JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY ANANTAPUR
(Established by Govt. of A.P., ACT No.30 of 2008)
ANANTHAPURAMU – 515 002 (A.P) INDIA

MASTER OF COMPUTER APPLICATIONS

Course Code	NETWORK SECURITY	L	T	P	C
21F00304b		3	0	0	3
Semester		III			

Course Objectives:

- Network security using various cryptographic algorithms.
- Underlying network security applications. It also focuses on the practical applications that have been implemented and are in use to provide email and websecurity.

Course Outcomes (CO): Student will be able to

- Understand the most common type of cryptographic algorithm
- Understand the Public-Key Infrastructure
- Understand security protocols for protecting data on networks
- Be able to digitally sign emails and files
- Understand vulnerability assessments and the weakness of using passwords for authentication
- Be able to perform simple vulnerability assessments and password audits

UNIT - I — Lecture Hrs:

Attacks, Services and Mechanisms, Security Attacks, Security Services, Integrity check, digital Signature, authentication, has algorithms.

UNIT - II — Lecture Hrs:

Block Encryption, DES rounds, S-Boxes IDEA: Overview, comparison with DES, Key expansion, IDEA rounds, Uses of Secret key Cryptography; ECB, CBC, OFB, CFB, Multiple encryptions DES

UNIT - III — Lecture Hrs:

Length of hash, uses, algorithms (MD2, MD4, MD5, SHS, MD2: Algorithm (Padding, checksum, passes.) MD4 and 5: algorithm (padding, stages, digest computation.) SHS: Overview, padding, stages. Algorithms, examples, Modular arithmetic (addition, multiplication, inverse, and exponentiation) RSA: generating keys, encryption and decryption. Other Algorithms: PKCS, Diffie-Hellman, El-Gamal signatures, DSS, Zero-knowledge signatures.

UNIT - IV — Lecture Hrs:

Password Based, Address Based, Cryptographic Authentication. Passwords in distributed systems, on-line vs offline guessing, storing. Cryptographic Authentication: passwords as keys, protocols, KDC's Certification Revocation, Interdomain, groups, delegation. Authentication of People: Verification techniques, passwords, length of passwords, password distribution, smart cards, biometrics.

UNIT - V

What is security policy, high and low level policy, user issues? Protocol problems, assumptions, Shared secret protocols, public key protocols, mutual authentication, reflection attacks, use of timestamps, nonce and sequence numbers, session keys, one-and two-way public key based authentication.

Text Books:

1. AtulKahate, Cryptography and Network Security, McGraw Hill.
2. Kaufman, c., Perlman, R., and Speciner, M., Network Security, Private Communication in a public world, 2nd ed., Prentice HallPTR., 2002.
3. Stallings W.Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall PTR.,2003
4. Stallings, W. Network security Essentials: Applications and standards, Prentice Hall, 2000.
5. Cryptography and Network Security; McGraw Hill; Behrouz A Forouzan.
6. Information Security Intelligence Cryptographic Principles and App. CalabresThomson.
7. Securing A Wireless Network Chris Hurley SPD.