Hellman key exchange with an example. **5**

Section D

7. (a) It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible ? 5

(b) Explain AES. What is the main advantages of AES over DES ? 5

8. (a) Explain the Key Generation, Encryption and Decryption of DES algorithm in detail. 5

(b) What is meant by Computer Crime ? Explain various solutions to prevent computer crime. 5

(Compulsory Question)

9. Attempt all questions : **2×10=20**

(a) What do you understand by integrity of message ?

(b) Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires.....

(c) In asymmetric key cryptography, who kept the private key ?