MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

M. Tech COURSE PLAN

Theory Course

Department :	Computer Science and Engineering			
Course Name & code :	**ADVANCED CRYPTOGRAPHY CSE 5171**	**Core**		
Semester & branch :	**I Sem. M.Tech.**	**Computer Science and Information Security**		
Name of the faculty :	**Dr. RENUKA A**			
No of contact hours/week:	**L**	**T**	**P**	**C**
	3	**1**	**0**	**4**

COURSE OUTCOMES (COs)

At the end of this course, the student should be able to:		No. of Contact Hours	Marks
CO1	Describe the principles of number theory for cryptography	12	24
CO2	Apply number theory concepts in cryptographic algorithms	10	22
CO3	Analyse the various hashing algorithms	8	17
CO4	Compare the various digital signature schemes	8	17
CO5	Demonstrate the concepts of entity authentication and key management	10	20
	Total		**100**

ASSESSMENT PLAN

Components	Sessional 1	Sessional 2	Flexible Assessments (2 – 3 in number).	End semester/Makeup examination
Duration	60 minutes	60 minutes	To be decided by the faculty	180 minutes
Weightage	15%:	15%:	20%	50%
Typology of questions	Applying; Analysing;	Applying; Analysing;	Applying; Analysing. Evaluating. Creating	Applying; Analysing; Evaluating; Creating
Pattern	Answer all questions	Answer all questions	To decide by the Faculty. May be Assignments, Mini project, Assignment etc. Advisable to have Abstract, Literature, Problem Statement, Comparative analysis, design, Conclusion etc.	Answer all 5 full questions of 10 marks each. Each question may have 2 to 3 parts of 3/4/5/6/7 marks
Schedule	31/10/2022 to 5/11/2022	12/12/2022 to 17/12/2022	4 assignments descriptive type	2/1/2023 onwards
Topics covered	L1-L16 T1-T5	L17-L32 T6-T11	L1-L6, T1-T2 L7-L14, T3-T4 L15-L21, T5-T7 L22-L27, T8-T9	Comprehensive examination covering the full syllabus. Students are expected to answer all questions

LESSON PLAN

L No	TOPICS	Course Outcome Addressed
L0	Introduction to the course	NA
L1	A quick introduction to groups, rings	CO1
L2	Introduction to integral domain, and fields, Characteristic of a field, prime fields	CO1
L3	Arithmetic of polynomials over fields, Construction of fields with the help of an irreducible polynomial	CO1
T1	Tutorial on groups, rings, fields	CO1
L4	The fundamental theorem of Galois Theory, Overview of Fermat's Little Theorem, Euler's Theorem	CO1
L5	Chinese remainder theorem	CO1
L6	Primality testing algorithm, Euclid's algorithm for integers, quadratic residues	CO1
T2	Tutorial on Fermat's Theorem, Euler's Theorem, CRT, Euclid Algorithm	CO1
L7	Public Key Cryptosystem- RSA Cryptosytem	CO2
L8	RSA variants- Rabin Cryptosystem, ElGamal Cryptosystem	CO2
L9	Elliptic Curve Architecture and Cryptography Elliptic Curve over real numbers	CO2
T3	Tutorial on RSA, ElGamal	CO2
L10	Elliptic Curve over GF(p)	CO2
L11	Elliptic Curve Cryptography simulating ElGamal	CO2
L12	Elliptic Curve over GF(2^n)	CO2
T4	Tutorial on ECC	CO2
L13	Diffie- Hellman Key Exchange	CO2
L14	ECDH, ECDSA	CO2
L15	Hashing- Cryptographic hash functions, Properties of hashing, Serial and parallel hashing, Hashing based on Cryptosystems	CO3
L16	MD5, Keyed hashing	CO3
T5	Tutorial on Hashing functions	CO3
L17	Authentication requirements, Authentication functions	CO3
L18	Message Authentication Codes, Secure Hash Algorithm	CO3
L19	HMAC, CMAC	CO3
T6	Tutorial on SHA, HMAC, CMAC	CO3
L20	Iterated cryptographic Hash Function - Whirlpool	CO3
L21	Whirlpool- Contd..	CO3
T7	Tutorial on Whirlpool	CO3
L22	Digital Signatures- Services, Process, Digital Signature Schemes - RSA	CO4
L23	Digital Signature Schemes - El Gamal Digital Signature scheme	CO4
L24	Schnorr Signature Scheme	CO4
T8	Tutorial on Digital signature schemes	CO4
L25	Digital Signature Standard	CO4
L26	Elliptic Curve Digital Signature Scheme	CO4
L27	Variations and applications for digital signatures- Time stamped signatures, Blind Signatures, Undeniable signature	CO4
T9	Tutorial on Digital signature schemes	CO4
L28	Entity Authentication - Data-origin versus Entity Authentication, One-time password, Challenge – Response using a symmetric- key cipher	CO5
L29	Challenge – Response using keyed-hash functions, using an asymmetric-key cipher, using a digital signature	CO5
T10	Tutorial on Entity authentication	CO5

L30	Zero-Knowledge, Fiat -Shamir protocol, Feige-Fiat-Shamir protocol	CO5
L31	Guillou-Quisquater protocol, Biometric	CO5
L32	Key Management- Symmetric key distribution, KDC, session keys, servers. the symmetric key agreement	CO5
T11	Tutorial on Zero Knowledge, Key management	CO5
L33	Station to station key agreement. public key distribution, Public announcements, trusted center, controlled trusted center	CO5
L34	Certification authority, X.509, public key infrastructure, trust model, hijacking.	CO5
L35	Field extensions, Minimal Polynomial	CO1
L36	Splitting field of a polynomial, Separable polynomial and Separable extensions	CO1
T12	Tutorial on PKI and field extensions	CO1

References

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay – "Cryptography and Network Security", McGraw Hill, 2nd Edition, 2008.
2. S. Vaudenay, "A Classical Introduction to Cryptography: Applications for Communications Security", Springer International Edition, 2006.
3. Lawrence C. Washington, "Elliptic curves: number theory and cryptography", Chapman & Hall/ CRC Second Edition, 2008.
4. William Stallings,"Cryptography And Network Security Principles And Practice", Fifth Edition, Pearson Education, 2013

COURSE LEARNING OUTCOMES (CLOs)

CO	At the end of this course, the student should be able to:	No. of Contact Hours	Marks	Program Outcomes (PO's)	BL
CO1	Describe the principles of number theory for cryptography	12	24	PO1, PO3, PO5	L3
CO2	Apply number theory concepts in cryptographic algorithms	10	22	PO1, PO3, PO4, PO5	L3
CO3	Analyse the various hashing algorithms	8	17	PO1, PO2, PO3,PO4, PO5	L4
CO4	Compare the various digital signature schemes	8	17	PO1,PO2, PO3, PO4, PO5	L4
CO5	Demonstrate the concepts of entity authentication and key management	10	20	PO1,PO2, PO3, PO4, PO5	L4
	Total		**100**		

Course Articulation Matrix

CO/CLO	PO1	PO2	PO3	PO4	PO5
CO1	1	-	2	3	2
CO2	2	1	3	3	3
CO3	2	1	3	2	2
CO4	2	1	3	3	3
CO5	2	1	3	2	2
Average Articulation Level	1.8	1	2.8	2.6	2.6

Submitted by:
(Signature of the faculty)

Date: 12/9/2022

Approved by:

(Signature of HOD)

Date: 12/9/2022

FACULTY MEMBERS TEACHING THE COURSE (IF MULTIPLE SECTIONS EXIST):

FACULTY	SECTION	FACULTY	SECTION
RENUKA A	CSIS	NA	NA