MOHAMMED SATHAK A J COLLEGE OF ENGINEERING

Siruseri IT park, OMR, Chennai - 603103

LESSON PLAN

Department of COMPUTER SCIENCE AND ENGINEERING

Name of the	CRYPTOGRAPHY AND NETWORK TECHNOLOGY	Name of the handling Faculty	Mrs.Mandakini Sigh
Subject Code	CS8792	Year / Sem	IV/VII
Acad Year	2021-2022	Batch	2018-2022

Course Objective

- To understand Cryptogarphy theories , algorithms and system .
- To understand necessary approaches and techniques to build protection mechanism in order to secure computer networks .
- To be able to secure a message over insecure channel by various means
- To learn about how to maintain the Confidentiality, Integrity and Availability of a data

Course Outcome

CO1. Understand the fundamentals of networks security, security architecture, threats and vulnerabilities .
CO2. Apply the different cryptographic operations of symmetric cryptographic algorithms
CO3. Apply the different cryptographic operations of public key cryptography
CO4. Apply the various Authentication schemes to simulate different applications
CO5. Understand various Security practices and System security standards

Sl. No.		T / R* Book	Periods Required	Mode of Teaching (BB / PPT / NPTEL / MOOC / etc)	Blooms Level (L1-L6)	CO	PO
UNIT-I	INTRODUCTION						
1	Security trends	T	1	BB	L1	CO1	PO1
2	Need for Security at Multiple levels, Security Policies	T	2	BB	L1	CO1	PO1-PO3
3	Model of network security	T	1	BB	L1	CO1	PO1-PO3
4	OSI security architecture	T	1	BB	L1	CO1	PO2
5	Classical encryption techniques	T	1	BB	L2	CO1	PO2
6	Foundations of modern cryptography	T	1	BB	L2	CO1	PO2
7	cryptanalysis.	T	1	BB	L2	CO1	PO3
8	cryptosystem	T	1	BB	L3	CO1	PO3
	Suggested Activity: Assignment / Case Studies / Tuorials/ Quiz / Mini Projects / Model Developed/others Planned if any						
1	**Define cryptography**						
2	**Define OSI security architecture**						
3	**Explain classical encryption technique**						
4	**Explain model of network security ?**						
5	**Difference between cryptosystem and cryptoanalysis**						
UNIT II	SYMMETRIC KEY CRYPTOGRAPHY						
10	Algebraic structures	T	1	BB	L1	CO2	PO1-PO3
11	Euclid"s algorithm	T	1	BB	L1	CO2	PO2
12	Congruence and matrices	T	1	BB	L2	CO2	PO2
13	SDES	T	1	BB	L2	CO2	PO2
14	DES	T	1	BB	L1	CO2	PO3
15	Block cipher design principles	T	1	BB	L1	CO2	PO3
16	AES	T	1	BB	L3	CO2	PO1
	Suggested Activity: Assignment / Case Studies / Tuorials/ Quiz / Mini Projects / Model Developed/others Planned if any						
1	**Explain DES in detail ?**						
2	https://docs.google.com/forms/d/e/1FAIpQLSeYOoN1RCs8WcTEZjV7bYRhlHuw8lpxt6Sl3WkXDBkNogM7vA/viewform						
3	**Explain AES ?**						
Evaluation method							
UNIT III	PUBLIC KEY CRYPTOGRAPHY						
19	MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY	T	1	BB	L1	CO3	PO1
20	Primes – Primality Testing –Factorization	T	1	BB	L1	CO3	PO1
21	Euler's totient function	T	1	BB	L2	CO3	PO2
22	Fermat's and Euler's Theorem	T	1	BB	L2	CO3	PO2
23	Chinese Remainder Theorem	T	1	BB	L2	CO3	PO2
24	Exponentiation and logarithm	T	1	BB	L2	CO3	PO2
25	RSA cryptosystem	T	1	BB	L2	CO3	PO3
26	Diffie Hellman key exchange	T	1	BB	L4	CO3	PO4
27	ElGamal cryptosystem	T	1	BB	L3	CO3	PO1-PO3
28	Elliptic curve cryptography	T	1	BB	L2	CO3	PO1-PO2
	Suggested Activity: Assignment / Case Studies / Tuorials/ Quiz / Mini Projects / Model Developed/others Planned if any						
1	**Briefly explain Deffie Hellman key exchange with an example.**						
2	**Explain fermats and eulers theorem ?**						
3	**Difference between Symmetric and Asymmetric key Cryptography**						
UNIT IV	MESSAGE AUTHENTICATION AND INTEGRITY						
28	Authentication requirement	T	1	BB	L1	CO4	PO1-PO3
29	Hash function	T	1	BB	L2	CO4	PO1

30	MAC	T	1	BB	L2	CO4	PO1
31	Biometrics, Passwords, Challenge Response protocols-	T	1	BB	L2	CO4	PO2
32	Authentication applications-Kerberos	T	1	BB	L3	CO4	PO2
33	X.509	T	1	BB	L3	CO4	PO2

1	**Explain the format of the X.509 certificate?**
2	**Explain the technical details of firewall and describe any three types of firewall with neat diagram?**
3	**Explain the firewall design principles?**
4	https://docs.google.com/forms/d/e/1FAIpQLScYZDPDP0rKVWQjt6uY7LmEdkYtSQH2RZJcB2ZTlbnkL8uLfQ/viewform
Evaluation method	
UNIT V	SECURITY PRACTICE AND SYSTEM SECURITY

37	Electronic Mail security	T	1	BB	L1	CO5	PO1-PO3
38	PGP, S/MIME	T	1	BB	L1	CO5	PO1
39	IP security – Web Security	T	1	BB	L2	CO5	PO1
40	SYSTEM SECURITY	T	2	BB	L2	CO5	PO2

1	Explain firewalls and how they prevent intrusions
2	Define intrusion detection and the different types of detection mechanisms, in detail.
Evaluation method	
Content Beyond the Syllabus Planned	
1	
2	

	Text Books
1	William Stallings, Cryptography and Network Security: Principles and Practice, PHI3rd Edition, 2006

	REFERENCE BOOKS
1	BehrouzA.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007
2	C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wiley India Pvt.Ltd
3	Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: PRIVATE Communication in a PUBLIC World, Prentice Hall, ISBN 0-13-046019-2
	Website / URL References
1	https://www.tutorialspoint.com/cryptography/index.htm
2	https://cs.nju.edu.cn/daihp/ns_course/03HaipengDai_SymmetricCrypto_1.pdf
3	https://www.tutorialspoint.com/cryptography/message_authentication.htm

Blooms Level						
Level 1 (L1) : Remembering Level 2 (L2) : Understanding Level 3 (L3) : Applying	Lower Order Thinking	Fixed Hour Exams	Level 4 (L4) : Analysing Level 5 (L5) : Evaluating Level 6 (L6) : Creating		Higher Order Thinking	Projects / Mini Projects

Mapping syllabus with Bloom's Taxonomy LOT and HOT

Unit No	Unit Name	L1	L2	L3	L4	L5	L6	LOT	HOT	Total
Unit 1	INTRODUCTION	4	3	2	0	0	0	9	0	9
Unit 2	SYMMETRIC KEY CRYPTOGRAPHY	4	2	3	0	0	0	9	0	9
Unit 3	PUBLIC KEY CRYPTOGRAPHY	2	5	1	1	0	0	8	1	9
Unit 4	MESSAGE AUTHENTICATION AND INTEGRITY	1	4	4	0	0	0	9	0	9
Unit 5	SECURITY PRACTICE AND SYSTEM SECURITY	0	0	8	1	0	0	8	1	9
Total		11	14	18	2	0	0	43	2	45
Total Percentage		24.444	31.11	40	4.444444444	0	0	95.55556	4.44444	100

CO PO Mapping

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	1	0	0	0	0	0	0	0	0	0	3	2
CO2	3	2	1	0	0	0	0	0	0	0	0	0	3	2
CO3	3	2	1	1	0	0	0	0	0	0	0	0	3	2
CO4	3	2	1	0	0	0	0	0	0	0	0	0	3	2
CO5	3	2	1	I	0	0	0	0	0	0	0	1	3	2
Avg	3	2	1	0.25	0	0	0	0	0	0	0	0	3	2

Justification for CO-PO mapping	
CO1	The student is able to analyze and Implement the algorithms for specific problem.
CO2	Explain the various standards Symmetric Encryption algorithms used to provide confidentiality.
CO3	Explain the various standards Asymmetric Encryption algorithms to achieve authentication.
CO4	Apply authentication techniques to safeguard the data transfer .
CO5	Understand security attacks, services, mechanisms andencryption algorithmsto mitigate security issues in a network .

3	High level	2	Moderate level	1	Low level

Name & Sign of Subject Expert	:Mrs.Mandakini Sigh
Head of the Department	:CSE
Format No :231	