# Intro to Cryptography

## Introduction

* 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 intentions 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

## What is Privacy?

* The state or condition of being free from public attention to the degree that you determine.
  + Before technology became so advanced, it was relatively easy to choose the level of privacy
  + This is no longer possible. Data is automatically collected, often without user’s knowledge or consent.
* “Terms of condition” or “privacy policy” is too long or often difficult to understand.

## What is Secure Communication?

* Consider the following scenario:
  + Alice and Bob want to communicate “securely”
  + Trudy may intercept, delete, add, or modify messages

Diagram

Description automatically generated

* The communication is secure if the following are met:
  + **Confidentiality**: only Alice and Bob should see message contents
  + **Authentication**: Alice and Bob can confirm identity of each other
  + **Message Integrity**: Alice and Bob can ensure message not altered without detection
  + **Nonrepudiation**: receiver can prove to third party that sender in fact sent message
  + **Traffic Analysis**: Alice and Bob hide that they are communicating
  + **No Denial of Service**: Alice and Bob can communicate

## Security Attacks, Services and Mechanisms

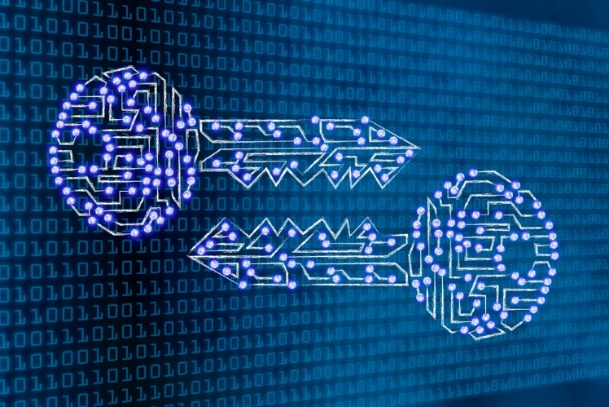
* To assess security needs of an org effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements.
* One approach is to consider three aspects of information security:
  + **Security attack** – Any action that compromises the security of information owned by an org.
  + **Security mechanism** – A mechanism that is designed to detect, prevent or recover from a security attack.
  + **Security service** – A service intended to counter security attacks and enhance security of the data processing systems and the transfer of org info.

## Threat Model: What can an attacker do?

* Q: What can a “bad guy” do? A: a lot!
  + **eavesdrop**: passively intercept messages
  + actively ***insert, modify, or delete*** messages into connection
  + **impersonation**: can fake (spoof) source address in network packet (or any field in packet)
  + **hijacking:** “take over” ongoing connection by removing sender or receiver, inserting himself in place
  + **denial of service**: prevent service from being used by others (e.g., by overloading resources)

## What is Cryptography?

* The science of protecting information by encoding it into an unreachable format
  + store and transmit data in a form that is unintelligible
  + only intended recipients can transform data back into original form and read it
* Effective way of protecting privacy and sensitive information (via providing mechanisms to meet confidentiality, authentication, and integrity)



## Steganography

* The methods of steganography *conceal* *the existence* of the message
* The word, steganography, originating from Greek, means “covered writing” because, unlike cryptography, it covers/hides the message’s existence
* Example: covering data under color image; (1) RGB data of color image used to get data.
* Example: an arrangement of words or letters within an apparently innocuous text spells out the real message: (1) sequence of first letters of each word of the overall message spells out the real (hidden) message; (2) subset of words of the overall message is used to convey the hidden message.
* Various other techniques have been used historically, some of them are:
  + **Character marking** – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.
  + **Invisible ink** – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
  + **Pin punctures** – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.
  + **Typewritten correction ribbon** – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.
* Drawbacks of steganography:
  + Requires a lot of overhead to hide relatively few bits of information.
  + Once the system is discovered, it becomes virtually worthless.

## Cryptography Terms

* 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 sender & receiver
* encipher (encode) = process of converting plaintext to cipher text using a cipher and a key
* decipher (decode) = process of converting cipher text back into plaintext using a cipher and a key
* cryptoanalysis (code breaking) = study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key
* cryptology = both cryptography and cryptoanalysis
* code = an algorithm for transforming an intelligible message into an unintelligible one using a code-book

## Two Principles of Cryptography

* Confusion
  + Making the relationship between ciphertext and key as complex and intricate as possible
  + To hide the relationship between the ciphertext and the key
  + Makes it difficult to find the key from the ciphertext
  + If a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected
  + Provided by (advanced) substitution techniques
* Diffusion
  + The redundancy in the statistical nature of plaintext is reduced in the statistics of the ciphertext
  + To hide the relationship between the ciphertext and the plaintext
  + Provided by transposition techniques