6TH SEM./CS & E /I T / 2023(S)

TH- 1 Cryptography and Network security

Full Marks: 80 Time- 3 Hrs

Answer any five Questions including Q No.1& 2
Figures in the right hand margin indicates marks

1. Answer **All** questions 2 x 10
   a. Define Brute-force attack.
   b. What is masquerade?
   c. Compare Substitution and Transposition techniques.
   d. Convert the Given Text "ALL THE BEST" into cipher text using Rail fence Technique.
   e. What is Tiny Fragment attack?
   f. Define static and dynamic webpage.
   g. Define digital envelop.
   h. Define CRL.
   i. Write the name of participants in the SET system.
   j. Write the problem associated with clear text password.

2. Answer **Any Six** Questions 6 x 5
   a. Differentiate between symmetric key and asymmetric key cryptography.
   b. Explain briefly about SSL protocol.
   c. Discuss different types of attacks.
   d. Define authentication token and illustrate how Challenge/Response Tokens works.
   e. Write the mechanism to protect private keys.
   f. Define digital certificate and the different process to revoke a digital certificate
   g Explain the followings:
   (a) Caesar cipher (b) Polygram substitution cipher**.**

3 Write the RSA algorithm and explain it with example 10

4 Encrypt "SWARAJ IS MY BIRTH RIGHT" by play fair cipher using the keyword MONARCHY. 10

5 Briefly Discuss about key principle of network security 10

6 Explain in detail about architecture of IP Security 10

7 Write short notes on any two 10
   a) PKIX Services.
   b) VPN
   c) Biometric Authentication.
   d) Encryption and Decryption