53 (IT 811) CRNS

2021

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)* Explain the RSA algorithm in details. Write *any one* technique of attaching RSA. 5+5=10

   (b) Differentiate between active and passive security attacks. Categorize these attacks and give *one* example of each. 10

2. Explain Diffie-Hellman key exchange algorithm in details with the help of an example. 20

3. Discuss the security services provided by *X*.800 architecture. 20

Contd.

4. Consider a Hill cipher with key K as

$$K=\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

(i) What is the cipher text corresponding to the plaintext : HELL ? 10

(ii) Show the decryption process to get back the plaintext for the above question. 10

5. Encrypt the following using Play-fair cipher using the keyword "MONARCHY". The plain text is "SWARAJ IS MY BIRTH RIGHT". 20

6. *(a)* Differentiate between public key and private key. 10

(b) What do you mean by "Man-In-The-Middle" Attack ? 10

7. Write short notes on : ***(any four)*** 5×4=20

(a) Digital Signature

(b) IPSec

(c) Hash function

(d) Caesar Cipher

(e) Substitution and transposition Cipher.