JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name – Cryptography and Network Security

Session no.: 01

Session Name- Introduction to Security

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

- Review of previous Session- NIL

Topic to be discussed today- Today We will discuss about **– Introduction to security and Basic Concepts**

- Lesson deliverance (ICT, Diagrams & Live Example)-
  - ➢ Diagrams

Introduction & Brief Discussion about the Topic **– Introduction to security**

Introduction to Security

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit.

Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

Security Attacks, Services and Mechanisms

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Basic Concepts

Cryptography: The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

Plaintext: The original intelligible message

Cipher text: The transformed message

Cipher: An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Key: Some critical information used by the cipher, known only to the sender& receiver

Encipher (encode): The process of converting plaintext to cipher text using a cipher and a key

Decipher (decode): The process of converting cipher text back into plaintext using a cipher and a key

Cryptanalysis: The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking

Cryptology: Both cryptography and cryptanalysis

Code: An algorithm for transforming an intelligible message into an unintelligible one using a code-book

Reference-

1. **Book:** William Stallings, “Cryptography & Network Security”, Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. List the types of security?

Q2. What are security attacks, mechanisms and services?

Q3. What are the basic concepts in cryptography and network security?

Next, we will discuss about Cryptography.

- Academic Day ends with-

  National song ‘Vande Mataram’