Unit 6: Replication and Storage Security: **(6)**

Local Replication, Uses of Local Replicas, Data Consistency, Local Replication Technologies, Restore and Restart Considerations.

Storage Security: Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementations in Storage Networking.

Text Books:

1. A Information Storage and Management by G. Somasudaram – EMC Education Services (Wiley India Edition).
2. Storage Networks Explained by Ulf Troppen, Rainer Erkens, Wolfgang Müller (Wiley India Edition).

5. INFORMATION SECURITY

Lectures : 3 Hrs/week   Theory : 100 Marks
Tutorials: 1 hr/week   Termwork :25 Marks

Course Objectives:
1. To introduce Information security services and mechanisms to the students.
2. To make students feel the security services widely used in Internet and Web services.
3. To give hands on exposure to various security tools and security related issues.
4. To practice ethics in using and developing security softwares.

UNIT I. Classical Encryption Techniques: Overview – The OSI Security Architecture, Security Attacks, Services and Mechanism, A Model for Network Security, Classical Encryption Techniques – Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography. (6)

UNIT II. DES and Public Key Cryptography: Block Cipher and Data Encryption Standard – Block Cipher Principles, The Data Encryption Standard, The Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles. Public Key Cryptography and RSA - Principles of Public Key Cryptosystems, The RSA Algorithm. (7)

UNIT III. Key Management and Authentication: Key Management; Other Public-Key Cryptosystems- Key Management, Diffie-Hellman Key Exchange, Message Authentication and

HASH Functions- Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions. (5)

UNIT IV. Digital Signatures and Authentication Applications: Digital Signatures and Authentication Protocols - Digital Signatures, Authentication Protocols, Digital Signature Standard. Authentication Applications - Kerberos, X.509 Authentication Service, Public - Key Infrastructure. (7)

UNIT V. Electronic mail and IP security: Electronic Mail Security - Pretty Good Privacy, S/MIME, IP Security – IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload. (6)

UNIT VI. Web and System Security: Web Security - Web Security Considerations, Secure Socket Layer and Transport Layer Security, Secure Electronic Transaction. Intruders - Intruders, Intruder Detection, Password Management, Firewall - Firewall Design Principles, Trusted Systems. (5)

Text Book:

1. Cryptography and Network security Principles and Practices – Williams Stallings (Pearson Education).

Reference Books:

1. Cryptography and network security – Atul Kahate (TMGH).
2. Cryptography and security – Shyalama (Wiley India).
3. Information Systems Security - Nina Godbole (Wiley India).
4. Cryptography & Network Security-Forouzan (Tata McGraw-Hill Education).

Term work: It should consist of 10-12 assignments based on exercise problems given in the text book and should include study of the following.

1. To study the Viruses, Threads and Advanced Block Cipher Encryption Techniques.
2. To study and analysis of security tools like OpenPuff security Tool, CloudSecurity Readiness Tool, Kismet, John the Ripper.