Marwadi University

Syllabus for Bachelor of Technology

Computer Engineering

Subject Code: 01CE0603

Subject Name: Computer Security

B.Tech. Year - III

Objective: This course is to provide students with a knowledge of the Computer Security with different models and practical .aspects of securing information on computer through various cryptography approach

Credits Earned: 05

Course Outcomes: After completion of this course, students will be able to

- Apply the ideas of classical cryptosystems and public key cryptosystems techniques. (Apply)
- Analyze different cryptographic protocols. (Analyze).
- Test Different Digital Signature Schemes and Digital Certificates mechanisms and its requirement. (analyze)
- Analyze different security models. (Analyze)
- Apply methods for authentication, access control, intrusion detection and prevention. (Apply)

Pre-requisite of course: NA.

Teaching and Examination Scheme

Teaching Scheme (Hours)			Credits	Theory Marks			Tutorial/ Practical Marks		Total Marks
Theory	Tutorial	Practical		ESE (E)	Mid Sem (M)	Internal (I)	Viva (V)	Term work (TW)	
4	0	2	5	50	30	20	25	25	150

Contents:

Unit	Topics	Contact Hours
1	▪ Introduction: Fundamentals of computer security ▪ Computer security keywords: Goals, Threats, Vulnerabilities ▪ Ethical aspects ▪ Organizational details	8

2	**Cryptography Fundamentals : I** ▪ Symmetric-key cryptography: Models and attack types, Kerchoff's Principle ▪ Block ciphers ▪ AES and DES	8
3	**Cryptography Fundamentals : II** ▪ Modes of operations ▪ Integrity ▪ MAC and Hash Functions, Cryptographic Hash Functions ▪ Authenticated encryption	8
4	**Cryptography Fundamentals : III** ▪ Padding oracle attacks ▪ Modular arithmetic ▪ RSA Encryption Algorithm	8
5	**Cryptography Fundamentals : IV** ▪ Factoring Attacks ▪ Digital signatures ▪ Certificates and public-key infrastructures ▪ TLS/SSL discussion	8
6	**Crypto Passwords and authentication** ▪ Crypto pitfalls: Random-number generation and side channels ▪ Authentication and Passwords ▪ Password hashing	8
7	**Security Models** ▪ Browser security model: The browser as an OS and execution platform , Protocols, isolation, communication. ▪ Web application security: Application pitfalls and defences ▪ Session management and user authentication: How users authenticate to web sites, Browser-server mechanisms for managing state ▪ HTTPS: goals and pitfalls: Network issues and browser protocol handling	8
	Total Hours	**56**

References:

1. Cryptography And Network Security Principles And Practice Fourth Edition, William Stallings, Pearson Education.
2. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall PTR
3. Cryptography: Theory and Practice by Douglas R. Stinson, CRC press
4. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 2002

Suggested Theory distribution:

The suggested theory distribution as per Bloom's taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery and evaluation					
Remember	Understand	Apply	Analyse	Evaluate	Create
10%	20%	30%	30%	5%	5%

Suggested List of Experiments:

1. Study and write a program for any Classical Ciphers technique
2. Implement polyalphabetic Cipher
3. W.A.P. to implement Rail fence technique
4. Implement AES Algorithm
5. Implement DES Algorithm
6. Implement RSA Algorithm
7. Implement any one of the variant of SHA.
8. Design Digital signature for Any given document.

Note: Any Programming language can be used to implement above cryptographic algorithm. Also Perform above experiment using Virtual labs (http://cse29-iiith.virtual-labs.ac.in/exp8/index.php)

Open Ended Problems:

1. Study of Hardware firewall and analyse its various security rules.
2. Implement security mechanism with the help of CISCO security tools.