DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE
(AUTONOMOUS)
(Approved by AICTE & Affiliated to Anna University, Chennai)
Re-Accredited by NAAC with 'A' Grade
Accredited by NBA for AERO, BME, CSE, ECE, EEE, IT & MECH.
PERAMBALUR-621212, TAMILNADU, INDIA.
Website: www.dsengg.ac.in

LABORATORY COURSE PLAN (2025-2026 Odd Semester)

LAB COURSE TITLE	**NETWORK SECURITY LABORATORY**			
LAB COURSE CODE	**U20IT704**			
LAB COURSE STRUCTURE	**LECTURE**	**TUTORIAL**	**PRACTICAL**	**CREDIT**
	0	**0**	**4**	**2**
REGULATION	**BRANCH**	**YEAR**	**SEMESTER**	**ACADEMIC YEAR**
2020	**IT**	**IV**	**VII**	**2025-2026**
COURSE INCHARGE				

SYLLABUS

COURSE OBJECTIVE:

The student should be made to:

- To learn different cipher techniques
- To implement the algorithms DES, RSA,MD5,SHA-1
- To use network security tools and vulnerability assessment tools

LIST OF EXPERIMENTS

1. Perform encryption, decryption using the following substitution techniques
(i) Ceaser cipher, (ii) Play air cipher (iii) Hill Cipher (iv) Vigenere cipher
2. Perform encryption and decryption using following transposition techniques i) Rail fence ii) row & Column Transformation
3. Implement RSA Algorithm using HTML and JavaScript
4. Implement the Diffie-Hellman Key Exchange algorithm for a given problem.
5. Calculate the message digest of a text using the SHA-1 algorithm.
6. Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w.

7. Automated Attack and Penetration Tools Exploring N-Stalker, a Vulnerability Assessment Tool

8. Defeating Malware

i) Building Trojans ii) Root kit Hunter

TOTAL: 60 PERIODS

TEXT/REFERENCE BOOKS:

T1: William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

R1: C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wiley India Pvt.Ltd

R2: BehrouzA.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.

R3: Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: PRIVATE Communication in aPUBLIC World, Prentice Hall, ISBN 0-13-046019-2

VIRTUAL LAB LINK
https://www.vlab.co.in
https://engineering-computer-science.wright.edu/computer-science-and-engineering/virtual-cyber-security-lab
https://cse29-iiith.vlabs.ac.in

EXP. NO.	NAME OF THE EXPERIMENTS	NO. OF PERIODS	CUMULATIVE PERIODS
	CYCLE I		
1	Perform encryption, decryption using the following substitution techniques (i) Ceaser cipher, (ii) Play air cipher (iii) Hill Cipher(iv) Vigenere cipher	8	8
2	Perform encryption and decryption using following transposition techniques i) Rail fence ii) row & Column Transformation	8	16
3	Implement RSA Algorithm using HTML and JavaScript	8	24

4	Implement the Diffie-Hellman Key Exchange algorithm for a given problem.	8	32
	CYCLE II		
5	Calculate the message digest of a text using the SHA-1 algorithm.	8	40
6	Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w.	8	48
7	Automated Attack and Penetration Tools Exploring N-Stalker, a Vulnerability Assessment Tool	4	52
8	Defeating Malware i) Building Trojans ii) Root kit Hunter	8	60

COURSE OUTCOME

At the end of the course, the student should be able to:

CO1: Develop code for classical Encryption Techniques to solve the problems. (K3)
CO2: Build cryptosystems by applying symmetric and public key encryption algorithms. (K3)
CO3: Construct code for authentication algorithms. (K3)
CO4: Develop a signature scheme using Digital signature standard. (K3)
CO5: Demonstrate the network security system using open source tools (K3)
C06: Implement a java interface for RSA algorithm (K3)

CO-PO mapping:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PS02
CO1	3	3	3	3	3	-	-	-	-	-	-	-	2	-
CO2	2	2	2	2	2	-	-	-	-	-	-	-	2	-
CO3	2	2	2	2	2	-	-	-	-	-	-	-	2	-
CO4	3	2	2	2	3	-	-	-	-	-	-	-	2	-
CO5	3	2	2	2	2	-	-	-	-	-	-	-	2	-
CO6	**2**	**2**	**2**	**2**	**2**	-	-	-	-	-	-	-	2	-
AVG	**2.5**	**2.16**	**2.16**	**2.16**	**2.33**								**2.00**	-

ADDITIONAL EXPERIMENTS		
EXP. NO.	**NAME OF THE EXPERIMENTS**	**Identified Resource link**
1.	Breaking the shift Cipher	http://cse29iiith.vlabs.ac.in/exp1/Theory.html?domain=Computer%20Science&lab=Cryptography%20Lab
2	Message Authentication code	http://cse29iiith.vlabs.ac.in/exp4/Experiment.html?domain=Computer%20Science&lab=Cryptography%20Lab
3	Public key cryptosystems	http://cse29iiith.vlabs.ac.in/exp9/Manual.html?domain=Computer%20Science&lab=Cryptography%20Lab
Further References:		https://www.geeksforgeeks.org/playfair-cipher-with-examples/ https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

MODEL LAB DETAILS

BATCH	REGISTER NO.	MODE OF LAB CONDUCT	DATE	TIMING
I		OFFLINE	-	-

SAMPLE UNIVERSITY QUESTIONS:

1. Implement the RSA Algorithm using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (Bob).

2. Write a Java/C/C++ program to implement the DES algorithm logic.

3. Write a Java/C/C++ program to implement substitution technique using Caesar cipher algorithm with shift key = 19.
4. Implement and show how to protect your system from Malware using Root kit Hunter.

5. Write a Java/C/C++ program to implement rail fence algorithm with a depth of 4.
6. Write a program FOR Row and Column Transformation Technique

7. Implement an application that will be using AES algorithm with key size 128 bits.
8. Implement an application that will be using HTML as front end and JavaScript to do RSA encryption/decryption.

9. Implement Rail-fence technique to do encryption of plaintext

10. Create a Trojan or download Sub Seven like Trojan and demonstrate it in a virtual machine.

11. Demonstrate Sub Seven Trojan or equivalent Trojan execution in a safe environment.

12. Implement an application that will be using AES algorithm with key size 192 bits.

VIVA QUESTIONS

1. Define Digital Signatures.
2. What is message authentication?
3. List out the services provided by digital certificates?
4. What are Digital certificates?
5. Define DES.
6. State RSA algorithm.
7. How do you use RSA for both authentication and secrecy?
8. What is SHA-1?
9. Difference between DSA and RSA?
10. What is Data encryption?
11. State RIP.
12. What are the factors that affect the performance of the network?
13. Name the types of errors?
14. What are Brute Force Attacks?
15. What is Authentication Header and how it provides the protection to IP header?
16. What is the Public Key Encryption?
17. What is a Firewall?
18. Which protocols uses application layer?
19. Difference between routing protocol and routed protocol**.**
20. What is the difference between DSA and RSA?

Google class Name:
Google class code:

Prepared By **Verified By**

AP/IT **HOD/IT**

Approved By
Principal