MOHAMMED S

Si

Department of_____	
Name of the Subject	CRYPTOGRAPI
Subject Code	
Acad Year	
• To understand Cryptogarphy theories , algorithms and system .	
• To understand necessary approaches and techniques to build protection mechanism in order to secur	
•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	
CO1. Understand the fundamentals of networks security, security architecture, threats and vulnerabili	
CO2. Design the different cryptographic operations of symmetric cryptographic algorithms	
CO3. Identify the different cryptographic operations of public key cryptography	
CO4. Describethe various Authentication schemes to simulate different applications	
CO5. Understand various Security practices and System security standards	
Sl. No.	
UNIT-I	INTRODUCTION
1	Security trends
2	Legal,Ethical and Professional Aspects of Security
3	Need for Security at Multiple levels, Security Policies
4	Model of network security
5	OSI security architecture
6	Classical encryption techniques
7	Foundations of modern cryptography
8	cryptanalysis.
9	cryptosystem
	Suggested Activity: Assignment / Case Stu
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
11	Euclid‟s algorithm
12	Congruence and matrices
13	Groups,Rings,Fields
14	SDES

15	DES
16	Block cipher design principles
17	AES
18	RC4- Key Distribution

1	**Explain DES in detail ?**
2	https://docs.google.com/forms/d/e/1FAIpQLSeYOoN1RCs8WcTEZjV7bYRhlHuw8lpxt6Sl3WkXDBk
3	**Explain AES ?**
Evaluation method - Test	
UNIT III	PUBLIC KEY CRYPTOGRAPHY
19	Primes – Primality Testing –Factorization
20	Euler‘s totient function
21	Fermat‘s and Euler‘s Theorem
22	Chinese Remainder Theorem
23	Exponentiation and logarithm
24	RSA cryptosystem
25	Diffie Hellman key exchange
26	ElGamal cryptosystem
27	Elliptic curve cryptography
	Suggested Activity: Assignment / Case Stu

UNIT IV	MESSAGE AUTHENTICATION AND INTEGRITY
28	Authentication requirement
29	Hash function
30	MAC
31	SHA
32	DSS
33	Entity Authentication
34	Authentication applications-Kerberos
35	Biometrics, Passwords, Challenge Response protocols-
36	X.509
1	**Explain the format of the X.509 certificate?**
2	**Explain the technical details of firewall and describe any three types of firewall with**
3	**Explain the firewall design principles?**
4	https://docs.google.com/forms/d/e/1FAIpQLScYZDPDP0rKVWQjt6uY7LmEdkYtSQH2RZJcB2ZTlbn
Evaluation method - Test	
UNIT V	SECURITY PRACTICE AND SYSTEM SECURITY
37	Electronic Mail security
38	PGP, S/MIME
39	IP security
40	Web Security
41	SYSTEM SECURITY

42	Intruders
43	Malicious Software
44	Viruses
45	Firewalls
	Suggested Activity: Assignment
1	**Briefly explain Deffie Hellman key exchange with an example.**
2	**Explain fermats and eulers theorem ?**
3	**Difference between Symmetric and Asymmetric key Cryptography**
1	Explain firewalls and how they prevent intrusions
2	Define intrusion detection and the different types of detection mechanisms, in detail.

Evaluation method - Test

Content Beyond the Syllabus Planned

1	Cryptography in the age of quantum computers
2	The crypto wars: should we have end-to-end encryotion?

1	William Stallings, Cryptography and Network Security: Principles and Practice, PHI3rd Ed

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,
3	Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: PRIVATE Comn

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

Level 1 (L1) : Remembering
Level 2 (L2) : Understanding
Level 3 (L3) : Applying

Mapping syllabus with Bl

Unit No	Unit Name
Unit 1	INTRODUCTION
Unit 2	SYMMETRIC KEY CRYPTOGRA
Unit 3	PUBLIC KEY CRYPTOGRAPHY
Unit 4	MESSAGE AUTHENTICATION
Unit 5	SECURITY PRACTICE AND SYS
Total	
Total Percentage	

	PO1	PO2	PO3	PO4
CO1	3	2	1	0
CO2	3	2	1	0
CO3	3	2	1	1

CO4	3	2	1	0
CO5	3	2	1	I
Avg	3	2	1	0.25

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 confidenti
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 sec

3	High level

Name & Sign of Subject Expert	:
Head of the Department	:

Format No :231

SATHAK A J COLLEGE OF ENGINEERING

ruseri IT park, OMR, Chennai - 603103

LESSON PLAN

INFORMATION TECHNOLOGY **Engineering**

HY AND NETWORK TECHNOLOGY	Name of the handling Faculty	
CS8792	Year / Sem	
2022-2023	Batch	

Course Objective

e computer networks .

Course Outcome

ties .

	T / R* Book	Periods Required	Mode of Teaching (BB / PPT / NPTEL / MOOC / etc)
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	2	BB
	T	1	BB
	T	1	BB
	T	1	BB

udies / Tuorials/ Quiz / Mini Projects / Model Developed/others Planned if any

	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB

	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB

‹NoqM7vA/viewform

	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB

udies / Tuorials/ Quiz / Mini Projects / Model Developed/others Planned if any

	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB

neat diagram?

kL8uLfQ/viewform

	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB

	T	1	BB
	T	1	BB
	T	1	BB
	T	1	BB

t / Case Studies / Tuorials/ Quiz / Mini Projects / Model Developed/others Planned if any

Text Books

dition, 2006

REFERENCE BOOKS

Wiley India Pvt.Ltd

nunication in a PUBLIC World, Prentice Hall, ISBN 0-13-046019-2

Website / URL References

Blooms Level

Lower Order Thinking	Fixed Hour Exams	Level 4 (L4) : Analysing
		Level 5 (L5) : Evaluating
		Level 6 (L6) : Creating

oom's Taxonomy LOT and HOT

	L1	L2	L3	L4	L5
	4	3	2	0	0
APHY	4	2	3	0	0
	2	5	1	1	0
AND INTEGRITY	1	4	4	0	0
STEM SECURITY	0	0	8	1	0
	11	14	18	2	0
	24	31	40	4	0

CO PO Mapping

PO5	PO6	PO7	PO8	PO9	PO10
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

Justification for CO-PO mapping

ality.

.

curity issues in a network .

2	Moderate level	

Mrs. AYSHA SUFREEN

III/VI

2017-2021

Blooms Level (L1-L6)	CO	PO
L1	CO1	PO1
L1	CO1	PO1
L1	CO1	PO1-PO3
L1	CO1	PO1-PO3
L1	CO1	PO2
L2	CO1	PO2
L2	CO1	PO2
L2	CO1	PO3
L3	CO1	PO3
L1	CO2	PO1-PO3
L1	CO2	PO2
L2	CO2	PO2
L2	CO2	PO2
L2	CO2	PO2

L1	CO2	PO3
L1	CO2	PO3
L3	CO2	PO1
L3	CO2	PO1

L1	CO3	PO1
L2	CO3	PO2
L2	CO3	PO2
L2	CO3	PO2
L2	CO3	PO2
L2	CO3	PO3
L4	CO3	PO4
L3	CO3	PO1-PO3
L2	CO3	PO1-PO2

L1	CO4	PO1-PO3
L2	CO4	PO2
L2	CO4	PO2
L2	CO4	PO1
L2	CO4	PO2
L2	CO4	PO2
L3	CO4	PO2
L2	CO4	PO1
L3	CO4	PO2

L1	CO5	PO1-PO3
L1	CO5	PO1
L2	CO5	PO1
L2	CO5	PO1
L2	CO5	PO1

L2	CO5	PO1
L2	CO5	PO1
L2	CO5	PO1
L2	CO5	PO2

		Higher Order Thinking	Projects / Mini Projects

L6	LOT	HOT	Total
0	9	0	9
0	9	0	9
0	8	1	9
0	9	0	9
0	8	1	9
0	43	2	45
0	95.556	4.44444	100

PO11	PO12	PSO1	PSO2
0	0	3	2
0	0	3	2
0	0	3	2

0	0	3	2
0	1	3	2
0	0	3	2

	Low level