Academic Year 2018 - 19

Course name: - NETWORK SECURITY AND CRYPTOGRAPHY
Duration: - Throughout the semester
Venue: - VIVA Institute of Technology
Co-ordinator: - Prof. Vinit Raut
Enrolled students: - 57

Course Objective:-

1. To understand the foundations of cryptographic attacks.
2. To gain knowledge of encrypting data, and to choose between different algorithms.
3. Prepare students for research in the area of cryptography and enhance students communication and problem solving skills
4. To differentiate between the encryption techniques and know their suitability to an application.
5. To effectively apply their knowledge to the construction of secure cryptosystems.

Course Outcomes: -

After successful completion of the course, the students are able to

1. Understand the various types of cryptographic attacks and the mathematics behind cryptography.
2. Describe the various types of ciphers and hash functions.
3. Apply the different cryptographic techniques to solve real life problems.
4. Evaluate different techniques as to their suitability to various applications.
5. Develop a cryptosystem keeping in view social issues and societal impacts.

Course Schedule: -

Day 1: - Introduction to Cryptography and Block Ciphers

Session 1: Introduction to security attacks
introduction to cryptography
classical encryption techniques

Session 2: Modern Block Ciphers
Block ciphers principals
block cipher modes of operations

Day 2: - Confidentiality and Modular Arithmetic

Session 1: Confidentiality using conventional encryption
Introduction to graph

Session 2: Fermat's and Euler's theorem
Primality testing

Day 3: - Public key cryptography and Authentication requirements

Session 1: Principles of public key crypto systems
Introductory idea of Elliptic curve cryptography

Elgamel encryption

Session 2: Message Authentication and Hash Function
Authentication requirements
Security of hash functions and MACS

Day 4: - Integrity checks and Authentication algorithms

Session 1: Secure hash algorithm
Digital Signatures
Digital signature standards

Session 2: Authentication Applications
Directory authentication service

Day 5: - IP Security and System Security

Session 1: IP Security: Architecture
Encapsulating security payloads
key management

Session 2: Secure socket layer and transport layer security
firewall design principals

Report: -

Computer engg. department of VIVA Institute of Technology conducted a course on "NETWORK SECURITY AND CRYPTOGRAPHY" for Last year students. Total 57 students had been enrolled for this course.

This course was conducted by Prof. Vinit Raut in order to provide knowledge of Cryptography and Network Security. The course covers fundamental aspects of security in a modern networked environment with the focus on system design aspects and cryptography in the specific context of network / internetwork security

It also dwells into basics of cryptographic techniques, algorithms and protocols required to achieve these properties; computational issues in implementing cryptographic protocols and algorithms; and system/application design issues in building secure networked systems. Students enjoyed the course and completed it successfully.

CO-PO Mapping: -

Course Outcome	Program Outcome											
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO 9	PO1 0	PO1 1	PO1 2
CO 1	-	3	-	-	-	-	-	-	-	-	-	-
CO2	3	-	-	-	-	-	-	-	-	-	-	-
CO3	-	-	3	-	-	-	-	-	-	-	-	-
CO4	-	-	-	2	-	-	2	-	-	-	-	-
CO 5	-	-	-	-	-	3	-	-	-	-	-	-

Ashwini Save
HOD, Computer Engg.