December 26, 2013

CSHT-615 – Information Security

Sr. No.	Topic	Chapter	Reference	Duration (hours)
1	**Introduction:** Security, Attacks, Computer Criminals, Security Services, Security Mechanisms.	[1] 1.1, 1.2, 1.3, 1.4 [2] 1.3 - 1.5	1 2	8
2	**Cryptography**: Substitution ciphers, Transpositions Cipher, Confusion, diffusion, Symmetric, Asymmetric Encryption.DES Modes of DES.,Uses of Encryption.,Hash function,key exchange, digital signatures,Digital Certificates.	2.1, 2.2, 2.3, 2.5, 2.9	1	16
3	**Program Security**: Secure programs,Non malicious Program errors, Malicious codes virus,trap doors,salami attacks, covert channels,Control against program	3.1, 3.2, 3.3, 3.4 [pg. 163 – 169 Trojans, trap doors, Salami attacks], [pg. 174 – 183 Covert channels], 3.5	1	8
4	**Threats.Protection in OS**: Memory and Address Protection, Access control, File Protection, User Authentication.	4.1, 4.2, 4.3, 4.4, 4.5	1	6
5	**Database Security**: Requirements, Reliability, Integrity, Sensitive data, Inference, Multilevel Security.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7	1	8

6	**Security in Networks**: Threats in Networks and Network security Controls, firewalls, Intrusion detection systems, Secure e-mails	7.1, 7.2, 7.3, 7.4, 7.5, 7.6	1	6
7	**Administrating Security**: Security Planning, Risk Analysis, Organizational Security Policy, PhysicalSecurity. Ethical issues in Security: Protecting Programs and data. Information and law.	8.1, 8.2, 8.3, 8.4 11.1, 11.2, 11.6	1	8

References

[1] Charles P Pfleeger, S.L. Pfleeger, **Security in Computing,** 4th Edition {Pearson}

[2] William Stallings, **Network Security Essentials Applications and Standards,** 4th Edition {Pearson}

CSHP-614 – Software Lab based on CSHT-615

Implement the following encryption and decryption techniques

1) Caesar Cipher
2) Columnar Transposition Cipher
3) Vernam Cipher
4) Vigenere Cipher
5) Additive & Multiplicative Ciphers
6) Mono alphabetic Cipher
7) Poly alphabetic Cipher
8) Stream Cipher using XOR
9) Hash function
10) Simple DES

Study of security of OS, DBMS and firewall installed in your college to be covered as part of internal assessment.