Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Third Year Bachelor of Engineering (Information Technology)

(In Effect From Academic Year 2019-20)

Subject Code: IT602-N	**Subject Title:** Information Security
Pre-requisite	

Teaching Scheme (Credits and Hours)

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
03	00	02	05	04	03	70	30	20	30	150

The course is intended to familiarize the student to the domain of information and network security. After introducing the basics of cryptography and security along with the essential mathematical background, the course aims to elaborate the understanding of various cryptographic primitives such as symmetric/asymmetric key encryption, hash, MAC, key management, digital signature etc. Together with the various attacks, the course also includes few modern security protocols. At the end, the course concludes with brief introduction about latest and forthcoming trends in the sphere of security.

Course Objective: This course aims to

- To learn the fundamentals of Information Security.
- To prepare students with the technical knowledge and skills needed to provide security in Networks/Network applications.
- To make the students aware regarding the different issues in security breaches.

Outline of the Course:

Sr. No	Title of the Unit	Minimum Hours
1	Introduction	5
2	Conventional Cryptography	5
3	Network Security	7
4	Security Protocols	7
5	Mathematical Background	6
6	Symmetric and Asymmetric Cryptographic Techniques	10
7	Authentication Techniques	8

Total hours (Theory): 48
Total hours (Lab): 32
Total hours: 80

Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Third Year Bachelor of Engineering (Information Technology)

(In Effect From Academic Year 2019-20)

Detailed Syllabus

No	Topic	Lecture (Hrs)	Weightage (%)
1	Introduction to Information Security : Attacks, Vulnerability, Security Goals, Security Services and mechanisms	5	9
2	Conventional Cryptography : Conventional substitution and transposition ciphers, one time pad, steganography	5	9
3	Network Security: Network Security issues, Different types of Network layer attacks, IP spoofing, Common Threats, Intruders, Viruses, Worms, Firewall, IDS	7	15
4	Security Protocols: Protocol Building Blocks ,Basic Protocols , Intermediate Protocols, Advanced Protocols, Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity - Blind Signatures	7	14
5	Mathematical background: Number Theory, Modular Arithmetic, Euclidean and Extended Euclidean algorithm, Prime numbers, Fermat and Euler's Theorem.	6	14
6	Symmetric and Asymmetric Cryptographic Techniques : DES, AES, RSA algorithms	10	22
7	Authentication Techniques: Authentication Requirement, Functions, Message Authentication Code, Hash Functions, Security Of Hash Functions And MACs, MD5-Message Digest Algorithm, SHA-Secure Hash Algorithm, Digital Signatures, Digital Signature Standard (DSS).	8	17
	Total	48	100

Instructional Method and Pedagogy:

- At the start of course, significance of the course, content delivery pattern, and other required details regarding subject will be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, smart boards etc.
- Attendance is compulsory in lecture and laboratory which will be reflected in Continuous Internal Assessment (CIA) component in the examination scheme of the course.
- Internal / Mid-semester examinations shall be conducted for theoretical evaluation.
- Assignments based on the course content will be given to the students and will be evaluated at regular interval 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 this course, the student should be able to:

- Describe the fundamental concepts of information system security.
- Understand the terms :security policy, host based security, firewall, and packet filtering and intrusion detection.
- Differentiate threats to information systems from attacks against information systems.

- Know the concepts of authentication and authorization, intrusion detection and information security techniques.

e-Resources:

- https://nptel.ac.in/courses/106105162/
- http://williamstallings.com/Cryptography/
- http://williamstallings.com/NetworkSecurity/
- https://www.coursera.org/learn/crypto

Reference Books:

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. Network Security Essentials: Applications and Standards, by William Stallings, Prentice Hall.
4. Information Security Principles and Practice By Mark Stamp, Willy India Edition
5. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGraw Hill
6. Cryptography: Theory and Practice by Douglas R. Stinson, CRC press.
7. Cryptography & Network Security, Atul Kahate, McGraw Hill
8. Cryptography & Network Security, V.K. Jain, Khanna Publishing House
9. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India

List of experiments:

No	Name of Experiment
1	To implement Caesar Cipher Encryption - Decryption
2	To implement Hill Cipher Encryption
3	To implement Poly-alphabetic Cipher (Vigener Cipher) Technique
4	To implement Play-Fair Cipher Technique.
5	Write a program to implement Rail-Fence Encryption Technique
6	To implement S-DES algorithm for data encryption.
7	Write a program to implement RSA asymmetric (public key and private key)-Encryption
8	Study of MD5 hash function and implement the hash code using MD5.
9	Study of SHA-1 hash function and implement the hash code using SHA-1.
10	Write a program to generate digital signature using Hash code.
11	Implement a code to simulate buffer overflow attack.