NITTE EDUCATION TRUST

NITTE MEENAKSHI
INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, Affiliated To Visvesvaraya Technological University Belagavi, Accredited by NAAC-“A+” Grade, approved by AICTE, New Delhi.Yelahanka,Bangalore-64)

Department of Computer Science and Engineering

Department: *Computer Science and Engineering*	***Course Type:*** *Programme Core*
Course Title: *Cryptography and Network Security Lab*	***Course Code:****18CSL68*
L-T-P:*0-0-2*	***Credits:*** *1*
Total Contact Hours: *36 Hours*	***Duration of SEE:*** *3 Hours*
SEE Marks*: 50*	***CIE Marks:*** *50*

COURSE DESCRIPTION

This laboratory course focuses on the introduction of network security using various cryptographic algorithms, to understand the basic mathematical foundations of cryptography, and to gain insightful experience by working with fundamental cryptographic applications

PREREQUISITES

- Students should have the knowledge of Computer Networks.
- Students should have knowledge of Mathematics and Algorithm Concepts.

COURSE OBJECTIVES

- Understand the most common type of cryptographic algorithm
- Understand various block cipher cryptosystems
- Understand various substitution and transposition cipher techniques
- Analyse public cryptosystems and key management Systems
- Understand and apply authentication techniques to provide secure communication

LAB EXERCISES

1. Implement Caesar Cipher encryption & Decryption technique which is by replacing each character by another character that will be some fixed number of positions down to it.
2. Demonstrate the playfair cipher, consider the key table 5×5 grid of alphabets that acts as the key for encrypting the plaintext.
3. Implement Data encryption and decryption using Hill Cipher method.
4. Encrypt the plaintext we using a Vigenere table that consists of the alphabet from A to Z written out 26 times in different rows, further each alphabet must be shifted cyclically to the left compared to the previous alphabet.
5. Implement Rail fence cipher technique using the row & Column Transformation.
6. Demonstrate the Data Encryption Standard based on the two fundamental attributes of cryptography: substitution (also called as confusion) and transposition (also called as diffusion).
7. Execute the program for simple RSA algorithm to encrypt and decrypt the data.

8. Implement diffie Hellman (DH) key exchange algorithm as a method for securely exchanging cryptographic keys over a public communications channel.

ASSESSMENT METHODS

Parameters	Marks
Experiment write up, Execution, Viva & Record writing	30
Lab Internal Test	20
Total	**50**
Final Exam will be conducted for 100 marks (SEE)	

COURSE OUTCOMES

At the end of the course students will be able to

COs	Description	Bloom’s level
CO 1	Understand the concepts of different ciphers	**L2**
CO 2	Implement Message authentication code in real-time	**L3**
CO 3	Apply DES and AES algorithms in real-time problem solving.	**L3**
CO 4	Experiment and use Diffie-Hellman Key Establishment in problem solving	**L3**
CO 5	Analyze the public key crypto system	**L3**

Mapping of Course outcomes (COs) to Program outcomes (POs*)& PSO **

	Course Outcomes mapping to Program Outcomes												**PSOs**		
POs **COs**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**PSO1**	**PSO2**	**PSO3**
CO1	**3**	**3**											**3**		
CO2	**3**	**3**	**2**										**3**		
CO3	**3**	**3**											**3**		
CO4	**3**		**2**										**3**		
CO5	**3**													**2**	

3: Strong, 2: Medium, 1: Weak ** H: Highly related S: Supportive