

PARUL UNIVERSITY
FACULTY OF ENGINEERING & TECHNOLOGY
Diploma Engineering, Mid semester Examination

Semester: 5th Sem
Subject Code: 03606305
Subject Name: Information Security

Date: (09/08/2022)
Time: (1hr: 30min)
Total Marks: 40

Instructions:

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.
4. English version is considered to be Authentic.

Q.1 Answer any six out of Ten. (2 Marks Each) (12)

1. What is Information Security?
2. Define Encryption & Decryption.
3. List out Information Security Services.
4. What are threats?
5. Write Applications of Public Key cryptosystems.
6. List out Requirements for Public-Key Cryptography.
7. What is public key?
8. What is Private Key?
9. What is Cryptography?
10. Using Rail fence Cipher perform Encryption with plaintext: Information Security & depth: 3.

Q.2 A) write short note on Steganography. (03)**OR**

- A) Explain one time pad. (03)
 B) Difference between Active and Passive Attack. (03)

OR

- B) Difference between worm & virus. (03)
 C) Explain Hill cipher and perform encryption on a given plaintext. (04)
 Plain text: Cyber crime
 Key: 8 1
 1 5

OR

- C) Explain Hill cipher and perform decryption on a given plaintext. (04)
 Cipher text: OQFGAZ
 Key: 3 1
 5 2

- D) Explain and draw diagrams of Digital Certificate. (04)

Q.3 A) Explain Asymmetric key model. (03)**OR**

- A) Explain symmetric key model. (03)
 B) Explain Caesar's cipher and perform encryption and decryption on a given plaintext with key value 3. (03)
 Plain text: Computer & Networks security

OR

- B) Explain Caesar's cipher and perform encryption and decryption on a given plaintext with key value 5. (03)
 Plain text: Introduction to Information Security
 C) Explain playfair cipher and perform encryption and decryption on a given plaintext with key value digital. Plain text: Communication (04)

OR

- C) Explain playfair cipher and perform encryption and decryption on a given plaintext with key value india. Plain text: Good Moring (04)
 D) Difference between Centralized and Decentralized Key infrastructures. (04)

