SRINIVAS UNIVERSITY
COLLEGE OF ENGINEERING & TECHNOLOGY

Department Of Computer Science and Engineering

TEACHING/LESSON PLAN (EVEN Semester 2021-22)

Subject Code		**19SEC641**	**Title**	**CRYPTOGRAPHY, NETWORK SECURITY AND CYBER LAW**		**Class**	**VITH SEM**		
Prerequisites					**Faculty Name**		**Prof. Veeranna Kotagi**		
Credits	**4**	**Hours/week**	**L-T-P: 4**		**CIE Marks**	**50**	**SEE Marks**	**50**	**Total Hours**	**50**

Course Objectives:

1.Understand the use of number theory and finite fields network security.
2.Explain the concepts of encryption techniques.
3. Illustrate key management issues and solutions.
4.Familiarize with cryptography and very essential algorithms.

Course Outcomes of the Course:

On Completion of this Course the Student was able to,

CO id	Course Outcome
CO1	Define and explain number theory and finite fields network security.
CO2	Discuss cryptography and it's needs to various applications.
CO3	Define types of ciphers.
CO4	Design and develop simple cryptography algorithms.
CO5	Use hash functions.

CO-PO Mapping:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	3	3	-	-	2	-					
CO2	3	3	2	-	1	-	-					
CO3	1	2	2	3	-	2	2					
CO4	2	1	3	2	2	-	1					
CO5	2	3	3	-	2	1	3					

Lesson/Teaching Plan of the Course:

Hour No.	Plan Date	Actual Date	Topic to be covered	CO Mapping	Mode of Delivery	Text/ Reference book
1	15/03/2022	15/03/2022	Module-1: Basic concepts of number theory and finite fields: Divisibility	1	PPT/CHALK	T1
2	15/03/2022	19/03/2022	Divisibility algorithm	4	PPT/CHALK	T1
3	15/03/2022	22/03/2022	Euclidian algorithm	4	PPT/CHALK	T1
4	15/03/2022	29/03/2022	Modular arithmetic	1	PPT/CHALK	T1
5	15/03/2022		Groups	3	PPT/CHALK	T1
6	15/03/2022		Rings	3	PPT/CHALK	T1
7	15/03/2022		Fields	3	PPT/CHALK	T1

8	15/03/2022		Finite fields if the form GF(p)	1	PPT/CHALK	T1
9	16/03/2022		Polynomial arithmetic	1	PPT/CHALK	T1
10	17/03/2022		Finite fields of the formGF(2n)	2	PPT/CHALK	T1
11	19/03/2022		Module-2: Classical encryption techniques: Symmetric cipher model	2	PPT/CHALK	T1
12	22/03/2022		Symmetric cipher model (Cont..)	3	PPT/CHALK	T1
13	22/03/2022		Substitution techniques	3	PPT/CHALK	T1
14	23/03/2022		Substitution techniques (Cont..)	3	PPT/CHALK	T1
15	24/03/2022		Transposition techniques	4	PPT/CHALK	T1
16	26/03/2022		Transposition techniques (Cont..), Stegnography	4	PPT/CHALK	T1
17	29/03/2022		Symmetric ciphers: Traditional block cipher structure	4	PPT/CHALK	T1
18	30/03/2022		Traditional block cipher structure (Cont..)	4	PPT/CHALK	T1
19	31/03/2022		Data encryption technique	2	PPT/CHALK	T1
20	01/04/2022		Data encryption technique (Cont..)	2	PPT/CHALK	T1
21	05/04/2022		Module-3: Symmetric ciphers: AES cipher	4	PPT/CHALK	T2
22	06/04/2022		Pseudo-Random –Sequence Generators and Sream ciphers.	4	PPT/CHALK	T2
23	07/04/2022		Linear congruential generators	4	PPT/CHALK	T2
24	09/04/2022		Linear congruential generators (Cont..)	4	PPT/CHALK	T2
25	12/04/2022		Linear feedback shift registers	4	PPT/CHALK	T2
26	13/04/2022		Linear feedback shift registers (Cont..)	4	PPT/CHALK	T2
27	16/04/2022		Linear feedback shift registers (Cont..)	**4**	PPT/CHALK	T2
28	26/04/2022		Design and analysis of stream ciphers using LFSRs	4	PPT/CHALK	T2
29	27/04/2022		Design and analysis of stream ciphers using LFSRs (Cont..)	4	PPT/CHALK	T2
30	28/04/2022		Design and analysis of stream ciphers using LFSRs (Cont..)	1	PPT/CHALK	T2
31	30/04/2022		Module-4: More number theory	1	PPT/CHALK	T2
32	04/05/2022		Prime numbers	1	PPT/CHALK	T2
22	05/05/2022		Fermat’s theorem	1	PPT/CHALK	T2
34	07/05/2022		Euler theorem	1	PPT/CHALK	T2
35	10/05/2022		Primality testing, Chinese remainder theorem	4	PPT/CHALK	T2
36	11/05/2022		Discrete logarithm	4	PPT/CHALK	T2
37	12/05/2022		The RSA algorithm	4	PPT/CHALK	T2

38	14/05/2022		Diffie-Hellman key exchange	3	PPT/CHALK	T2
39	17/05/2022		Elliptic curve arithmetic	3	PPT/CHALK	T2
40	18/05/2022		Elliptic curve cryptography	3	PPT/CHALK	T2
41	19/05/2022		Module-5: One way hash functions: Background, Snefru	5	PPT/CHALK	T1
42	21/05/2022		N-Hash, MD4, Secure hash algorithm	5	PPT/CHALK	T2
43	24/05/2022		One way hash functions using symmetric block algorithms	5	PPT/CHALK	T1
44	25/05/2022		Using public key algorithms	4	PPT/CHALK	T1
45	26/05/2022		Choosing one way hash functions	4	PPT/CHALK	T2
46	28/05/2022		Message authentication codes	3	PPT/CHALK	T2
47	31/05/2022		Digital signature algorithm	4	PPT/CHALK	T2
48	01/06/2022		Digital signature algorithm (Cont..)	4	PPT/CHALK	T1
49	02/06/2022		Discrete logarithm signature scheme	4	PPT/CHALK	T2
50	04/06/2022		Discrete logarithm signature scheme (Cont..)	4	PPT/CHALK	T2

TEXT/REFERENCE BOOKS:

T/R	BOOK TITLE/AUTHORS/PUBLICATION
T1	Cryptography, Network Security And Cyber Law – William Stallings, Pearson Education, 7th edition.
T2	Cryptography, Network Security, 2nd edition, Debadeep Mukhyopadhyay
R1	Network Security: The Complete Reference Paperback – 1 July 2017 by Roberta Bragg (Author), Mark Rhodes-Ousley (Author), Keith Strassberg (Author)
R2	Cryptography And Network Security | 3rd Edition Paperback – 1 January 2015 by Forouzan

Faculty Member **HOD**

Date: