



# SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

**An Autonomous Institution**

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

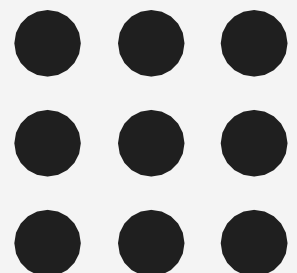
## DEPARTMENT OF INFORMATION TECHNOLOGY

**Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY**

**III YEAR / VI SEMESTER**

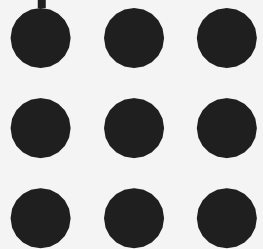
**Unit 1: INTRODUCTION TO NETWORK AND CYBER SECURITY**

**Topic 1: Introduction to Cryptography Security trends, Legal, Ethical and Professional Aspects of Security**





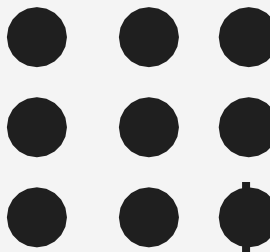
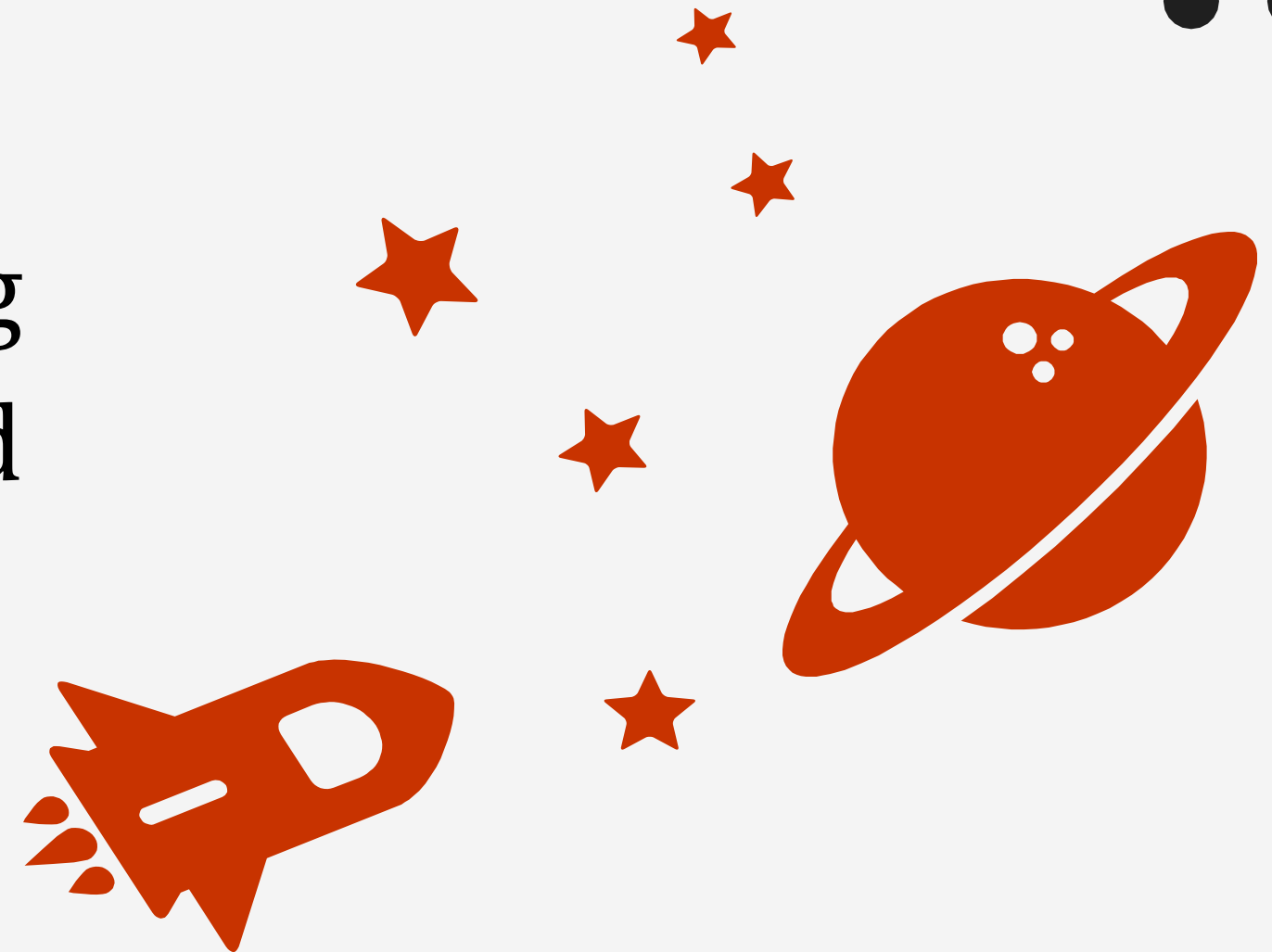
## Cryptography

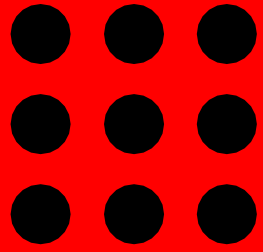




# Cryptography

Science and Art of transforming message to make them secure and immune to attacks





# Basic Terminologies

## Plain Text

- Clear Text
- Message which is readable by humans

Hi user,  
This is an sample message.

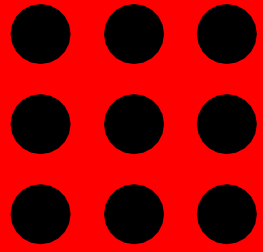


## Cipher Text

- Unreadable Text

KL XVHU,  
WKLV LV DQ VDPSONH PHVVDJH





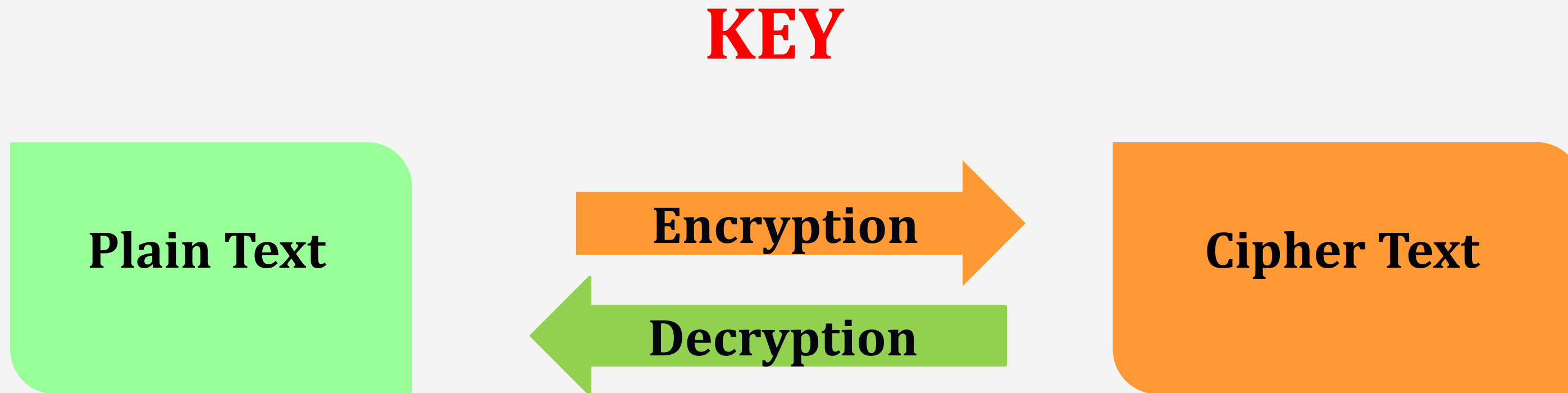
# Basic Terminologies (Continued..)

## Encryption

- The process of converting plaintext to ciphertext

## Decryption

- The process of reverting ciphertext to plaintext



# Information Security

## Information Security

**physical or  
Administrative**

**unauthorized access,  
use, disclosure,  
disruption, modification,  
perusal, inspection,  
recording or destruction**



# Network Security

## Network Security

**business, government  
and academic  
organization**

**Interconnect their data  
processing equipment  
with a collection of  
interconnected networks**



# Computer Security

## Computer Security

telephone network,  
data network or over  
internet

Protect data and thwart  
hackers







# CIA Triad





## CONFIDENTIALITY

- Data confidentiality-Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- Privacy-Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

## INTEGRITY

- Data integrity-Assures that information and programs are changed only in a specified and authorized manner.
- System integrity-Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

## AVAILABILITY

- Assures that systems work promptly and service is not denied to authorized users



# References

- William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.
- Behrouz A. Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.