# CHAPTER 5

Anonymity, Security, Privacy, and Civil Liberty

# INTRODUCTION

- There is a large quantity of information available and there is an increase in demand for this information
- Factors that contribute to the need for Anonymity, Security, Privacy, and Civil Liberty:
  - High digitization of information and increasing bandwidth
  - Declining costs of digital communication
  - Increased miniaturization of communication devices
  - Awareness

# ANONYMITY

- From the Greek word for being nameless
- Types usually used:
  - Pseudo-identity
  - Untraceable identity
  - Anonymity with a pseudo-address
- Anonymity and the internet:
  - Two channels for carrying out anonymity
    - Anonymous servers
    - Anonymous users

# ANONYMITY

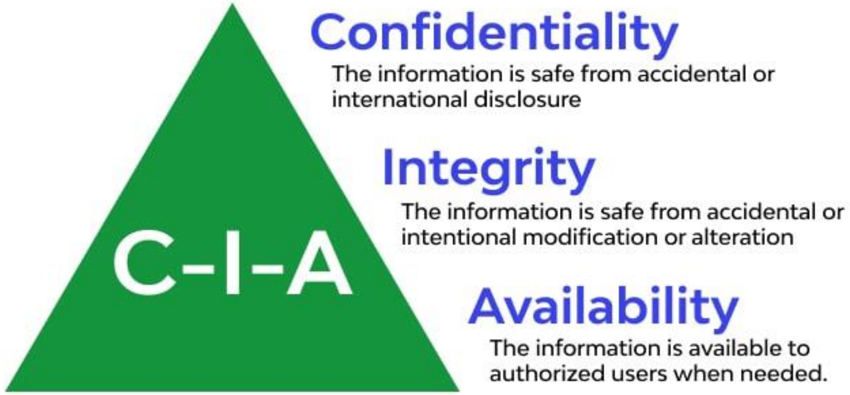
- Advantages and disadvantages to anonymity
- Legal view of anonymity

# GROUP DISCUSSION

- List roles in society that might require anonymity. Is this beneficial to society?
- Discuss the disadvantages to anonymity.

# SECURITY

- A means to prevent unauthorized access, use, alteration, and theft of physical damage to property.
- Elements of security:
  - Confidentiality
  - Integrity
  - Availability
- Types of security:
  - Physical security
  - Information security



**Confidentiality**

The information is safe from accidental or international disclosure

**Integrity**

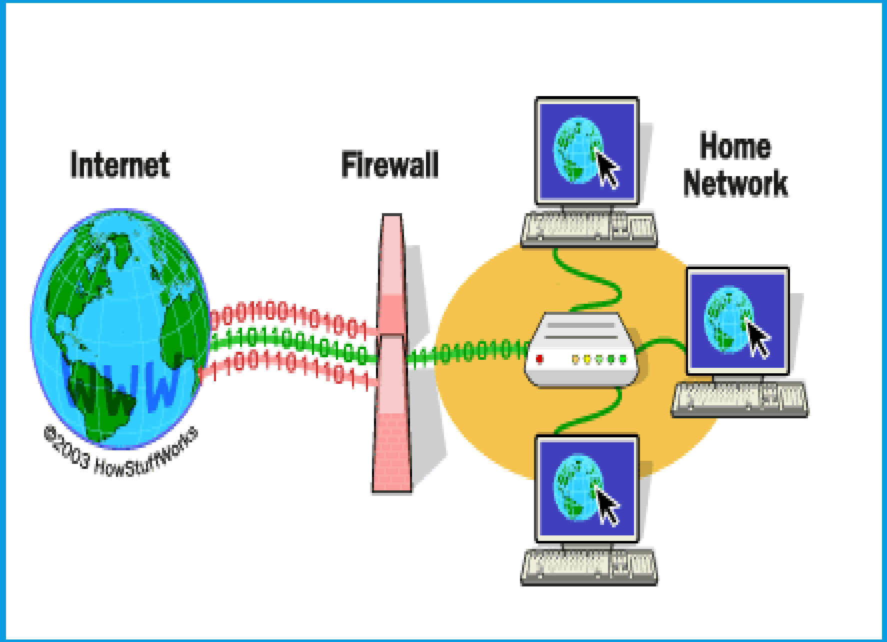
The information is safe from accidental or intentional modification or alteration

**Availability**

The information is available to authorized users when needed.

# PHYSICAL SECURITY

- Mechanisms for guaranteeing physical security:
  1. Deterrence
  2. Prevention
  3. Detection
  4. Response
- Physical access controls
  - Physical security barriers
  - Electronic access controls
    - Card access control
    - Passwords
    - Firewalls: Packet filters, Proxy servers, Stateful inspection



# INFORMATION SECURITY CONTROLS

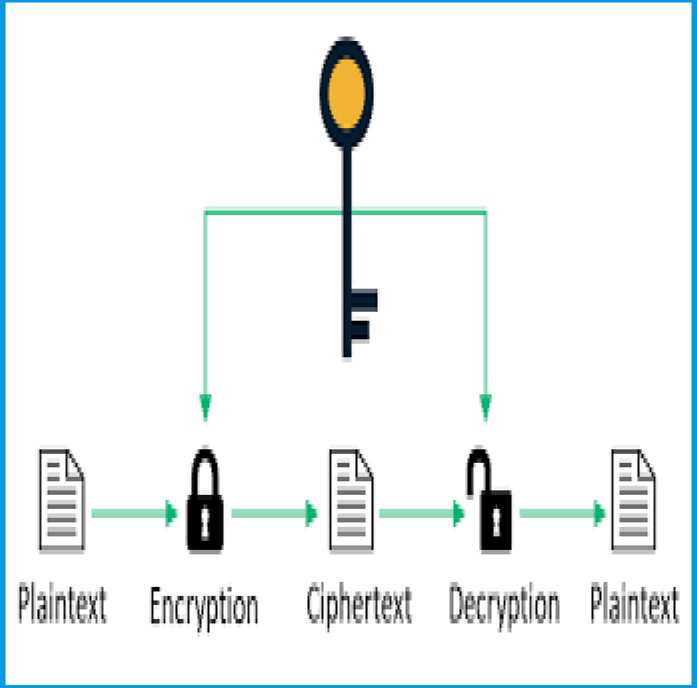
- Includes the integrity, confidentiality, and availability of information at the servers and in transition between servers and between clients and servers.
- Can be ensured by:
  - Cryptography- during transition
  - Authentication –at source and destination

# INFORMATION SECURITY CONTROLS – ENCRYPTION 1

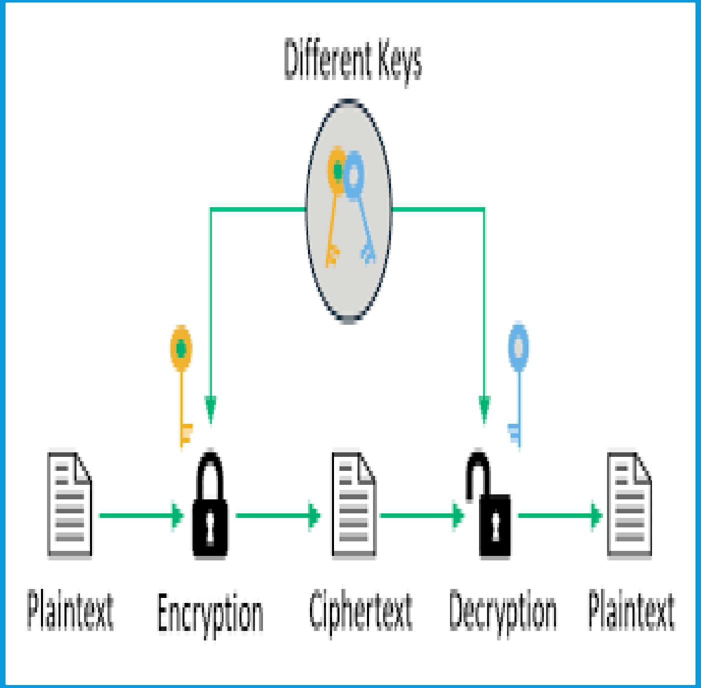
- A method that protects the communication channel from sniffers.
- ***Sniffers***: programs written for and installed on the communication channel to eavesdrop on network traffic.
- ***Cryptography*** uses an encryption algorithm and key to transform data at the source, called *plaintext*; turn it into an encrypted form called *ciphertext*; and finally recover it at the *sink*.
- Encryption algorithm can be either *symmetric* or *asymmetric*.

# INFORMATION SECURITY CONTROLS – ENCRYPTION 2

## Symmetric Encryption

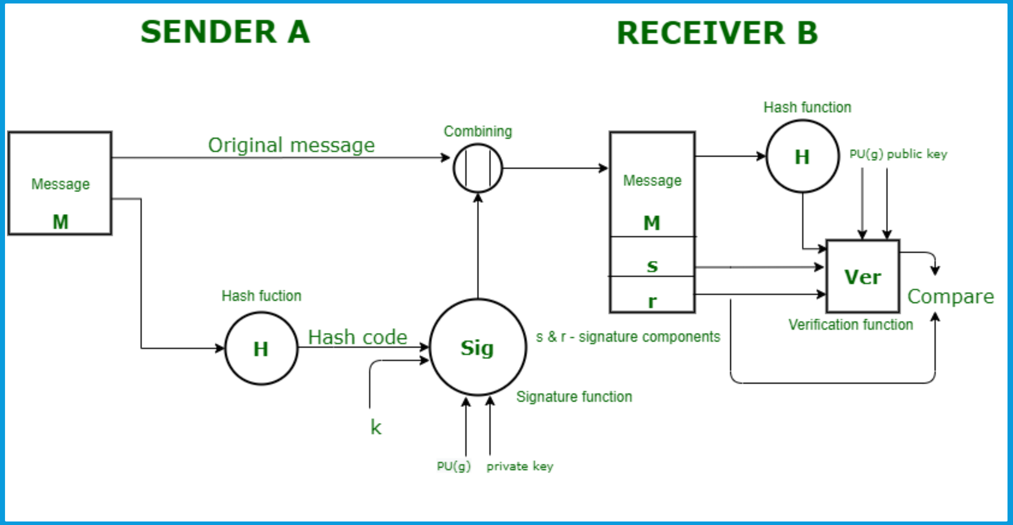


## Asymmetric Encryption



# INFORMATION SECURITY CONTROLS – AUTHENTICATION 1

- A process whereby the gathers and builds up information about the user to assure that the user is genuine.
- Also used to ensure the digital message recipient of the identity of the sender and integrity of the message.
- Digital signature once submitted can never be disowned- called *nonrepudiation*.
- Digital signature system consists of two parts: A method for signing a document and authentication that the message was generated by them.



# INFORMATION SECURITY CONTROLS – AUTHENTICATION 2

- Physical Authentication Methods
  - Username
  - Password
  - Biometrics like retinal images
  - Fingerprints
  - Physical location (IP address)
  - Identity cards

# OPERATIONAL SECURITY

- Policies and procedures for safeguarding the assets of the organization.
- Spelt out in the Security Policy.
- Includes guidelines for security recovery and response incase of an incident.

# PRIVACY

- A human attribute consisting of solitude, anonymity, intimacy and reserve.
- Organized in two categories:
  1. Control of external influence
     - Solitude
     - Anonymity
     - Intimacy
  2. Control of personal information
     - Reserve

# TYPES OF PRIVACY

- Personal privacy
- Informational privacy
  - Personal information
  - Financial information
  - Medical information
  - Internet
- Institutional privacy

# VALUE OF PRIVACY

- Gained more importance in the information age
- Consider three attributes of privacy
  - Personal identity
  - Autonomy
  - Social relationships

# PRIVACY IMPLICATIONS OF DATABASE SYSTEMS

- Information gathering
- Tools have improved, becoming smaller and more stealthily
  - Internet crawlers
- Tremendous legal and privacy issues that need to be dealt with
  - Legislation and enforcing of new laws cannot keep up with fast pace of technology development

# PRIVACY VIOLATIONS AND LEGAL IMPLICATIONS

- Causes of violations
  1. Consumers willingly giving up information
  2. Lack of knowledge
  3. Inadequate privacy policies
  4. Failure to follow privacy policies
  5. Internet temptation
- Privacy violations include
  - Intrusion
  - Misuse of information
  - Interception of information, at source or sink, or during transit
  - Information Matching

# PRIVACY PROTECTION

- Guidelines and structures for protecting privacy rights
  - Technical
  - Contractual
  - Legal