

Security Of Information Systems/ Internet Security (IT-8002)

Course Code	IT-8002	Credits-4	L – 3, T- 1, P-0
Name of the Course	Security Of Information Systems/ Internet Security		
Lectures to be Delivered	52 (1 Hr Each) (L= 39, T = 13 for each semester)		
Semester End Examination	<i>Max. Marks: 100</i>	<i>Min. Pass Marks: 40</i>	Maximum Time:3hrs
Continuous Assessment (based on sessional tests (2) 50%, Tutorials/Assignments 30%, Quiz/Seminar 10%, Attendance 10%)	<i>Max. Marks: 50</i>		

Instructions

- For Paper Setters:** The question paper will consist of five sections A, B, C, D, and E. Section E will be Compulsory, it will consist of a single question with 10-20 subparts of short answer type, which will cover the entire syllabus and will carry 40% of the total marks of the semester end examination for the course. Section A, B, C and D will have two questions from the respective sections of the syllabus and each section will carry 15% of the total marks of the semester end examination for the course.
- For Candidates:** Candidates are required to attempt five questions in all selecting one question from each of the sections A, B, C and D of the question paper and all the subparts of the questions in section E.. Use of non-programmable calculators is allowed.

Section A

Basic Encryption and Decryption: Terminology and Background: Encryption, Decryption and Cryptosystems, Plain Text and Cipher Text, Encryption algorithms, Cryptanalysis.
 Introduction to Ciphers: Monoalphabetic Substitutions such as the Caesar Cipher, Cryptanalysis of Monoalphabetic ciphers, Polyalphabetic Ciphers such as Vigenere Tableaux, Cryptanalysis of Polyalphabetic Ciphers, Perfect Substitution Cipher such as the Vernam Cipher, Stream and Block Ciphers, Characteristics of 'Good' Ciphers: Shannon Characteristics, Confusion and Diffusion, Information Theoretic Tests, Unicity Distance.

Section – B

Secure Encryption systems: Hard Problems: Complexity: NP – Complete problems, Characteristics of NP-Complete Problems, The Meaning of NP- Completeness and Cryptography.
 Properties of Arithmetic Operations: Inverses, Primes, Greatest Common Divisor, Euclidean algorithm, Modular Arithmetic, Properties of Modular Arithmetic, Computing the inverse, Fermat's Theorem, algorithm for computing inverses, Random number generation
 Public Key (Asymmetric key) Encryption Systems: Concept and Characteristics of Public Key Encryption system, Introduction to Merkle-Hellman Knapsacks, rivest – Shamir-Adlman (RSA) Encryption in Detail, introduction to Digital Signature Algorithms, The Digital Signature Standard (DSA).
 Hash Algorithms: Hash concept, description of Hash Algorithms, Message Digest Algorithms such as MD4 and MD5, Secure Hash Algorithms such as SH1 and SHA2.

Section – C

Secure Secret Key (Symmetric) Systems: The Data encryption Standard (DES), Analyzing and Strengthening of DES, Key Escrow and Clipper, Introduction to Advance Encryption Standard (AES)
 Applied Cryptography, protocols and Practice: Key Management protocols: Solving Key Distribution Problem, Diffie-Hellman Algorithm, Key Exchange with Public Key Cryptography.
 Public Key Infrastructure (PKI): Concept of digital Certificate, Certificate Authorities and it's roles, X509 Structure of Digital Certificate, Types of public Key Infrastructures. Legal Issues: Copyrights, Patents, Trade Secrets, Computer Crime, Cryptography and the Law.
 Operating System, Database and program Security;

Section – D

Operating Systems security: Security policies, Models of Security, Security Features of Ordinary Operating System, Security Features of Trusted Operating System.
 Database Security; Security Requirements of Databases, reliability and integrity, Protection of Sensitive Data, Inference problem: direct and Indirect Attacks
 Program Security: Kinds of Malicious Code, How viruses Attach and Gan Control, Homes for Viruses, Virus

signatures, Preventing Virus Infection, Trapdoors, Convert channels, Control Against program Threats, Java Mobile codes.

Network Security

Network Security Issues such as Impersonation, Message Confidentiality, Message Integrity, Code Integrity, Denial of Service, Secure Communication Mechanism such as IPSec, PKI based Authentication and Kerberos Authentication , biometrics Authentication Mechanisms, Access Control Mechanisms Firewalls

Web Security: Solving privacy problems, Solving Authentication problems, secure socket Layer (SSL) protocol, Secure Electronic Transaction (SET) Protocol, Safe Guarding Web Servers.

Secure Electronic Mail: Privacy Enhanced Email (PEM), Pretty Good Privacy (PGP), Public Key Cryptography Standards – PKCS#7, Secure/ Multipurpose Internet Mail extensions (S/MIME)

Books:

1. "Security in Computing (Second Edition)", Charles P. Pfleeger, 1996, Prentice Hall International, Inc.
2. "Applied Cryptography protocols, Algorithms, and Source Code in C (Second edition)", Bruce Schneier, 1995, John Wiley & Sons. Inc.
3. "Security Technologies for the world wide web", Rolf Oppliger, Artech House, Inc.
4. "Digital Certificates Applied Internet Security", Jalal Feghhi, Jalli Feghhi and Peter Williams, Addison Wesley Longman, Inc.
5. "The World Wide Web Security FAQ", Lincoln D. Stein, world Wide Web Consortium, [online] Available at <http://www/w3.org/Security/Faq/www-security-faq.html>
6. Cryptographic Message Syntax Standard, public Key Cryptography Standard, RSA Laboratories, [online] Available at <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html>