INFORMATION AND NETWORK SECURITY (Minor Elective – I)

Semester I (Computer Engineering)

SUB CODE: MECE105-A

Teaching Scheme (Credits and Hours)

Teaching scheme				Total	Evaluation Scheme					
L	**T**	**P**	**Total**	**Credit**	**Theory**		**Mid Sem Exam**	**CIA**	**Pract.**	**Total**
Hrs	**Hrs**	**Hrs**	**Hrs**		**Hrs**	**Marks**	**Marks**	**Marks**	**Marks**	**Marks**
03	**00**	**02**	**05**	**04**	**3**	**70**	**30**	**20**	**30**	**150**

LEARNING OBJECTIVES:

The educational Objectives of this Course are:

- Understand information security’s importance in our increasingly computer-driven world.
- Master the key concepts of Information and Network security and how they “work.”
- Develop a “security mindset:” learn how to critically analyze situations of computer and network usage from a security perspective, identifying the salient issues, viewpoints, and trade-offs.

OUTLINE OF THE COURSE:

Unit No	**Topics**
1	Introduction
2	Mathematical Foundation
3	Symmetric Key Cryptography
4	Asymmetric Key Cryptography
5	Message Digest and Hash Functions
6	Authentication Mechanisms
7	System and Network Security

Total hours (Theory): 45

Total hours (Tutorial): 30

Total hours: 75

DETAILED SYLLABUS:

Sr. No	Topic	Lecture Hours	Weight age
1	**Introduction** Security Goals, Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security, Internet Standards and RFCs	03	10
2	**Mathematical Foundation** Groups and subgroups, rings, finite fields, Galois Fields, Primitive root, Polynomial arithmetic, Quadratic residues, discrete logarithms, elliptic curve arithmetic. Divisibility, gcd, prime numbers, fundamental theorem of arithmetic, congruences, Fermat's theorem, Euler function, primality testing, solution of congruences, Chinese remainder theorem. Secret sharing and splitting	07	20
3	**Symmetric Key Cryptography** Classical Substitution and Transposition Techniques, DES, Triple DES, AES, RC4, modes of operation.	05	10
4	**Asymmetric Key Cryptography** RSA cryptosystem, Diffie-Hellman, elliptic curve cryptography, ElGamal, Digital Signature.	07	15
5	**Message Digest and Hash Functions** Message authentication, Secure Hash Functions, MD5, SHA	05	10
6	**Authentication Mechanisms** Public-Key Infrastructure (PKI), Authentication: Classifications, Mutual authentication Algorithms, Kerberos	07	15
7	**System and Network Security** Buffer overflow, format string vulnerabilities, SQL Injection, TCP session hijacking, ARP attacks, route table modification. IPsec, Secure Socket Layer (SSL), E-mail Security, S/MIME, PGP, Firewalls, Auditing and Intrusion Detection System.	11	20

INSTRUCTIONAL METHOD AND PEDAGOGY (Continuous Internal Assessment (CIA) Scheme)

- At the start of course, the course delivery pattern, prerequisite of the subject will be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, OHP etc.
- Attendance is compulsory in lecture and tutorial which carries 10 marks in overall evaluation.
- Two internal exams will be conducted and average of the same will be converted to equivalent of 30 Marks as a part of internal theory evaluation.
- Assignments based on the course content will be given to the students for each unit and will be evaluated at regular interval evaluation.

- Surprise tests/Quizzes/Seminar/tutorial will be conducted having a share of 15 marks in the overall internal evaluation.
- The course includes tutorials, where students have an opportunity to revise the concepts being taught in lectures.

STUDENTS LEARNING OUTCOMES:

On successful completion of the course, the student will:

- The course shall give students a basic foundation for assessing security solutions required for particular applications, for making informed technology choices about security in Systems and Network, and for assess information security risks.
- The Students can help the organization to continue its commercial activities in the event of significant information security incidents.
- Students can establish responsibility and accountability for information security in organizations.
- To be proficient in various forensic tools and usage of tools for disk imaging and recovery processes.
- The students will be able to design security procedures and policies.
- They can be well versed in various security standards and security testing techniques.

STUDY MATERIAL:

Text Books:

1. Cryptography and Network Security Principals and Practices, by William Stalling, Pearson Education
2. Network Security, 2nd edition by Charlie Kaufman, Radia Perlman, Mike Speciner

Reference Books and Materials:

1. Cryptography & Network Security, by Behrouz A. Forouzan, Tata McGraw Hill.
2. Introduction to Cryptography with Coding Theory, 2nd edition by Wade Trappe and Lawrence C. Washington
3. Aleph One. "Smashing the Stack for Fun and Profit." *Phrack Magazine7*, 49 (1996): File 14 of 16. http://www.phrack.org/archives/49/P49-14.
4. Jason Deckard, " Defeating Overflow Attacks", as part of *SANS Institute InfoSec Reading Room*
5. Tim Newsham, "Format String Attacks", *Guardent Inc.*, September 2000
6. Steve Friedl , "SQL Injection Attacks by Example", Unixwiz.net.
7. Nikita Borisov UC Berkeley, Ian Goldberg Zero-Knowledge Systems and David Wagner UC Berkeley, "Intercepting Mobile Communications: The Insecurity of 802.11", Proceedings of the 7th annual international conference on Mobile computing and networking, MobiCom '01 Pages 180 - 189

- Other reference material will be provided by respective faculty member if it is needed.

LIST OF PRACTICALS:

Sr. No	Name of Experiment
1	Implementation of Affine Cipher
2	Implementation of Hill Cipher
3	Implementation of Playfair Cipher
4	Implementation of Vigener Cipher.
5	Implementation of Rail fence Technique
6	Implementation of double columner transposition technique
7	Implementation of Advanced Columnar Transposition technique.
8	Implementation of SDES
9	Implementation of SDES with CBC Mode
10	Implementation of MAC or HashFunction (One Algorithm per student)
11	Study of snort (IDS)
12	Study of A Security Tool (One tool per student)