

**ANDHRA LOYOLA INSTITUTE OF ENGINEERING AND
TECHNOLOGY**

**Department of Computer Science and Engineering
Micro Lesson Plan**

Subject: CRYPTOGRAPHY AND NETWORK SECURITY

Teacher : Dr RAJENDRA BABU CHIKKALA

Academic Year: 2020-21

Year/Semester: IV-SEM-I

Name of the Program: B.Tech

Section: CSE-1

Course Outcomes:

Factual	• To understand the principles and practice of cryptography and network security.
Conceptual	• To understand key concepts Classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers) • To be familiarity with information security awareness and a clear understanding of its importance.
Procedural	• Algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes • To master protocols for security services • To master fundamentals of secret and public cryptography
Applied	• To be familiar with network security designs using available secure solutions (such as PGP, SSL, IPSec, etc) • To be familiar with network security threats and countermeasures

Text book References:

Text book-1 : Cryptography and Network Security, Behrouz A Forouzan, Debdeep Mukhopadhyay, (3e) Mc Graw Hill.

Text book-2 : Cryptography and Network Security, William Stallings, (6e) Pearson

Text book-3 : Network Security and Cryptography, Bernard Meneges, Cengage Learning.

Contents/Activities:

1	Factual: Factual knowledge consists of the basic elements students must know to be acquainted with a discipline	• Security Attacks(Unit-I) • Security Services(Unit-I) • Security Mechanisms(Unit-I) • Symmetric Key Cryptography(Unit-II) • Asymmetric Key Cryptography(Unit-III) • Hash function(UNIT-IV) • Digital Signature(UNIT-IV) • Key Management(UNIT-IV) • S/MIME(UNIT-V) • PGP(UNIT-V) • SSL(UNIT-V) • TLS(UNIT-V) • IPSec(UNIT-VI) • System Security(UNIT-VI)
2	Conceptual: Conceptual knowledge consists of the interrelations among the basic elements within a larger structure	• Cryptographic attacks(Unit-I) • Modular arithmetic (Unit-I) • Congruence (Unit-I) • Kerckhoff's Principle • Product ciphers(Unit-II) • Traditional Ciphers(Unit-II) • Algebraic structures(Unit-II) • Exponentiation and logarithm(Unit-III) • ElgamalCryptosysyem(Unit-III) • Elliptic curve Cryptosystems(Unit-III) • Pigeon hole principle(UNIT-IV) • Message Authentication(UNIT-IV) • Digital signature(UNIT-IV) • Public key distribution(UNIT-IV) • Certification Authority(UNIT-IV) • SSL(UNIT-V) • Security protocols(UNIT-VI) • Firewalls(UNIT-VI)
3	Procedural: methods of inquiry, and criteria for using skills, algorithms, techniques, and methods.	•
4	Applied: awareness of one's own learning, control and regulation of cognitive processes, self-knowledge, contextual knowledge, and conditional learning	• Generation of cipher text(Unit-1) • Digital signature(UNIT-IV) • Message Authentication Code(UNIT-IV) • Firewall((UNIT-VI)

Day	Topic	Objectives	Before Class-Videos, e-Books, Case Studies	In-Class-Activitie s, Quiz	Post-Class-Assign ment, Discussion Forum
UNIT-I					
1	Basic Principles	To understand the security attacks, services and mechanisms	Refer Text book -1	Lecture on Basics Q & A Session	Discussion in Forum
2	Introduction		Refer Text book -1	Lecture on introduction Q & A Session	Discussion in Forum
3	Security goals		Refer Text book -1 • Refer the video https://www.youtube.com/watch?v=yJN3A4FasO0 • Refer the video https://www.youtube.com/watch?v=hqDVvijah4s	Lecture on Security goals Q & A Session	Discussion in Forum
4	Service Mechanism		Refer Text book -1 • Refer the video https://www.youtube.com/watch?v=oUUmAQLea-A https://www.youtube.com/watch?v=KOv4csT0W1s	Lecture on service mechanism Q & A Session	Discussion in Forum
5	Integer Arithmetic’s		Refer Text book -1 • Refer the video https://www.youtube.com/watch?v=uNzaMrcuTM0	Lecture on Integer Arithmetic’s Q & A Session	Discussion in Forum
6	GCD , Euclidean Algorithm		Refer Text book -1	Lecture on GCD Q & A Session	Discussion in Forum
7	Linear Diophantine Equation		Refer Text book -1	Lecture on LDE Q & A Session	Discussion in Forum
8	Modular Arithmetic’s		Refer Text book -1	Lecture on Modular Arithmetic’s Q & A Session	Discussion in Forum
9	Inverse of a Matrix		Refer Text book -1	Lecture on Inverse of a matrix Q & A Session	Discussion in Forum
10	Set of linear Equations and Examples		Refer Text book -1	Lecture on linear equation Q & A Session	Discussion in Forum
UNIT-II					

11	Algebraic Structure: Groups	To understand key concepts of symmetric key cryptography	Refer Text book -1	Lecture on Basics Q & A Session	Discussion in Forum
12	Group axioms, Cyclic notation, Cyclic group order of elements		Refer Text book -1	Lecture on Groups Q & A Session	Discussion in Forum
13	Rings ,fields		Refer Text book -1	Lecture on Rings,fields Q & A Session	Discussion in Forum
14	GF(P),polynomials, Operations on polynomials		Refer Text book -1	Lecture on GF Q & A Session	Discussion in Forum
15	Multiplicative Inverse in polynomial		Refer Text book -1	Lecture on Multiplicative polynomial Q & A Session	Discussion in Forum
16	Fiestel Cipher		Refer Text book -1	Lecture on Fiestel Q & A Session	Discussion in Forum
17	Data Encryption standard, S-DES Examples		Refer Text book -1 Refer the following videos https://www.youtube.com/watch?v=edQIJvaUhHg https://www.youtube.com/watch?v=SaZGjQBItBc https://www.youtube.com/watch?v=O4xNJsjtN6E	Lecture on DES Q & A Session	Discussion in Forum Short Quiz
18	Structure IP & FP		Refer Text book -1	Lecture on IP Q & A Session	Discussion in Forum
19	Round Functions, Implementation using examples		Refer Text book -1	Lecture on Round Functions Q & A Session	Discussion in Forum
20	CAST- 128, Blowfish		Refer Text book -1	Lecture on CAST Q & A Session	Discussion in Forum
21	IDEA		Refer Text book -1	Lecture on IDEA Q & A Session	Discussion in Forum
22	AES,AES-Round Key Generation		Refer Text book -1	Lecture on AES Q & A Session	Discussion in Forum
UNIT III					
23	Asymmetric Encryption	To learn asymmetric key cryptography	Refer Text book -1 Refer the following videos https://www.youtube.com/watch?v=mjWTU-hRmyg https://www.youtube.com/watch?v=4RnqrLeY4xY	Lecture on Asymmetric encryption Q & A Session	Discussion in Forum
24	Modern Mathematics of Cryptography		Refer Text book -1	Lecture on MMC Q & A Session	Discussion in Forum
25	Eulers Theorem		Refer Text book -1	Lecture on Eulers theorem Q & A Session	Discussion in Forum

26	Fermats Theorem		Refer Text book -1	Lecture on Fermats Theorem Q & A Session	Discussion in Forum
27	CRT		Refer Text book -1	Lecture on CRT Q & A Session	Discussion in Forum
28	Logarithm		Refer Text book -1	Lecture on Log Q & A Session	Discussion in Forum
29	Knapsack, OAEP		Refer Text book -1	Lecture on OAEP Q & A Session	Discussion in Forum
30	RSA		Refer Text book -1	Lecture on RSA Q & A Session	Discussion in Forum
31	Rabin, El gamal, Elliptic Curve		Refer Text book -1	Lecture on Rabin Q & A Session	Discussion in Forum

UNIT IV

32	Message Integrity	To understand the concept and various kinds of hash functions. To learn about digital signature and key management	Refer Text book -1	Lecture on MI Q & A Session	Discussion in Forum
33	Hashing		Refer Text book -1	Lecture on Hashing Q & A Session	Discussion in Forum
34	Random oracle model		Refer Text book -1 Refer the following videos https://www.youtube.com/watch?v=xKtmNb6dU4k https://www.youtube.com/watch?v=vJTFa3havZA https://www.youtube.com/watch?v=TmA2QWSLSPg https://www.youtube.com/watch?v=8lpWVONYFBg	Lecture on random oracle model Q & A Session	Discussion in Forum
35	Birth day problem,MDC		Refer Text book -1	Lecture on BDP Q & A Session	Discussion in Forum
36	MAC		Refer Text book -1	Lecture on MAC Q & A Session	Discussion in Forum
37	Nested MAC,HMAC,CMAC		Refer Text book -1	Lecture on Nested MAC,HMAC Q & A Session	Discussion in Forum
38	RSA ,Elgamal		Refer Text book -1	Lecture on RSA Q & A Session	Discussion in Forum
39	Schnorr, DSS, Elliptic Curve DS		Refer Text book -1	Lecture on DSS Q & A Session	Discussion in Forum
40	Kerberos		Refer Text book -1	Lecture on Kerberos Q & A Session	Discussion in Forum
41	Diffie Hellman		Refer Text book -1	Lecture on Diffie Hellman Q & A Session	Discussion in Forum
42	Public Key Distribution CA		Refer Text book -1	Lecture on PKD Q & A Session	Discussion in Forum
43	X.509		Refer Text book -1	Lecture on X.509 Q & A Session	Discussion in Forum

UNIT V					
44	Network Security-I	To understand the security at the application layer	Refer Text book -1 Refer the following videos https://www.youtube.com/watch?v=sLnbvjtfyk0 https://www.youtube.com/watch?v=Aaom6MHW93Y https://www.youtube.com/watch?v=dsuVPxuU_hc	Lecture on IP Q & A Session	Discussion in Forum
45	PGP		Refer Text book -1	Lecture on PGP Q & A Session	Discussion in Forum
46	PGP		Refer Text book -1	Lecture on PGP Q & A Session	Discussion in Forum
47	S/MIME		Refer Text book -1	Lecture on S/MIME Q & A Session	Discussion in Forum
48	S/MIME		Refer Text book -1	Lecture on S/MIME Q & A Session	Discussion in Forum
49	Security at the Transport Layer		Refer Text book -1	Lecture on STL Q & A Session	Discussion in Forum
50	SSL		Refer Text book -1	Lecture on SSL Q & A Session	Discussion in Forum
51	SSL		Refer Text book -1	Lecture on SSL Q & A Session	Discussion in Forum
52	TLS		Refer Text book -1	Lecture on TLS Q & A Session	Discussion in Forum
53	TLS		Refer Text book -1	Lecture on TLS Q & A Session	Discussion in Forum
UNIT VI					
54	Network Security-II	To understand the security at the network layer	Refer Text book -1	Lecture on NS-II Q & A Session	Discussion in Forum
55	IPSec		Refer Text book -1	Lecture on IPSec Q & A Session	Discussion in Forum
56	Security Modes		Refer Text book -1 Refer the following videos https://www.youtube.com/watch?v=tuDVWQOG0C0 https://www.youtube.com/watch?v=GTxPzKfriOU	Lecture on Security models Q & A Session	Discussion in Forum
57	IKE		Refer Text book -1	Lecture on IKE Q & A Session	Discussion in Forum
58	Payloads		Refer Text book -1	Lecture on Payloads Q & A Session	Discussion in Forum

59	System Security		Refer Text book -1	Lecture on System Security Q & A Session	Discussion in Forum
60	IDS,Virus,Firewalls		Refer Text book -1	Lecture on IDS Q & A Session	Discussion in Forum
	Total No. of classes required =60				

Text Books:

1) Cryptography and Network Security, Behrouz A Forouzan, DebdeepMukhopadhyay, (3e)

Mc Graw Hill.

2) Cryptography and Network Security, William Stallings, (6e) Pearson.

3) Everyday Cryptography, Keith M.Martin, Oxford.

Reference Books:

1) Network Security and Cryptography, Bernard Meneges, Cengage Learning.