Program: Third Year B.Tech. in Computer Engineering	**Semester : VI**
Course : Information Security	**Course Code: DJ19CEC603**
Course : Information Security Laboratory	**Course Code: DJ19CEL603**

<table>
<tr><th colspan="4" rowspan="2">Teaching Scheme
(Hours / week)</th><th colspan="7">Evaluation Scheme</th></tr>
<tr><th colspan="3">Semester End Examination Marks (A)</th><th colspan="3">Continuous Assessment Marks (B)</th><th rowspan="2">Total
marks
(A+ B)</th></tr>
<tr><th rowspan="2">Lectures</th><th rowspan="2">Practical</th><th rowspan="2">Tutorial</th><th rowspan="2">Total Credits</th><th colspan="3">Theory</th><th>Term Test 1</th><th>Term Test 2</th><th>Avg.</th></tr>
<tr><td colspan="3">75</td><td>25</td><td>25</td><td>25</td><td>100</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">2</td><td rowspan="3">-</td><td rowspan="3">4</td><th colspan="3">Laboratory Examination</th><th colspan="2">Term work</th><th rowspan="2">Total Term work</th><td rowspan="3">50</td></tr>
<tr><th>Oral</th><th>Practical</th><th>Oral &Practical</th><th>Laboratory Work</th><th>Tutorial / Mini project / presentation/ Journal</th></tr>
<tr><td>-</td><td>-</td><td>25</td><td>15</td><td>10</td><td>25</td></tr>
</table>

Pre-requisite: Knowledge of Programming Basics and Computer Network.

Objectives:

1. To introduce classical encryption techniques and concepts of modular arithmetic and number theory.
2. To explore the working principles and utilities of symmetric cryptographic algorithms.
3. To distinguish symmetric and asymmetric cryptography and explore the working principles and utilities of asymmetric cryptographic algorithms.
4. To understand data integrity and explore the design issues and working principles of various authentication protocols, PKI standards and various secure communication standards
5. To understand network and system attacks and develop utility programs for secure communication.
6. To explore Software vulnerability and develop and apply preventive measures.

Outcomes: On completion of the course, learner will be able to:

1. Understand system security goals and concepts, classical encryption techniques and acquire fundamental knowledge on the concepts of modular arithmetic and number theory.
2. Understand, compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication
3. Apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.
4. Apply different digital signature algorithms to achieve authentication and design secure applications
5. Understand network security basics, analyze different attacks on networks and systems.
6. Understand Software vulnerability and Apply preventive measures.

Detailed Syllabus: (unit wise)

Unit	Description	Duration
1	**Introduction and Number Theory** Services, Mechanisms and attacks-the OSI security architecture-Network security model classical Encryption techniques (Symmetric cipher models, substitution techniques, transposition Techniques), Number theory Groups, Rings, Fields-Modular arithmetic-Euclid's algorithm-Finite fields-Polynomial Arithmetic –Prime numbers-Fermat's and Euler's theorem, Chinese Remainder theorem.	07
2	**Symmetric Cryptography:** Block cipher principles block cipher modes of operation, Simplified Data Encryption Standard (DES), DES, Double DES, Triple DES, Simplified Advanced Encryption Standard (S-AES), AES- Blowfish, IDEA.	07
3	**Asymmetric Cryptography:** Symmetric vs. Asymmetric Cryptography, Principles of public key cryptosystems, and Essential Number Theory for Public-Key Algorithm: Euclidean algorithm, Extended Euclidean Algorithm, Euiler's Phi Function, Fermat's Little Theorem and Euiler's Theorem. The RSA algorithm, Key management, Diffie Hellman Key exchange, Elliptic curve arithmetic, Elliptic curve cryptography.	08
4	**Integrity, Authentication and Digital Certificates:** Cryptographic hash functions, Properties of secure hash function, MD5, SHA-1, MAC, HMAC, CMAC. User Authentication and Entity Authentication, One-way and mutual authentication schemes, Needham Schroeder Authentication protocol, Kerberos Authentication protocol. RSA Signature Schemes, Elgamal Digital Signatures, Digital Signature Algorithm. Digital Certificate: X.509, PKI.	07
5	**Network Security:** Network security basics: TCP/IP vulnerabilities (Layer wise), Packet Sniffing, ARP spoofing, port scanning, IP spoofing, TCP syn flood, DNS Spoofing. Denial of Service: Classic DOS attacks, Source Address spoofing, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service, Defenses against Denial-of-Service Attacks. Internet Security Protocols: SSL, IPSEC, Secure Email: PGP, Firewalls, IDS and types, Honey pots, Case Study on Network Security.	08

6	**Software Security** Software Vulnerabilities: Buffer Overflow, Salami Attack, Format string, cross-site scripting, SQL injection, Malware: Viruses, Worms, Trojans, Logic Bomb, Bots, Rootkits Introduction to Secured Software Development Life Cycle. , Case Study on Software Security.	05

Books Recommended:

Text books:

1. William Stallings, Cryptography and Network Security, Principles and Practice, 7thEdition, Pearson Education, June 2017.
2. Behrouz A. Ferouzan, **—**Cryptography & Network Security, Tata Mc Graw Hill, 2007

Reference Books:

1. Applied Cryptography, Protocols Algorithms and Source Code in C, Bruce Schneier, Wiley.
2. Charles Pfleeger, Shari Lawrence Pfleeger & Jonathan Margulies, Security in Computing, 5th Edition, Prentice Hall
3. Secured Development Life Cycle by Michael Howard, Steve Lipner , Microsoft Press.

List of Laboratory Experiments: (Any Seven)

Sr. No.	Title of the Experiment
1	Design and Implement Caesar cipher cryptographic algorithm by considering letter [A..Z] and digits [0..9]. Apply Brute Force Attack to reveal secret.
2	Design and Implement Encryption and Decryption algorithm using Simple Columnar Transposition cipher technique. Study how dictionary attack can be applied on it.
3	Design and Implement your “own” cipher combining “Substitution” and “Transposition” techniques.
4	Implement RSA Cryptosystem using RSA Algorithm / Implement Elliptical Curve Digital Signature Algorithm (ECDSA).
5	Demonstrate the data integrity using various cryptographic algorithms viz. MD-5, SHA-1 using VLAB, IIT Bombay.
6	Implement registration webpage asking for information along with the password (Strong enough). Store the password in database in encrypted form after adding few salt characters in the password. Verify the strength of password and perform analyses using various attack.

7	Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.
8	Study of packet sniffer tools wireshark, : Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode. Explore how the packets can be traced based on different filters.
9	Implementation of Network Intrusion Detection System using SNORT and IPTABLE
10	Implement DOS Attack using HPing, Hping3 and other tools.
11	Implement Buffer Overflow Attack using Ollydbg, Splint, Cppcheck

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper based on the entire syllabus will comprise of 5 questions (All compulsory, but with internal choice as appropriate), each carrying 15 marks, total summing up to 75 marks.
2. Total duration allotted for writing the paper is 3 hrs.

Laboratory:

1. Oral and practical examination will be based on the entire syllabus including, the practicals performed during laboratory sessions.

Continuous Assessment (B):

Theory:

1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or an assignment on live problems or a course project.
2. Total duration allotted for writing each of the paper is 1 hr.
3. Average of the marks scored in both the two tests will be considered for final grading.

Laboratory: (Term work)

Term work shall consist of minimum 7 experiments, 1 Power Point Presentation and minimum 2 assignments.

The distribution of marks for term work shall be as follows:

i. Laboratory work (Performance of Experiments): 15 Marks
ii. Journal Documentation (Write-up, Power Point Presentation and Assignments: 10 marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work and upon fulfilling minimum passing criteria in the term work.

Prepared by   Checked by   Head of the Department   Principal