



# HINDUSTHAN INSTITUTE OF TECHNOLOGY



(An Autonomous Institution)

(Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai, Accredited with "A" Grade by NAAC and Accredited by NBA (Aero, CSE, ECE & Mech.)

Valley Campus, Pollachi Main Road, Coimbatore 641 032.

## Department of Computer Science and Engineering

### Innovative Teaching

Name :	Ms.R.Gnanakumari & Mr.Biju Balakrishnan
Subject code & Title:	20CS420 – Cryptography and Network Security
Academic year & Semester :	2023-2024 & VII

### Interactive Simulation - Virtual Lab (MHRD)

#### Objectives

1. To provide remote-access to simulation-based Labs in various disciplines of Science and Engineering.
2. To enthuse students to conduct experiments by arousing their curiosity. This would help them in learning basic and advanced concepts through remote experimentation.
3. To provide a complete Learning Management System around the Virtual Labs where the students/ teachers can avail the various tools for learning, including additional web-resources, video-lectures, animated demonstrations and self-evaluation.

### Cryptography Lab

#### Objectives

To keep the plaintext secret from eaves- droppers trying to get some information about the plaintext

#### Course Alignment

1. This laboratory is aligned with an introductory course on Cryptography

#### List of Experiments

1. Breaking the Shift Cipher
2. Breaking the Mono-alphabetic Substitution Cipher
3. One-Time Pad and Perfect Secrecy
4. Message Authentication Codes

5. Cryptographic Hash Functions and Applications
6. Symmetric Key Encryption Standards (DES)
7. Symmetric Key Encryption Standards (AES)
8. Diffie-Hellman Key Establishment
9. Public-Key Cryptosystems (PKCSv1.5)
10. Digital Signatures

The screenshot shows a web browser window with the URL `cse29-iiith.vlabs.ac.in`. The page header includes the Virtual Labs logo (An MoE Govt of India Initiative) and navigation links for HOME, PARTNERS, and CONTACT. The main content area is titled "Computer Science and Engineering" and features a sidebar with a table of contents: Introduction, Objective, List of experiments, Target Audience, Course Alignment, and Feedback. The main heading is "Cryptography", followed by a welcome message: "Welcome to the Cryptography lab. In this lab, we will do virtual experiments to understand the basic mathematical foundations of cryptography, to gain insightful experience by working with fundamental cryptographic applications and to train in the art of design and analysis of information security protocols." The footer is divided into three sections: "Community Links" (Sakshat Portal, Outreach Portal, FAQ: Virtual Labs), "Contact Us" (Phone: 011-26582050, Email: support@vlabs.ac.in), and "Follow Us" (social media icons for Twitter, Facebook, YouTube, and LinkedIn).

← → × cse29-iiith.vlabs.ac.in

Virtual Labs  
An MoE Govt of India Initiative

HOME PARTNERS CONTACT

## Computer Science and Engineering

**Introduction**

Objective

List of experiments

Target Audience

Course Alignment

Feedback

# Cryptography

Welcome to the Cryptography lab. In this lab, we will do virtual experiments to understand the basic mathematical foundations of cryptography, to gain insightful experience by working with fundamental cryptographic applications and to train in the art of design and analysis of information security protocols.

**Community Links**

Sakshat Portal  
Outreach Portal  
FAQ: Virtual Labs

**Contact Us**

Phone: General Information: 011-26582050  
Email: support@vlabs.ac.in

**Follow Us**

Twitter Facebook YouTube LinkedIn

← → ↻ cse29-iiith.vlabs.ac.in/List%20of%20experiments.html


HOME
PARTNERS
CONTACT

---

## Computer Science and Engineering

**Introduction**

**Objective**

**List of experiments**

**Target Audience**

**Course Alignment**

**Feedback**

# Cryptography

1. Breaking the Shift Cipher
2. Breaking the Mono-alphabetic Substitution Cipher
3. One-Time Pad and Perfect Secrecy
4. Message Authentication Codes
5. Cryptographic Hash Functions and Applications
6. Symmetric Key Encryption Standards (DES)
7. Symmetric Key Encryption Standards (AES)
8. Diffie-Hellman Key Establishment
9. Public-Key Cryptosystems (PKCSv1.5)
10. Digital Signatures

Community Links
Contact Us
Follow Us

← → ↻ cse29-iiith.vlabs.ac.in/Experiments/Cryptography


HOME
PARTNERS
CONTACT

---

Computer Science and Engineering > Cryptography > Experiments

**Aim**

Theory

**Objective**

Procedure

Simulation

Assignment

References

**Feedback**

## Breaking the Shift Cipher

A private-key encryption scheme consists of a set of all possible messages, called the message space  $M$ , and three algorithms, namely,

- (a) **Gen**
- (b) **Enc**
- (c) **Dec**

The algorithm for key generation **Gen** is used to choose a key  $k$  at random from the set of all possible secret keys, denoted by the key space  $K$ .

The algorithm for encryption **Enc** takes as inputs the message  $m$  and the secret key  $k$  and outputs the ciphertext  $c$ .

The algorithm for decryption **Dec** inputs the ciphertext  $c$  and the key  $k$  and outputs the message  $m$ .

**About the experiment:**

Apparently, the system is easily broken if the total number of distinct secret keys is small, that is the key space  $K$  is small.

In this experiment, we work with a well-known historical encryption scheme, namely the shift cipher, that has a very small key space.

Your task is to break the shift cipher. Specifically, given (only) the ciphertext in some instance of a shift cipher, you need to find the plaintext and the secret key.

**Community Links**

Sakshat Portal  
Outreach Portal  
FAQ: Virtual Labs

**Contact Us**

Phone: General Information: 011-26592050  
Email: support@vlabs.ac.in

**Follow Us**



### Course Report:

Students are learned about cryptography concepts through this virtual lab. They completed assignment given in this course and submitted.