Department of Computer Science and Engineering

Academic Year	:	2023-2024	Course Name	:	CRYPTOGRAPHY
Semester	:	VII	Course Code	:	18CS744
Scheme	:	2018	L: T: P: C	:	3:0:0
Total Contact hours	:	40	CIE Marks	:	40
Course Plan Author	:	Mrs. MEGHANA SAMBARE R	SEE Marks	:	60
Date	:	11/09/2023	Total Marks	:	100

Course Prerequisites:

- Basic Knowledge about encoding and decoding mechanism.
- Basic Knowledge of linear algebra, matrix multiplication and modulus calculation process.
- Basic knowledge of computer networking concepts.

Learning Objectives:

- Define cryptography and its principles.
- Explain Cryptography algorithms.
- Illustrate Public and Private Key cryptography.
- Explain Key management, distribution and certification.
- Explain authentication protocols, Tell about IPsec.

Course Outcomes:

CO	*At the end of the course, student should be able to . . .*		Blooms' Level
CO1	:	Define cryptography and its principles, ciphering types.	L1
CO2	:	Explain Cryptographic algorithms.	L2
CO3	:	Illustrate Public and Private Key cryptography.	L3
CO4	:	Explain Key management, distribution and certification.	L2
CO5	:	Explain authentication protocols and Tell about IPsec.	L2

Blooms' Taxonomy:

L1	L2	L3	L4	L5	L6
Remembering	Understanding	Applying	Analyzing	Evaluating	Creating

Program Outcomes:

PO1	:	Engineering knowledge	**PO7**	:	Environment and sustainability
PO2	:	Problem analysis	**PO8**	:	Ethics
PO3	:	Design/development of solutions	**PO9**	:	Individual and team work
PO4	:	Conduct investigations of complex problems	**PO10**	:	Communication
PO5	:	Modern tool usage	**PO11**	:	Project management and finance
PO6	:	The engineer and society	**PO12**	:	Life-long learning

Program Specific Outcomes:

PSO1:	Model computational problems by applying mathematical concepts and design solutions using suitable data structures & algorithmic techniques.
PSO2:	Demonstrate basic knowledge of computer science in efficient design of problem solutions of varying complexity.
PSO3:	Create a career path to become a successful computer science professional, entrepreneur and relish for higher studies.

CO-PO-PSO Mapping:

CO	Program Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	2	2	-	-	-	-	-	-	-	-	-	-	1	1	-
CO2	2	2	-	1	-	-	-	-	-	-	-	1	2	2	-
CO3	2	2	-	-	-	-	-	-	-	-	-	1	2	2	-
CO4	2	-	-	-	-	-	-	-	-	-	-	1	2	-	-
CO5	2	-	-	-	-	-	-	-	-	-	-	1	2	-	-
Target	2.0	2.0	-	1.0	-	-	-	-	-	-	-	1.0	1.8	1.7	-

Course Content (Syllabus)

Module 1	**CH**
Classical Encryption Techniques Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques, Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, One Time Pad. Block Ciphers and the data encryption standard: Traditional block Cipher structure, stream Ciphers and block Ciphers, Motivation for the feistel	**08**

Cipher structure, the feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm **Textbook 1: Ch. 2.1,2.2, Ch. 3 RBT: L1, L2**	
Module 2	
Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. public-key cryptanalysis. The RSA algorithm, desription of the algorithm, computational aspects, the security of RSA. Other Public-Key Cryptosystems: Diffie-hellman key exchange, The algorithm, key exchange protocols, man in the middle attack,Elgamal Cryptographic systems **Textbook 1: Ch. 9, Ch. 10.1,10.2 RBT: L1, L2**	**08**
Module 3	
Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over Zp, elliptic curves overGF(2m), Elliptic curve cryptography, Analog of Diffie-hellman key exchange, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography, Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA. Key Management and Distribution: Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory,public key 08 authority, public keys certificates. **Textbook 1: Ch. 10.3-10.5, Ch.14.1 to 14.3 RBT: L1, L2.**	**08**
Module 4	
X-509 certificates. Certificates, X-509 version 3, public key infrastructure .User Authentication: Remote user Authentication principles, Mutual Authentication, one wayAuthentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one way Authentication, Kerberos, Motivation , Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one way Authentication. Electronic Mail Security: Pretty good privacy, notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing, enhanced security services, Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow. **Textbook 1: Ch. 14.4, Ch. 15.1 to 15.4, Ch.19 RBT: L1, L2**	**08**
Module 5	
IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service Transport and tunnel modes, combining security associations, authentication plus confidentiality, basic combinations of security associations, internet key exchange, key determinations protocol, header and payload formats, cryptographic suits. **Textbook 1: Ch. 20.1 to 20.3 RBT: L1, L2**	**08**

Schedule of Instruction:

Class No	Topic	RBT	CO	Mode
1.	Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques	L1	CO 1	L
2.	Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher	L2	CO 1	L
3.	Hill Cipher, Polyalphabetic Cipher, One Time Pad	L2	CO 1	L
4.	Block Ciphers and the data encryption standard: Traditional block Cipher structure,	L2	CO 1	L
5.	stream Ciphers and block Ciphers, Motivation for the feistel Cipher structure, the feistel Cipher,	L2	CO 1	L
6.	The data encryption standard, DES encryption, DES decryption, A DES example, results	L2	CO 1	L
7.	the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm,	L2	CO 1	L
8.	timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm	L2	CO 1	L
9.	Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems	L1	CO 2	L
10.	Applications for public-key cryptosystems,	L1	CO 2	L
11.	Requirements for public-key cryptosystems. Public-key cryptanalysis.	L1	CO 2	L
12.	The RSA algorithm, description of the algorithm	L2	CO 2	L
13.	Computational aspects, the security of RSA.	L2	CO 2	L
14.	Public-Key Cryptosystems: Diffie-hellman key exchange	L2	CO 2	L
15.	The algorithm, key exchange protocols	L2	CO 2	L
16.	Man in the middle attack, Elgamal Cryptographic systems	L2	CO 2	L

Class No	Topic	RBT	CO	Mode
17.	Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over Zp,	L1	CO 3	L
18.	elliptic curves overGF(2m), Elliptic curve cryptography, Analog of Diffie-hellman key exchange	L1	CO 3	L
19.	Elliptic curve encryption/ decryption, security of Elliptic curve cryptography,	L1	CO 3	L
20.	Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA.	L1	CO 3	L
21.	Key Management and Distribution: Symmetric key distribution using Symmetric encryption, A key distribution scenario	L2	CO 3	L
22.	Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control	L2	CO 3	L
23.	controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution,	L2	CO 3	L
24.	secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys,	L2	CO 3	L
25.	Publicly available directory, public key 08 authority, public keys certificates.	L2	CO 3	L
26.	X-509 certificates. Certificates, X-509 version 3, public key infrastructure .User Authentication: Remote user Authentication principles,	L1	CO 4	V
27.	Mutual Authentication, one way Authentication, remote user Authentication using Symmetric encryption,	L2	CO 4	V
28.	Mutual Authentication, one way Authentication, Kerberos, Motivation ,	L2	CO 4	V
29.	Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption,	L2	CO 4	V
30.	Mutual Authentication, one way Authentication. Electronic Mail Security: Pretty good privacy,	L2	CO 4	V
31.	notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality,	L2	CO 4	V
32.	S/MIME messages, S/MIME certificate processing, enhanced security services,	L2	CO 4	V

Class No	Topic	RBT	CO	Mode
33.	Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow.	L2	CO 4	V
34.	IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing applications,	L1	CO 5	V
35.	IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations,	L1	CO 5	V
36.	Security associations database, Security policy database, IP traffic processing,	L2	CO 5	V
37.	Encapsulating Security payload, ESP format, encryption and authentication algorithms,	L2	CO 5	V
38.	Padding, Anti replay service Transport and tunnel modes,	L1	CO 5	V
39.	combining security associations, authentication plus confidentiality,	L2	CO 5	V
40.	basic combinations of security associations, internet key exchange,	L2	CO 5	V
41.	key determinations protocol	L2	CO 5	V
42.	Header and payload formats, cryptographic suits.	L2	CO 5	V

Textbooks:

T1	William Stallings: Cryptography and Network Security, Pearson 6th edition.

Reference books:

R1	V K Pachghare: Cryptography and Information Security, PHI 2nd Edition.

Web links and Video Lectures (e-Resources):

1.	https://sites.google.com/skit.org.in/meghanasambare-crypto?usp=sharing
2.	https://nptel.ac.in/courses/106105166
3.	https://youtu.be/tn5vjuV569Y

Assessment Schedule:

S.N.	Assessment Type	Content	CO	Duration	Marks	Date
1.	CIE Test 1	M1 and M2	CO1,CO2	1:15 hrs	30	30,31 and 2 of Oct and Nov
2.	CIE Test 2	M3 and M4	CO3,CO4	1:15 hrs	30	27.28,29 of Nov
3.	CIE Test 3	M4 and M5	CO4,CO5	1:15 hrs	30	28,29,30 of Dec
4.	Assignment 1	M1 and M2	CO1,CO2		10	Before 1st internals
5.	Assignment 2	M3 and M4	CO3,CO4		10	Before 2nd internals
6.	Seminar/*any planned activity*	M3, Quiz, Jeopardy Game, Mini projects	CO5	1 hr	10	In the month DEC
7.	Semester End Examination	M1,M2,M3,M4,M5	CO1,CO2,CO3,CO4,CO5	3:00 hrs	60	IN JAN, FEB (2024)

***RB** – Text Book/**R**eference **B**ook, ***L** – **L**ecture, **V**- Videos or any other mode, ***RBT** – **R**evised **B**looms' **T**axonomy, **L: T: P: C** – Theory/**L**ecture: **T**utorial: **P**ractical/Drawing: **C**redits, **SEE**: **S**emester **E**nd **E**xamination, **CIE**: **C**ontinuous **I**nternal **E**valuation, **Seminar**: Group of 6-8 students, **Module** 1,2,3,4 & 5,*

The sum of total marks of three tests, two assignments, and seminar will be out of 100 marks and will be scaled down to 40 marks. (As per the scheme), **CIE + SEE = 40 + 60 = 100 marks

Meghana Sambare R	**Savitha B Patil**	**Shantharam Nayak**
Faculty In charge	**Course Coordinator**	**HoD**