Second Semester

Network Security and Cryptology (MCS-121)
Department Elective (DE-II); 4 Credits (3-1-0)

Objectives:

The student should be made to: Understand OSI security architecture and classical encryption techniques. Acquire fundamental knowledge on the concepts of finite fields and number theory. Understand various block cipher and stream cipher models.

Unit	Contents	No. of Lectures
Unit 1	**Introduction & Number Theory:** Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography).FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic- Euclid's algorithm-Finite fields-Polynomial Arithmetic –Prime numbers-Fermat's and Euler's theorem- Testing for primality -The Chinese remainder theorem- Discrete logarithms	10
Unit 2	**BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY** :Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management – Diffie Hellman Key exchange- Elliptic curve arithmetic-Elliptic curve cryptography.	8
Unit 3	**HASH FUNCTIONS AND DIGITAL SIGNATURES** Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC –MD5 – SHA – HMAC – CMAC – Digital signature and authentication protocols – DSS – EI Gamal – Schnorr.	12
Unit 4	**SECURITY PRACTICE & SYSTEM SECURITY** Authentication applications – Kerberos – X.509 Authentication services – Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls – Firewall designs – SET for E-Commerce Transactions. Intruder – Intrusion detection system – Virus and related	8

threats – Countermeasures – Firewalls design principles – Trusted systems – Practical implementation of
cryptography and security.

Unit 5	**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-S/MIME. IPSecurity: Overview of IPSec – IP and IPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSLAttacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET).	**8**
		46

Reference/Text Books:

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education,March 2013..
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.

System and Network Administration (MCS-122)
Department Elective (DE-III); 4 Credits (3-1-0)

Objective:

1. This course will introduce the beginning computer user to basic computer concepts and applications thus providing an overview of computer information systems. Students will explore various topics such as computer hardware components, operating systems software, applications software, computer network basics, ethical issues in information technology, the Internet, and e-mail. Students will gain hands-on experience in the following areas: basic computer operations, basic operating system applications, Internet and e-mail applications, word processing application, spreadsheet applications, database management applications, and presentation applications.

Unit	Contents	No. of Lectures
Unit 1	**Configuring File Services:** • Configure a file server which Include: File share publishing, Offline files, share permissions, NTFS permissions, encrypting file system (EFS). • Configure Distributed File System(DFS). Include**:** DFS name space, DFS configuration and replication, creating and configuring targets, DFS replication. • Configure backup and restore. Include: Backup type, backup schedules, managing remotely, restoring data. • Manage disk quotas: Include Quota by volume or quota by user, quota entries, quota templates.	**05**
Unit 2	**Configuring the Active Directory infrastructure** • Configure a forest or a domain. Include: remove a domain, perform an unattended installation, raise forest and domain functional levels, interoperability with previous versions of Active Directory, alternate user principal name (UPN) suffix, forestprep, domainprep. • Configure Trusts. Include: forest trust, selective authentication versus forest-wide authentication, transitive trust, Parent-child trust, tree-root trust, Cross-forest trust, external trust, shortcut trust, realm trust, • Configuration Active Directory replication. Include: Distributed File system, one-way replication, bridgehead server, replication scheduling, force intersite replication. • Configure the global catalog. Include: Universal Group Membership Caching, partial attribute set, promote to global catalog. • Configuring additional Active Directory server roles • Configure the read-only domain controller(RODC)	**06**

	Include: Unidirectional replication, Administrator role sepration, read-only DNS, password replication, syskey.	
Unit 3	**Creating and maintaining Active directory objects:** • Automate creation of Active Directory accounts. **Include:** Bulk import, configure the UPN, create computer, user, and group accounts (script, import migration), template accounts, contact, distribution list. • Maintain Active Directory Accounts. **Include:** Configure group membership, account resets, delegation, Deny domain local group, local versus domain, protected Admin, Disabling accounts versus deleting accounts, deprovisioning, contacts, creating organizational units (OUs), delegation of control.	**04**
Unit 4	**Create and apply Group Policy Objects (GPOs)** Include: OU hierarchy, block inheritance and enabling user objects, group policy processing priority, Group policy filtering, Group policy loopback. • Configure GPO templates. Include: User rights, administrative templates, security templates, restricted groups, security options, starter GPOs, shell access policies. • Configure software deployment GPOs. Include: Publishing to users, assigning software to users, assigning to computers, software removal. • Configure account policies. Include: domain password policy, account lockout policy, fine-grain password policies. • Configure audit policy by using GPOs. Include: audit logon events, audit account login events, audit policy change, audit access privilege use, audit directory service access, audit object access.	**06**
Unit 5	**Backup and restore:** Configuration of Backup in Server 2008, Incremental versus complete	**10**

	backup, backup schedule in server 2008, restoration of backup,	
Unit 6	**Configuration of DHCP Server:** **Include:** Basic about DHCP Server and BOOTP Protocol, DHCP options, creating new options, Scope, Reservation, Lease, DHCP exclusion range, DHCP discover, DHCP offer, DHCP request, DHCP Acknowledgment etc, Configuration of DHCP Server, Backup and restore of DHCP, Industrial use of DHCP server,	**07**
		38

Reference/Text Books:

1. Configuration of Windows Server 2008 Active Directory by Dan Holme

Optimization Technique (MCS-123)
Discipline Core (DC); 4 Credits (3-1-0)

Objectives:

After successful completion of the course, student will be able to:

1. understand importance of optimization of industrial process management
2. apply basic concepts of mathematics to formulate an optimization problem
3. analyse and appreciate variety of performance measures for various optimization problems

Unit	Contents	No. of Lectures
Unit 1	**Introduction to Operation Research:** Operation Research approach, scientific methods, introduction to models and modeling techniques, general methods for Operation Research models, methodology and advantages of Operation Research, history of Operation Research.	**8**
Unit 2	**Linear Programming (LP):** Introduction to LP and formulation of Linear Programming problems, Graphical solution method, alternative or multiple optimal solutions, Unbounded solutions, Infeasible	**10**

	solutions, Maximization – Simplex Algorithm, Minimization – Simplex Algorithm using Big-M method, Two phase method, Duality in linear programming, Integer linear programming.	
Unit 3	**Transportation & Assignment Problems:** Introduction to Transportation problems, various methods of Transportation problem, Variations in Transportation problem, introduction to Assignment problems, variations in Assignment problems. **Network Analysis:** Network definition and Network diagram, probability in PERT analysis, project time cost trade off, introduction to resource smoothing and allocation. **Sequencing:** Introduction, processing N jobs through two machines, processing N jobs through three machines, processing N jobs through m machines.	**12**
Unit 4	**Inventory Model:** Introduction to inventory control, deterministic inventory model, EOQ model with quantity discount. **Queuing Models:** Concepts relating to queuing systems, basic elements of queuing model, role of Poison & exponential distribution, concepts of birth and death process. .	**6**
Unit 5	**Replacement & Maintenance Models:** Replacement of items, subject to deterioration of items subject to random failure group vs. individual replacement policies. **Simulation:** Introduction & steps of simulation method, distribution functions and random number generation.	**6**
		42

References/Text Books:

1. Rogers, "Procedural Elements of Computer Graphics", McGraw Hill
2. Asthana, Sinha, "Computer Graphics", Addison Wesley Newman and Sproul, "Principle of Interactive Computer Graphics", McGraw Hill

3.Steven Harrington, "Computer Graphics", A Programming Approach, 2nd Edition

4. Rogar and Adams, "Mathematical Elements of Computer Graphics", McGraw Hill.