ST.ANN'S COLLEGE OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
LESSON PLAN

NAME OF THE SUBJECT: **Cryptography and Network Security**
SECTION: **IV CSE-A**
NAME OF THE INSTRUCTOR: **T.Seshasai**

S.No	Topics	No. Of Classes Required
1	Introduction: Security attacks, services & mechanisms, Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Cyber threats and their defense (Phishing Defensive measures, web based attacks, SQL injection & Defense techniques) Buffer overflow & format string vulnerabilities, TCP session hijacking (ARP attacks, route table modification) UDP hijacking (man-in-the-middle attacks).	8
2	Traditional Block Cipher Structure, DES, Block Cipher Design Principles, AES-Structure, Transformation functions, Key Expansion, Blowfish, CAST-128, IDEA, Block Cipher Modes of Operations	7
3	Number Theory: Prime and Relatively Prime Numbers, Modular Arithmetic, Fermat's and Euler's Theorems, The Chinese Remainder theorem, Discrete logarithms. Public Key Cryptography: Principles, public key cryptography algorithms, RSA Algorithms, Diffie Hellman Key Exchange, Elgamal encryption & decryption, Elliptic Curve Cryptography.	13
4	Application of Cryptographic Hash Functions, Requirements & Security, Secure Hash Algorithm, Message Authentication Functions, Requirements & Security, HMAC & CMAC. Digital Signatures, NIST Digital Signature Algorithm. Key management & distribution.	12
5	User Authentication: Remote user authentication principles, Kerberos, Transport Level Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Shell(SSH), Electronic Mail Security: Pretty Good Privacy (PGP) and S/MIME.	5
6	IP Security: IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.Intrusion detection: Overview, Approaches for IDS/IPS, Signature based IDS, Host based IDS/IPS.	9

TOTAL NO. OF CLASSES REQUIRED: 54

TEXT BOOKS:

1. Cryptography & Network Security: Principles and Practices, William Stallings, PEA, Sixth edition.
2. Introduction to Computer Networks & Cyber Security, Chwan Hwa Wu, J.David Irwin, CRC press
3. Hack Proofing your Network, Russell, Kaminsky, Forest Puppy, Wiley Dreamtech.

REFERENCE BOOKS:

1. Everyday Cryptography, Fundamental Principles & Applications, Keith Martin, Oxford
2. Network Security & Cryptography, Bernard Menezes, Cengage,2010

FACULTY **HOD**