Diwaliba Polytechnic,
Mahuva

Date: 13/08/2024

Subject: Computer and Network Security **Course:** Diploma IT

Semester: 5

Faculty Name: Jignasa Erthana

Syllabus of Mid-I examination

Unit – I

Introduction to security and threat:

Basic concepts of security: Security, Need of Security, Attack, Threat, The OSI Security Architecture, Security Services, Security Attacks, A modelfor Network Security.

Unit – II

Cryptography and Symmetric encryption:

Cryptography, Cryptanalysis and Brute-Force Attack, Symmetric cipher model, Substitution techniques: Caesar cipher, Monoalphabetic ciphers,Polyalphabetic ciphers, One-Time Pad, Hill cipher, Playfair cipher, Transposition techniques: Rail fence, Columnar.

Unit – III

Public Key Cryptosystems:

Principles of public key cryptosystems: Public-key cryptosystems, Applications for Public-key cryptosystems, Requirements for Public-Key Cryptography, Public-Key Cryptanalysis, RSA Algorithm, The Security of RSA, Key management.

Question Paper format

Diwaliba Polytechnic, Mahuva

Uka Tarsadia University, Bardoli

Diploma IT 5th – Semester

MID-I Examination

Subject: Computer and Network Security

Date:

Time: 75 mins
Max. Marks: 30

Instructions:

1. Attempt ALL QUESTIONS
2. Make suitable assumptions wherever necessary.
3. Draw diagrams/figures whenever necessary.
4. Figures to the right indicate full marks allocated to that question.
5. Follow usual meaning of notations/abbreviations.

Q1 **(A)**Answer the following. (Any 3) [6]

1

2

3

4

Q2 **(A)**Answer the following in detail. (Any 1) [2]

1

2

(B) Answer the following (Any 2) [10]

1

2

3

Q3 **(A)** Answer the following in detail. (Any 2) [12]

1

2

3

Question no.	Unit no.	Marks
Q. 1 (A),(B)	Unit 1	06
Q. 2 (A),(B)	Unit 2	12
Q. 3 (A),(B)	Unit 3	12