SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Department of Applied Mathematics	LP: MA18186 Rev. No: 00 Date:05/01/2022
M.E/M.Tech : IT **Regulation:2018_** **PG Specialisation Cyber Forensics and Information Security** **Sub. Code /Sub.Name: MA18186/Mathematical Foundations For Information Security** **Unit I Number Theory**	

Unit Syllabus: Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theorem. Congruences - Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

Objective: Learn and understand the basic Number theoretic concepts regarding Cryptography.

Session No *	Topics to be covered	Ref	Teaching Aids
1	Introduction-Divisibility	1. Ch4 237	LCD/BB
2	Modular Arithmetic	1. Ch4 239/6 ch5 154	LCD/BB
3	Primes	1. Ch4 240	LCD/BB
4	GCD	1. Ch4 241/6 ch5 167	LCD/BB
5	Fermat Numbers	1. Ch4 242	LCD/BB
6	Euclidean Algorithm	1. Ch4 243/6 ch7 234	LCD/BB
7	Euler function/theorem	1. Ch4 237	LCD/BB
8	Congruences	1. Ch4 237/6 ch6 255	LCD/BB
9	Application of congruences	1. Ch4 237	LCD/BB
10	Residue classes	1. Ch4 237	LCD/BB
11	Chinese Remainder Theorem	1. Ch4 237/6 ch7 265	LCD/BB
12	Consolidation	1. Ch4 /6 ch4,5,6	LCD/BB

Content beyond syllabus covered (if any):

* Session duration: 50 minutes

Sub. Code / Sub. Name: MA18186/Mathematical Foundations For Information Security

Unit : II Algebraic Structures I

Unit Syllabus : Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Rings – Sub rings, ideals and quotient rings

Objective:

Session No *	Topics to be covered	Ref	Teaching Aids
1	Groups-Basic Introduction	2. Ch1 10	LCD/BB
2	Groups -Theorems	2. Ch1 14	LCD/BB
3	Cyclic groups	2. Ch1 59	LCD/BB
4	Cosets-Introduction	2. Ch2 96	LCD/BB
5	Cosets-Theorems	2 Ch2 97	LCD/BB
6	Modulo groups	1. Ch4 243	LCD/BB
7	Primitive roots	1. Ch4 237	LCD/BB
8	Rings	2. Ch4 167	LCD/BB
9	Sub rings	2. Ch4 170	LCD/BB
10	Rings/sub rings problems	2. Ch4 169	LCD/BB
11	Ideals	2. Ch5 237	LCD/BB
12	Quotient rings	7. Ch3 133	LCD/BB

Content beyond syllabus covered (if any):

* Session duration: 50 mins

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Sub. Code / Sub. Name: MA18186/Mathematical Foundations For Information Security

Unit : III Algebraic Structures II

Unit Syllabus : Integral domains, Fields – Finite fields - Classification - Structure of finite fields

Objective:

Session No *	Topics to be covered	Ref	Teaching Aids
1	Integral Domains Introduction	7. Ch3 140	LCD/BB
2	Integral Domain Examples/Theorems	7. Ch3 142	LCD/BB
3	Integral Domain Applications	7. Ch3 141	LCD/BB
4	Fields-Definition	7. Ch5 207	LCD/BB
5	Fields- Theorems	7. Ch5 208	LCD/BB
6	Fields- Application examples	7. Ch5 209	LCD/BB
7	Finite fields	7. Ch5 210	LCD/BB
8	Finite fields-Applications	7. Ch5 210	LCD/BB
9	Finite Fields -Problems	7. Ch5 211	LCD/BB
10	Classification	1. Ch4 237	LCD/BB
11	Structure of finite fields-discussion	1. Ch4 237/6 ch7 265	LCD/BB
12	Consolidation	1. Ch4 /6 ch4,5,6	LCD/BB

Content beyond syllabus covered (if any):

* Session duration: 50 mins

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Sub. Code / Sub. Name: MA18186/Mathematical Foundations For Information Security

Unit : IV Coding Theory

Unit Syllabus : Introduction - Basic concepts - Codes, minimum distance, equivalence of codes, Linear codes - Generator matrices and parity - Check matrices - Hamming codes

Objective:

Session No *	Topics to be covered	Ref	Teaching Aids
1	Coding theory Introduction	4. Ch1 1-2	LCD/BB
2	Coding theory definitions	4. Ch1 3	LCD/BB
3	Coding theory-Application problems	4. Ch1 4	LCD/BB
4	Coding-encoding decoding discussion	4. Ch2 8	LCD/BB
5	Minimum distances-Discussion	4. Ch2 10	LCD/BB
6	Equivalence of codes	4. Ch2 11	LCD/BB
7	Linear Codes	4. Ch4 44	LCD/BB
8	Linear codes Application examples	4. Ch4 45	LCD/BB
9	Generation matrices	4. Ch4 52	LCD/BB
10	Parity check matrices	4. Ch4 53	LCD/BB
11	Matrices -Application examples	4. Ch4 5	LCD/BB
12	Hamming Codes	4. Ch4 46	LCD/BB

Content beyond syllabus covered (if any):

* Session duration: 50 mins

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Sub. Code / Sub. Name: MA18186/Mathematical Foundations For Information Security

Unit : V Elliptic Curves and Pseudo random Number Generation

Unit Syllabus : Discrete Logarithm - Elliptic curves - Introduction to Pseudo random numbers.

Objective:

Session No *	Topics to be covered	Ref	Teaching Aids
1	Discrete Logarithm-Definition	5. Ch5 143	LCD/BB
2	Discrete Logarithm-discussion	5. Ch5 144	LCD/BB
3	Discrete Logarithm-Problems and applications	5. Ch5 145	LCD/BB
4	Elliptic Curves-Definition	5. Ch6 169	LCD/BB
5	Elliptic Curves-Discussion	5. Ch6 170	LCD/BB
6	Elliptic Curves-problems and Application	5. Ch6 171	LCD/BB
7	Random Number	3. Ch4 164	LCD/BB
8	Random variates	3. Ch4 165	LCD/BB
9	Pseudo Random number generation	3. Ch4 166	LCD/BB
10	Pseudo Random number generation	3. Ch4 167	LCD/BB
11	Pseudo Random number generation-Testing	3. Ch4 170	LCD/BB
12	Pseudo Random number generation-Testing	3. Ch4 171	LCD/BB

Content beyond syllabus covered (if any):

* Session duration: 50 mins

Sub Code / Sub Name: MA18186/Mathematical Foundations For Information Security

REFERENCES:

1. Kenneth H Rossen, Discrete Mathematics and its Applications, Seventh Edition, McGraw Hill, 2012.
2. Fraleigh J.B., A first course in abstract algebra, Pearson Education, 2005..
3. Jerry Banks, Discrete Event Simulation, Pearson, 2005.
4. San Ling, Chaoping Xing, Coding Theory-A first Course, Cambridge University Press,2004.
5. L. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman & Hall CRC, 2003.
6.Niven, H.S. Zuckerman, H. L. Montgomery, An introduction to the theory of numbers, John Wiley and Sons, 2001
7.I.N.Herstein, Topics in Algebra, John Wiley, 2nd Edition, 1975.

	Prepared by	Approved by
Signature		
Name	Dr.J.Vijayarangam	Dr.R.Muthucumaraswamy
Designation	Assistant Professor	Professor and Head
Date	05/01/2022	05/01/2022
Remarks *:		
Remarks *:		

* If the same lesson plan is followed in the subsequent semester/year it should be mentioned and signed by the Faculty and the HOD