Course Title : **Network Security**
Course Code : COM 732.3
Credit : 3
Class Load : 3 hours
Evaluation :

	Theory	**Practical**	**Total**
Sessional	50	-	50
Final	50	-	50
Total	100	-	100

Course Objective:

The course objective is to impart fundamental understanding of every facet of information security, from the basics to advanced cryptography, authentication, secure web, email services and emerging best practices with security standards.

Course Contents:

1. **Introduction** **(4 hrs)**
Security, Attacks, Attack Types, Viruses, Worms, Trojan Horses, Hacker Techniques, Security Services, Network Security Model, Security Levels, Internet Standards and RFCs.

2. **Conventional Encryption / Secret Key Cryptography** **(9 hrs)**
Cryptography, Cryptanalysis, Cipher Structure, Encryption Algorithms, Data Enncryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Modes of Operation, Symmetric Block Ciphers, Cipher Block Chaining (CBC), Multiple Encryption DES

3. **Public Key Cryptography and Message Digests** **(10 hrs)**
Hashes, Secure Hash Algorithm (SHA), Encryption with Message Digest (MD), MD5, Public Key Cryptography Principles, Public Key Cryptography Algorithms, RSA, Digital Signature Standard (DSS).

5. **Authentication and Public Key Infrastructure (PKI)** **(6 hrs)**
Overview of Authentication Systems (Password, Address, Crptographic), Security Handshake Pitfalls, Authentication Standards, Kerberos, PKI Trust Models, Revocation, Realtime Communication Security.

6. **Network Security** **(8 hrs)**
Email Security, PGP, S/MIME, IPSecurity, Architecture, Authentication Header, Security Association, Key Management, Web Security, Secure Socket Layer(SSL), Transport Layer Security(TLS), Secure Electronic Transaction(SET), Network Management Security, Different versions of SNMPs

7. **System Wide Security** **(3 hrs)**
Intruders, Viruses, Firewalls, DMZ

7. **Other Issues** **(5 hrs)**
Legal Issues, Various criminal laws related to Information Security, Privacy Issues, Policy, Importance of Policy, Various Policies, Risk Management, Measure Risks, Information Security Processes.

References:

1. Charlie Kaufman, Radia Perlman, Mike Speciner, *Nework Security Private Communication in a Public World*, Second Edition, 2004,Pearson.
2. William Stallings, *Network Security Essentials-Applications & Standards*, Pearson.
3. Eric Maiwald, *Fundamentals of Network Security*, 2004, Osborne/McGraw Hill, Dreamtech Press
4. Matt Bishop, *Computer Security, Art and Science*, Pearson