PARUL UNIVERSITY - Faculty of Engineering and Technology

Department of Computer Science & Engineering

SYLLABUS FOR 6th Sem BTech PROGRAMME

Information Security (203108381)

Type of Course: BTech

Prerequisite:

Rationale:

Teaching and Examination Scheme:

Teaching Scheme			Credit	Examination Scheme					Total
				External		Internal			
Lect Hrs/	Tut Hrs/	Lab Hrs/		T	P	T	CE	P	
3	0	0	3	60	-	20	20	-	100

Lect - Lecture, **Tut** - Tutorial, **Lab** - Lab, **T** - Theory, **P** - Practical, **CE** - CE, **T** - Theory, **P** - Practical

Contents:

Sr.	Topic	Weightage	Teaching Hrs.
1	**Introduction**: Computer Security Concept, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanism, A Model for Network Security	5%	3
2	**Classical Encryption Techniques**: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Steganography	10%	6
3	**Block Ciphers and the Data Encryption Standard**: Block Cipher Principles, Data Encryption Standard (DES), Deferential and Linear Cryptanalysis, Block Cipher Design Principles, Block Cipher Operation, RC4	15%	8
4	**Number theory and Advance Encryption Standard**: The Euclidean Algorithm, Modular Arithmetic, Groups, Rings, and Fields, Finite Fields of the Form GF(p), Polynomial Arithmetic, Advance Encryption Standard(AES): structure, key expansion	15%	8

5	**Asymmetric Ciphers**: Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality Principles of Public-Key Cryptosystems, The RSA Algorithm, DiffieHellman Key Exchange	15%	6
6	**Cryptographic Data Integrity Algorithms**: Hash Function: Hash Function and its Application, Security Requirements for Cryptographic Hash Functions, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA), Message Authentication code: Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs, HMAC, Digital Signature: Introduction to Digital Signatures, Digital Signature Standard	15%	8
7	**Key Management and Distribution**: Symmetric Key Distribution: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Asymmetric Key Distribution: Distribution of Public Keys, X.509 certificates. Pseudorandom numbers: Principles of Pseudorandom Number Generation, Pseudorandom Number Generators, Pseudorandom Number Generation Using a Block Cipher	15%	6
8	**User Authentication**: Remote User-Authentication Principles, Remote User-Authentication Using Symmetric Encryption, Kerberos, Remote User-Authentication Using Asymmetric Encryption	10%	4

***Continuous Evaluation:**

It consists of Assignments/Seminars/Presentations/Quizzes/Surprise Tests (Summative/MCQ) etc.

Reference Books:

1. Cryptography and Network Security
   William Stallings; Pearson Education
2. Cryptography & Network Security
   Behrouz A. Forouzan; Tata McGraw-Hill
3. Information Security Principles and Practice
   Deven Shah,; Wiley-India
4. Information Security Principles and Practice
   Mark Stamp; Wiley IndiaEdition