# Kadi Sarva Vishwavidyalaya

Faculty of Engineering and Technology

**First Year Master of Engineering (Computer Engineering)**

In Effect from Academic Year 2017-18

| Subject Code: MECE106-N-B | Subject Title: INFORMATION & NETWORK SECURITY |
|---|---|

| Teaching scheme | | | | Total Credit | Evaluation Scheme | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| L | T | P | Total | | Theory | | Mid Sem Exam | CIA | Pract. | Total |
| Hrs | Hrs | Hrs | Hrs | | Hrs | Marks | Marks | Marks | Marks | Marks |
| 04 | 00 | 02 | 06 | 05 | 03 | 70 | 30 | 20 | 30 | 150 |

**LEARNING OBJECTIVES:**

This course will provide students with a practical and theoretical knowledge of information and network security. By the end of the course, students should be able to:

- State the basic concepts in information security, including security policies, security models, and various security mechanisms.
- Explain concepts related to applied cryptography, including plaintext, ciphertext, symmetric cryptography, asymmetric cryptography, and digital signatures.
- State the requirements and mechanisms for identification and authentication.
- List network and distributed systems security issues and solutions, including authentication and network security protocols.
- Explain the network access control mechanisms, including the basic concepts of firewalls, packet filters, application gateways, and typical firewall configurations
- Explain SSL/TLS protocols.
- State program security issues, including virus, worm, and logical bombs.

**Outline of the Course:**

| Sr. No. | Title of the Unit | Minimum Hours |
|---|---|---|
| 1 | Introduction to Security Essentials | 07 |
| 2 | Concepts of Cryptography : Symmetric and Asymmetric Key Cryptography | 13 |
| 3 | Authentication and Digital Signature, Digital Certificate | 10 |
| 4 | Network Security Protocols : SSL/TLS, IPSec | 13 |
| 5 | Firewall and IDS | 13 |
| 6 | Virus and Malicious Programs | 08 |

**Total hours (Theory): 64**
**Total hours (Lab): 32**
**Total hours: 96**

# Kadi Sarva Vishwavidyalaya

Faculty of Engineering and Technology

**First Year Master of Engineering (Computer Engineering)**

In Effect from Academic Year 2017-18

**Detailed Syllabus:**

| Sr. No. | Topic | Lecture Hours | Weight age(%) |
|---|---|---|---|
| **1** | Introduction to Information Security : Security Attacks, Services and Mechanisms, Dimensions of Cryptography. | **7** | **11** |
| **2** | Block Cipher Design Principles, DES, 2DES,3DES, AES, Euclidean and Extended Euclidean Algorithms, Euler's Phi Function, Euler and Fermat's Theorem, RSA | **13** | **20** |
| **3** | Authentication using Symmetric and Asymmetric algorithm, Digital Signature using Elgamal Algorithm, Properties of secure Hash functions, Digital certificates & Certificate authorities | **10** | **16** |
| **4** | SSL architecture, SSL record, alert and handshake protocol, TLS an extension to SSL, TLS Architecture, TLS Record and Handshake protocol, Attacks against TLS/SSL, Differences between TLS and SSL, IPSec Protocol | **13** | **20** |
| **5** | Introduction to Firewalls, Network layer Firewalls, Application layer Firewalls, Proxy Firewalls, Intrusion Detection, Classifications of IDS, Detection methods, Host based intrusion detection systems, Network based intrusion detection systems, IDS Signatures, Anomaly detection, Intrusion Prevention, Classification and Detection methods, Tools for packet analysis and intrusion detection: Wireshark, Snort. | **13** | **20** |
| **6** | Viruses and Malicious Programs, Types of Virus, Taxonomy of Malicious Programs, Bacteria, Worm, Ad ware/Spy ware, Trojan Horse, Logic Bomb, Trap Door, Easter Egg, Virus Phases, Virus Protection, Virus Structure, Advanced Anti-Virus Techniques | **8** | **13** |
| | **Total** | **64** | **100** |

**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 laboratory which carries 10 marks in overall evaluation.
- One internal exam will be conducted 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 five marks in the overall internal evaluation.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
- Experiments shall be performed in the laboratory related to course contents.

**LEARNING OUTCOME:**

On successful completion of the course, the student will:

- understand the common threats faced today,
- understand the foundational theory behind information security,

- learn about the basic principles and techniques for designing a secure system,
- learn to think adversarially.
- become aware about how today's attacks and defenses work in practice and how to assess threats for their significance, and how to gauge the protections and limitations provided by today's technology.

**Reference Books:**

1. "Cryptography and Network Security Principles and Practice", Fourth Edition, by William Stallings, Pearson Education
2. Network Security Essentials: Applications and Standards, by William Stallings. Prentice Hall
3. "Network Security Bible", by Eric Cole, Dr. R. Krutz and J.W.Conley, Wiley Publications
4. "Intrusion Detection & Prevention", by Carl Endorf, Eugene Schultz, Jim Mellander, Jack Kozio, Mcgraw Hill publication
5. "The Transport Layer Security (TLS) Protocol, Version 1.2", T. Dierks, E. Rescorla (August 2008).
6. "SSL: Intercepted today, decrypted tomorrow", Netcraft, 2013-06-25
7. "The Secure Sockets Layer (SSL) Protocol Version 3.0", A. Freier, P. Karlton, P. Kocher (August 2011).
8. "SSL/TLS in Detail". Microsoft TechNet. Updated July 31, 2003.

**LIST OF EXPERIMENTS:**

| Sr. No. | Name of Practical |
|---|---|
| **1** | Implement SDES |
| **2** | Implement RSA |
| **3** | Implement a MAC algorithm. |
| **4** | Study of TLS with SMTP |
| **5** | Study of Windows Firewall/ Firewall simulation tool |
| **6** | Study of snort IDS |
| **7** | Study of Wireshark |