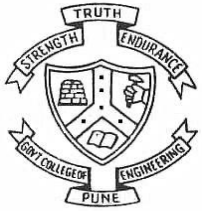
# Cryptography and Network Security

Dr. V. K. Pachghare




Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

# Definitions

- **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

# Cryptography

- **Cryptography** – *Secret writing*

  from the Greek for "secret writing" is the mathematical "scrambling" of data so that only someone with the necessary ***key*** can "unscramble" it.

- Cryptography allows secure transmission of private information over insecure channels

***Plaintext*** – A message in its natural format readable by an attacker (Original message/data)

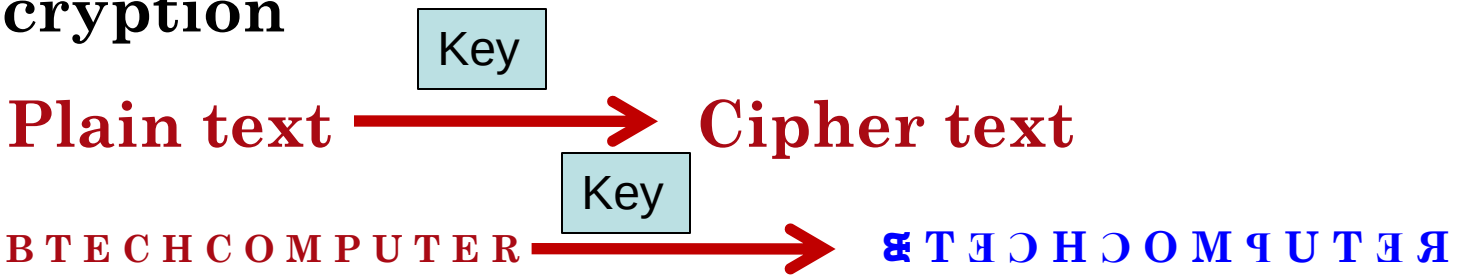
***Ciphertext*** – Message altered to be unreadable by anyone except the intended recipients (Encoded message/data)

***Key*** – Sequence that controls the operation and behavior of the cryptographic algorithm (Password)

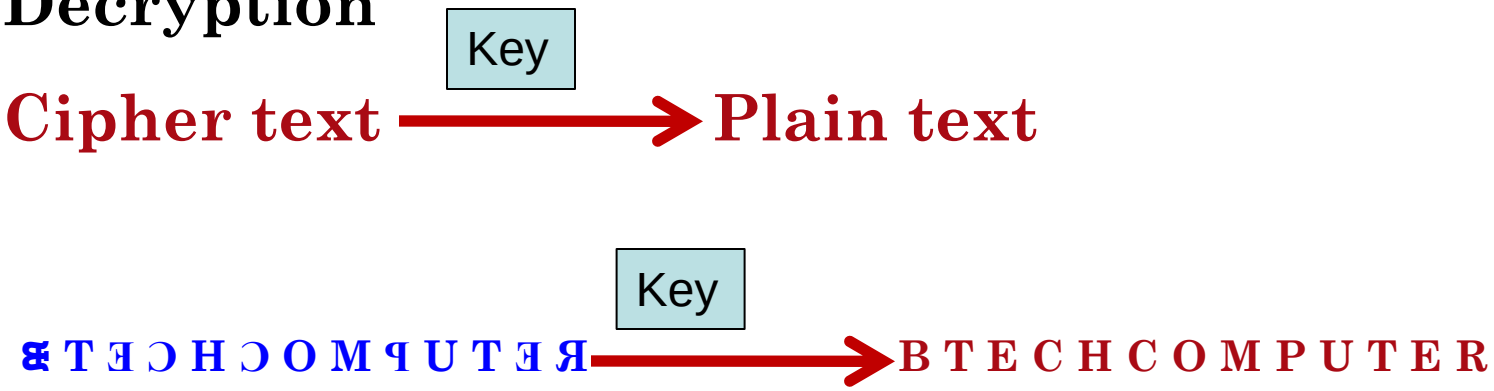
***Keyspace*** – Total number of possible values of keys in a crypto algorithm (ex. Suppose the key is binary and the key size is 3 then keyspace is $2^3$.)

**Cryptography also allows secure storage of sensitive data on any computer.**

**Encryption**




**Decryption**

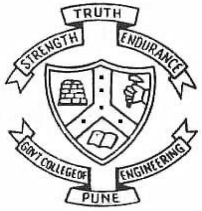


# Types of Cryptography

- Stream-based Ciphers
  - One bit at a time (A-D, B-Z……)
  - Mixes plaintext with key stream
  - Good for real-time services
- Block Ciphers
  - Substitution and transposition
  - Number of bits at a time (BALL – ZDCW)

# Encryption Systems

- Substitution Cipher
  - Convert one letter to another
- Transposition Cipher
  - Change position of letter in text
  - Word Jumble
- Monoalphabetic Cipher
  - Caesar
- Polyalphabetic Cipher
  - Vigenère
- One-time Pads
  - Randomly generated keys



# Attributes of Strong Encryption

- ***Confusion***
  - Change key values each round
  - Performed through substitution
  - Complicates ciphertext /key relationship
- ***Diffusion***
  - Change location of plaintext in ciphertext
  - Complicates ciphertext /plaintext relationship

# Hashing Algorithms

- **MD5**
  - Computes 128-bit hash value
  - Widely used for file integrity checking
- **SHA-1**
  - Computes 160-bit hash value
  - NIST approved message digest algorithm
- **RIPEMD-160**
  - Developed in Europe published in 1996
  - Patent-free

# Three Aspects of Information Security

- Security attack
- Security mechanism
- Security service

# Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

# Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**

# Security Attack

- any action that compromises the security of information

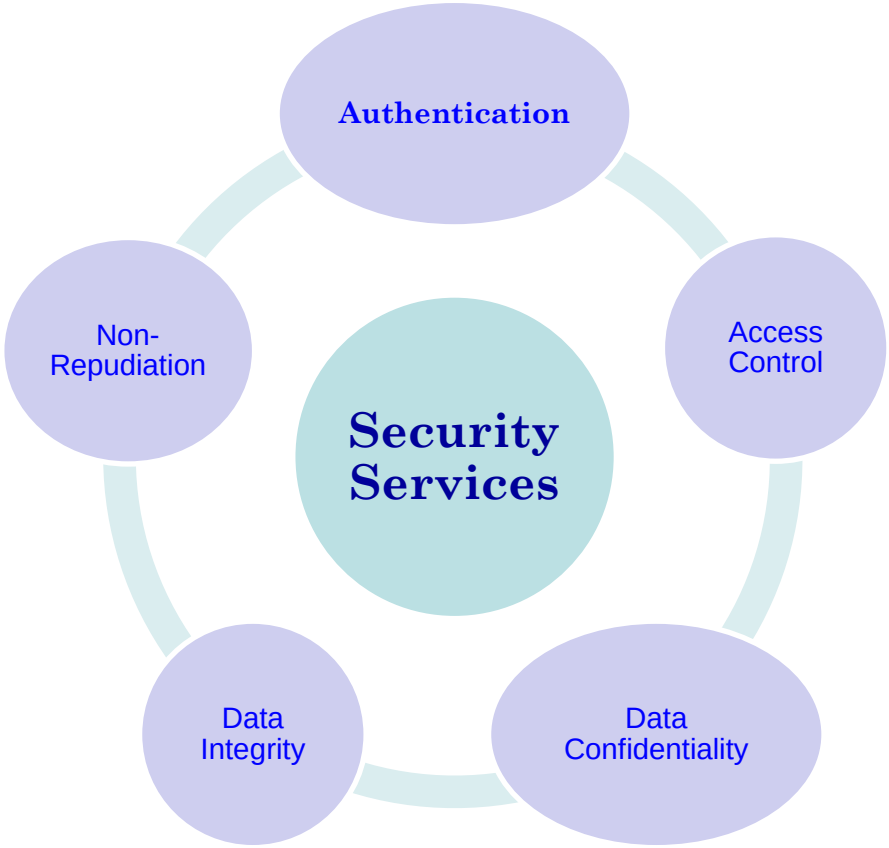
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems

# Security Services (X.800)

# Security Services (X.800)

- X.800 defines a security service as a service provided by a protocol layer of communicating open systems
- Security Services implement security policies and are implemented by security mechanisms
- X.800 divides these services into five categories and fourteen specific services

# Security Services



# Authentication

- assurance that the communicating entity is the one claimed
  - **Peer Entity Authentication**: Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - **Data Origin Authentication**: In a connectionless transfer, provides assurance that the source of received data is as claimed.

# Access Control

- prevention of the unauthorized use of a resource
- i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.

# Data Confidentiality

- protection of data from unauthorized disclosure
  - **Connection Confidentiality**: The protection of all user data on a connection.
  - **Connectionless Confidentiality**: The protection of all user data in a single data block
  - **Selective-Field Confidentiality**: The confidentiality of selected fields within the user data on a connection or in a single data block.
  - **Traffic Flow Confidentiality**: The protection of the information that might be derived from observation of traffic flows.

# Data Integrity

- assurance that data received is as sent by an authorized entity
- i.e., contain no modification, insertion, deletion, or replay
  - Connection Integrity with Recovery: Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
  - Connection Integrity without Recovery: As above, but provides only detection without recovery.

- Selective-Field Connection Integrity: Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- Connectionless Integrity: Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

- Selective-Field Connectionless Integrity: Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

# Non-Repudiation

- protection against denial by one of the parties in a communication
  - Non-repudiation, Origin: Proof that the message was sent by the specified party.
  - Non-repudiation, Destination: Proof that the message was received by the specified party

# Security Mechanisms (X.800)

- Specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control
- Pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery