Practical Plan

Branch: Computer Engineering
Semester: VI **Year: 2022-23**

Course Title: Cryptography and System Security lab (CSL602)	SEE: 2 Hours – Practical
Total Contact Hours: 20 Hours	
Practical Plan Author: Prof. Monica Khanore	Date:
Checked By:	Date:

Prerequisites: Computer Networks

Course Outcomes (CO):

On successful completion of course learner will be able to:

CSL602.1	Apply knowledge of cryptographic techniques to implement simple cipher.
CSL602.2	Explore different network reconnaissance, and packet sniffing tools to gather information about networks, and packets, respectively.
CSL602.3	Explore various attacks on the system security.
CSL602.4	Set up firewalls and explore email security.

List of Experiments

Sr. No.	*Title*	*Attained COs*
1	Design and Implementation of a product cipher using Substitution and Transposition ciphers	CSL602.1
2	Implementation of Diffie- Hellman Key exchange algorithm	CSL602.1
3	Implementation and analysis of RSA cryptosystem.	CSL602.1
4	Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc	CSL602.2
5	For varying message sizes, test integrity of message using MD-5, SHA-1, and analyse the performance of the two protocols	CSL602.1
6	Study of packet sniffer tools: Wireshark to explore how the packets can be traced based on different filters like ICMP, TCP, and HTTP	CSL602.2
7	Implementation of Salt and Pepper password protection technique	CSL602.1
8	Explore GPG tool of Linux to implement email security.	CSL602.4
9	Simulation of SQL injection attack	CSL602.3
10	Case study/Presentation/Project	CSL602.1 CSL602.2 CSL602.3

Newly Added Experiments

1	Explore GPG tool of Linux to implement email security.

CO-PO Mapping: (BL – Blooms Taxonomy, C – Competency, PI – Performance Indicator)

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
CSL602.1		1			1	3		2	3	2		2
CSL602.2					1	3		2	3	2		2
CSL602.3					1	3		2	3	2		2
CSL602.4					1	3						

CO-PSO Mapping:

CO	**BL**	**C**	**PI**	**PO**	**Mapping**
CSL602.2.	2, 3	2.2	2.2.1	PSO2	3
CSL602.3.	3	2.2	2.2.1	PSO2	3
CSL602.4.	3	2.3	2.3.3	PSO2	3

	PSO1	PSO2
CSL602.1.	--	--
CSL602.2.	--	3
CSL602.3.	--	3
CSL602.4.	--	3

CO Measurement Weightages for Tools:

Course Outcomes	***Direct Methods (80%)***				***Indirect Method (20%)***
	Lab Performance	Assignments/Post Lab Questions	Quizzes	End Sem Exam (TW)	Course exit survey
CSL602.1	30%	10%	10%	50%	100%
CSL602.2	30%	10%	10%	50%	100%
CSL602.3	30%	10%	10%	50%	100%
CSL602.4	30%	10%	10%	50%	100%

Attainment:

CO CSL602.1:

Direct Method

$$A_{\mathrm{CSL602.1}D} = 0.3 \ast Lab\ Performance + 0.1 \ast Assignment/Post\ Lab + 0.1 \ast Quizzes + 0.6 \ast SEE\_TW$$

Final Attainment:

$$A_{\mathrm{CSL602.1}} = 0.8 \ast A_{\mathrm{CSL602.1}D} + 0.2 \ast A_{\mathrm{CSL602.1}I}$$

CO CSL602.2:

Direct Method

$$A_{\mathrm{CSL602.2}D} = 0.3 \ast Lab\ Performance + 0.1 \ast Assignment/Post\ Lab + 0.1 \ast Quizzes + 0.6 \ast SEE\_TW$$

Final Attainment:

$$A_{\mathrm{CSL602.2}} = 0.8 \ast A_{\mathrm{CSL602.2}D} + 0.2 \ast A_{\mathrm{CSL602.2}I}$$

CO CSL602.3:

Direct Method

$$A_{\mathrm{CSL602.3}D} = 0.3 \ast Lab\ Performance + 0.1 \ast Assignment/Post\ Lab + 0.1 \ast Quizzes + 0.6 \ast SEE\_TW$$

Final Attainment:

$$A_{\mathrm{CSL602.3}} = 0.8 \ast A_{\mathrm{CSL602.3}D} + 0.2 \ast A_{\mathrm{CSL602.3}I}$$

CO CSL602.4:

Direct Method

$$A_{\mathrm{CSL602.4}D} = 0.3 * Lab\ Performance + 0.1 * Assignment/Post\ Lab + 0.1 * Quizzes + 0.6 * SEE\_TW$$

Final Attainment:

$$A_{\mathrm{CSL602.4}} = 0.8 * A_{\mathrm{CSL602.4}D} + 0.2 * A_{\mathrm{CSL602.4}I}$$

Resourses:

1. https://www.youtube.com/watch?v=FvstbO787Qo
2. https://www.tutorialspoint.com/nmap-cheat-sheet

Practical Session Plan

Batch	***Dates***		***Remarks***
	Planned	***Actual***	
Experiment No. 1 Design and Implementation of a product cipher using Substitution and Transposition ciphers			
A	25/01/2023		
B	24/01/2023		
C	23/01/2023		
D	27/01/2023		
Experiment No. 2 Implementation of Diffie- Hellman Key exchange algorithm			
A	01/02/2023		
B	31/01/2023		
C	30/01/2023		
D	03/02/2023		
Experiment No. 3 Implementation and analysis of RSA cryptosystem.			
A	08/02/2023		
B	07/02/2023		
C	06/02/2023		
D	10/02/2023		
Experiment No. 4 Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc			
A	15/02/2023		
B	14/02/2023		
C	13/02/2023		
D	17/02/2023		
Experiment No.5 For varying message sizes, test integrity of message using MD-5, SHA-1, and analyze the performance of the two protocols			
A	22/02/2023		
B	21/02/2023		
C	20/02/2023		Students were absent
D	24/02/2023		
Experiment No. 6 Study of packet sniffer tools: Wireshark to explore how the packets can be traced based on different filters like ICMP, TCP, and HTTP.			
A	08/03/2023		
B	14/03/2023		
C	13/03/2023		
D	03/03/2023		
Experiment No. 7 Implementation of Salt and Pepper password protection technique.			
A	15/03/2023		
B	21/03/2023		

C	20/03/2023		
D	10/03/2023		
Experiment No. 8 Explore GPG tool of Linux to implement email security.			
A	29/03/2023		
B	28/03/2023		
C	27/03/2023		
D	17/03/2023		
Experiment No. 9 Simulation of SQL injection attack.			
A	05/04/2023		
B	28/03/2023		
C	03/04/2023		
D	24/03/2023		
Experiment No. 10 Case study/Presentation/Project			
	12/04/2023		
	11/04/2023		
	10/04/2023		
	21/04/2023		

Verified by:

Programme Coordinator Subject Expert