An Introduction to Cryptographic Techniques

Modality: Self-Paced Learning

Duration: 1 Hour

SATV Value:

CLC:

NATU:

SUBSCRIPTION: Learn, Master

About this Course:

Cryptography is an essential tool for securing data and information in computer systems. The course is all about learning the inner functioning of cryptographic systems and the correct use of it in real-world applications. The course includes a detailed discussion about two parties communicating securely who have a shared secret key. It helps to protect when a powerful competitor spy and intrude into your business.

The course deals with the study of many deployed protocols along with the analysis of mistakes in existing systems. The course further surveys key techniques that allow two parties to create a shared secret key. Throughout the course, candidates will be able to learn many thrilling open problems in the field. We will work on fun programming projects which is optional. In the second course (Crypto II) we will study more advanced cryptographic tasks i.e. zero-knowledge, privacy mechanisms, and other forms of encryption.

Investigate the security of encrypted data

Is it possible to prove the security of encrypted data? In this course, you will be introduced to cryptography and cryptanalysis. From past examples of secret messages and the spies that cracked them to modern cryptographic applications, you will explore the base of data security. In this course, you will get a chance to try encrypting data yourself. You'll get an opportunity of completing a cryptography and cryptanalysis challenge..

Learn the five primary functions of cryptography:

There are five primary functions of cryptography today:

***Privacy/confidentiality*:** Make it sure that nobody can read the message except the intended recipient.

Authentication: The procedure of verification of one's identity.

***Integrity*:** Guarantee the recipient of the received message that it has not been changed and the same as the original.

***Non-repudiation*:** A process to confirm that the message was really sent by the sender and it’s not any fake sender.

***Key exchange*:** The method to share crypto keys between sender and recipient.

Goals and services of the course:

Goal:

The primary goal of cryptography is to protect information and data on the hard disk or a medium that may not be protected itself. The medium might be a computer network.

Services:

Cryptography can provide the following services:

Confidentiality (secrecy):

Assure that no other person can read the message except the intended recipient. Data is kept secure and a secret from improper credentials, even if the data passes through an insecure medium.

Integrity (anti-tampering):

Ensuring the recipient that the received message has not been changed and is same as the original.

Authentication:

Cryptography can aid in constructing an identity for verification, the procedure of proving one's identity. (Basic types of host-to-host authentication on the Internet today are name-based or address-based, and both of them are not well known.

Nonrepudiation:

A method to verify that the sender really sent that specific message.

What will you achieve?

At the end of the course, you'll be capable of:

- Describing the concepts used in early interchange and translation ciphers
- Applying cryptanalysis methods to simple ciphers
- Evaluating cryptographic techniques from a practical point of view
- Explaining the concepts of entropy, pseudo randomness, and unicity
- Indicating the use of hashing, salt, and nonces in many applications

Course Outline:

- Cryptography is an indispensable tool for protecting information in computer systems. we will cover more advanced cryptographic tasks such as zero-knowledge, privacy mechanisms, and other forms of encryption.