PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

APPLIED CRYPTOGRAPHY

Lecture 1

A Note on Security

- ☞ In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks.
- ☞ To be clear, you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner.
- ☞ In particular, you will comply with all my instructions when doing the labs.
- ☞ Any violation is at **YOUR RISK!**
  And may result in severe consequences.

In this course

We will discuss…

- Securing data (Encryption and decryption).
- Authentication.
- Digital Signature.
- Applications.
- Case studies.

What is our goal in this course?

- ☞ Our primary goal is to be able to identify security and privacy issues in various aspects of computing, including:
  - *Communication and networking*
  - *Operating systems*
  - *Internet applications*
  - *Databases*
  - *Cloud and IoT*
  - *Mobile applications*
- ☞ Secondarily, to be able to use this ability to design systems that are more protective of security and privacy.

What is Cryptography?

Cryptography

“The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification“.

Source: NIST

The CIA Triad - Core Security Principles

- Secrecy – Data hiding
- Confidentiality – Maintaining secrecy and Privacy
- Integrity - being honest
- Availability

Source: NIST standard FIPS 199
(*Standards for Security Categorization of Federal Information and Information Systems)*

Vulnerabilities, Threats and Attacks

☞ Categories of vulnerabilities

- Corrupted (loss of integrity)
- Leaky (loss of confidentiality
- Unavailable or very slow

☞Threats:

- Loss of Keys

Vulnerabilities, Threats and Attacks

- Attacks *(threats carried out)*
  - Passive – attempt to learn or make use of information from the system
  - Active – attempt to alter data.

Security and Reliability

- Security has a lot to do with reliability
- A secure system is one you can rely on to (for example):
  - *Keep your personal data confidential*
  - *Allow only authorized access or modifications to resources*
- *Give you correct and meaningful results when you want them*

What is Privacy?

There are many definitions of privacy

☞ A useful one: “informational self-determination”

- *This means that you get to control information about you*
- *“Control” means many things:*
  - ✑ *Who gets to see it*
  - ✑ *Who gets to use it*
  - ✑ *What they can use it for*
  - ✑ *Who they can give it to*

Context of Cryptography

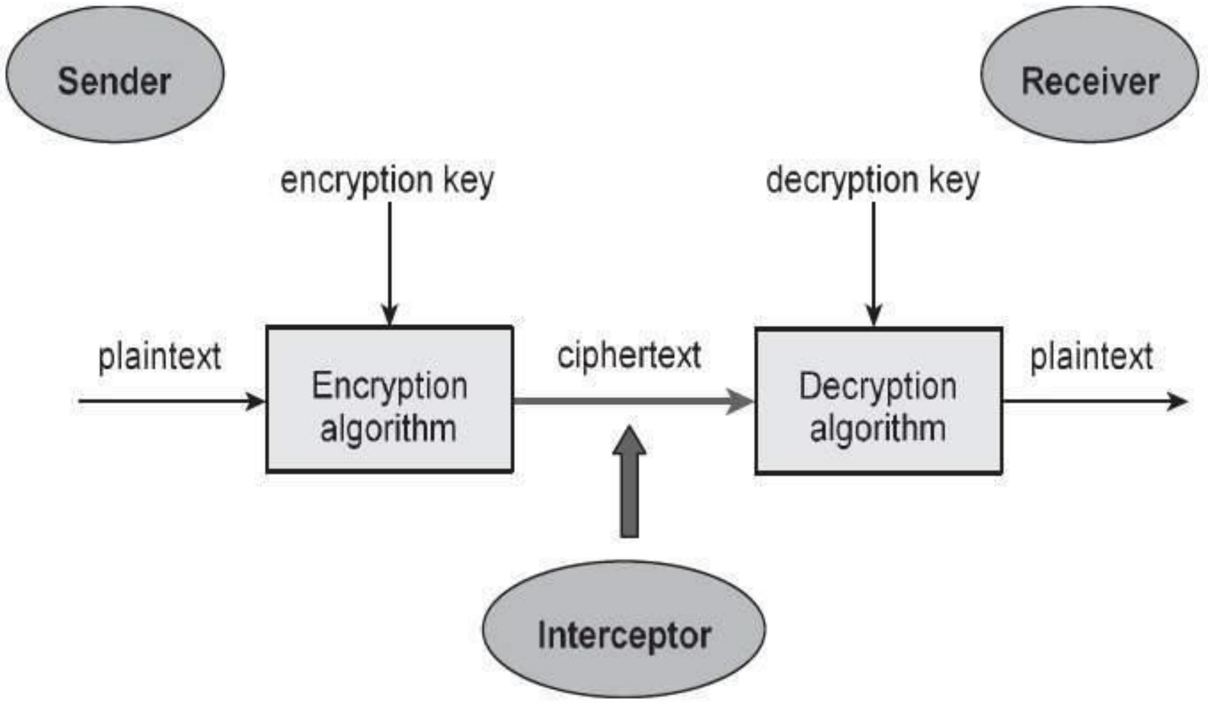
- Cryptology: the study of cryptosystems has two subdivisions
  - Cryptography

    The art and science of making a cryptosystem that can provide information security.

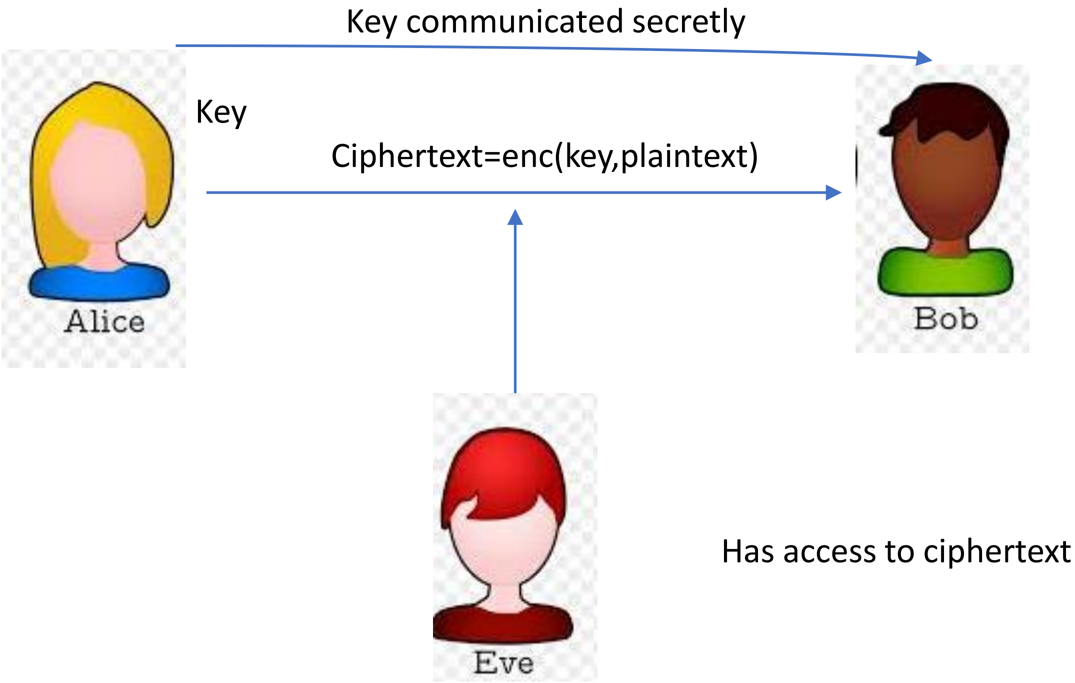
  - Cryptanalysis

    The art and science of breaking the cipher text is known as cryptanalysis.

Crypto system



Data secrecy



Key communicated secretly

Key

Ciphertext=enc(key,plaintext)

Has access to ciphertext

Thank You!

Next Class

- ☞ Mandatory reading for the next class
  - ☞ https://ifca.ai/pub/fc97/r4.pdf

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PESU Center for
Internet
of Things