SSN COLLEGE OF ENGINEERING
Department of CSE
COURSE PLAN

SUBJECT NAME	**:**	**CRYPTOGRAPHY AND NETWORK SECURITY**
SUBJECT CODE	**:**	**CS6701**
DEGREE / YEAR	**:**	**B.E. CSE / IV YEAR/ A & B Sections**
BATCH	**:**	**2013-2017**
SEMESTER	**:**	**VII (2016-17: Odd)**
NAME OF THE STAFF	**:**	**J. BHUVANA & V. BALASUBRAMANIAN**
DESIGNATION	**:**	**ASSOCIATE PROFESSOR**

Teaching Methodology and aids (Content Delivery Method (CDM)) : **PowerPoint presentations\Projector\Use of ICT\Chalk and Blackboard (For all topics)**

Sl. No	Unit No	Topic	CDM	No of Hrs (plan)	No of Hrs (actual)	Remarks
1.	**UNIT 1 (10 Hrs)**	**INTRODUCTION & NUMBER THEORY:** Services, Mechanisms and attacks , Network security model		**1**		
2.		Classical Encryption techniques (Symmetric cipher model, substitution techniques		**3**		
3.		Transposition techniques, Steganography		**1**		
4.		FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic		**1**		
5.		Euclid's algorithm-Finite fields- Polynomial Arithmetic		**1**		
6.		Prime numbers-Fermat's and Euler's theorem		**1**		
7.		Testing for primality		**1**		
8.		The Chinese remainder theorem, Discrete logarithms		**1**		
		Planned Hours		**10**		
9.	**UNIT 2 (10 Hrs)**	**BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY** Data Encryption Standard		**1**		
10.		Block cipher principles, block cipher modes of operation, Triple DES		**2**		
11.		Advanced Encryption Standard (AES)	**VL**	**1**		
12.		Blowfish, RC5 algorithm.		**1**		
13.		Public key cryptography: Principles of public key cryptosystems		**1**		
14.		The RSA algorithm		**1**		
15.		Key management		**1**		
16.		Diffie Hellman Key exchange		**1**		
17.		Elliptic curve arithmetic, Elliptic curve cryptography		**1**		
18.		**Planned Hours**		**10**		
19.	**UNIT 3 (8 Hrs)**	**HASH FUNCTIONS AND DIGITAL SIGNATURES:** Authentication requirement, Authentication function , MAC, Security of MAC		**1**		
20.		Hash function, Security of hash function		**1**		
21.		MD5, SHA		**2**		
22.		HMAC, CMAC		**1**		
23.		Digital signature and authentication protocols		**1**		
24.		DSS		**1**		
25.		EI Gamal, Schnorr		**1**		

Sl. No	Unit No	Topic	CDM	No of Hrs (plan)	No of Hrs (actual)	Remarks
26.		**Planned Hours**		**8**		
27.		**SECURITY PRACTICE & SYSTEM SECURITY** Authentication applications – Kerberos		**2**		
28.		X.509 Authentication services		**1**		
29.		Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs, Firewalls design principles		**2**		
30.	**UNIT 4**	SET for E-Commerce Transactions		**1**		
31.		Intruder – Intrusion detection system		**1**		
32.	**(8 Hrs)**	Virus and related threats – Countermeasures, Trusted systems, Practical implementation of cryptography and security**.**		**1**		
33.		**Planned Hours**		**8**		
34.		**E-MAIL, IP & WEB SECURITY** E-mail Security: Security Services for E-mail-attacks possible through E-mail - establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy		**2**		
35.		S/MIME		**1**		
36.	**UNIT 5**	IPSecurity: Overview of IPSec - IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding).		**3**		
37.	**(9 Hrs)**	Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSL Attacks fixed in v3- Exportability-Encoding		**2**		
38.		Secure Electronic Transaction (SET)		**1**		
39.		**Planned Hours**		**9**		

Total Number of Syllabus Hours: 45
Total Number of Planned Hours: 45

Content Delivery Methods (CDM): VL- Video Lecture

PREPARED BY

APPROVED BY
Dr.Chitra Babu
HOD-CSE