Information Security Awareness

Information Security

- Shortened to InfoSec
- It is the practice of defending information from
  - Unauthorized access
  - Use
  - Disclosure
  - Disruption
  - Modification
  - Perusal
  - Inspection
  - Recording
  - Destruction

Definitions

- Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.(ISO/IEC 27000:2009)
- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.(CNSS, 2010)
- Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability). (ISACA, 2008)
- Information Security is the process of protecting the intellectual property of an organization. (Pipkin, 2000)
- Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties. (Venter and Eloff, 2003)

IT Security

- Also referred to Computer Security
- It is information security applied to technology
- IT security specialists are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems

Information Assurance

- It is an act of ensuring that data is not lost when critical issues arise
- These issues include but are not limited to:
  - Natural disasters
  - Computer/server malfunction
  - Physical theft
  - Any other instance where data has the potential of being lost
- An off-site backup of the data in case one of the mentioned issues arise

Threats

- Software Attacks,
- Theft of intellectual property,
- Identity theft,
- Theft of equipment or information,
- Sabotage, and
- Information extortion

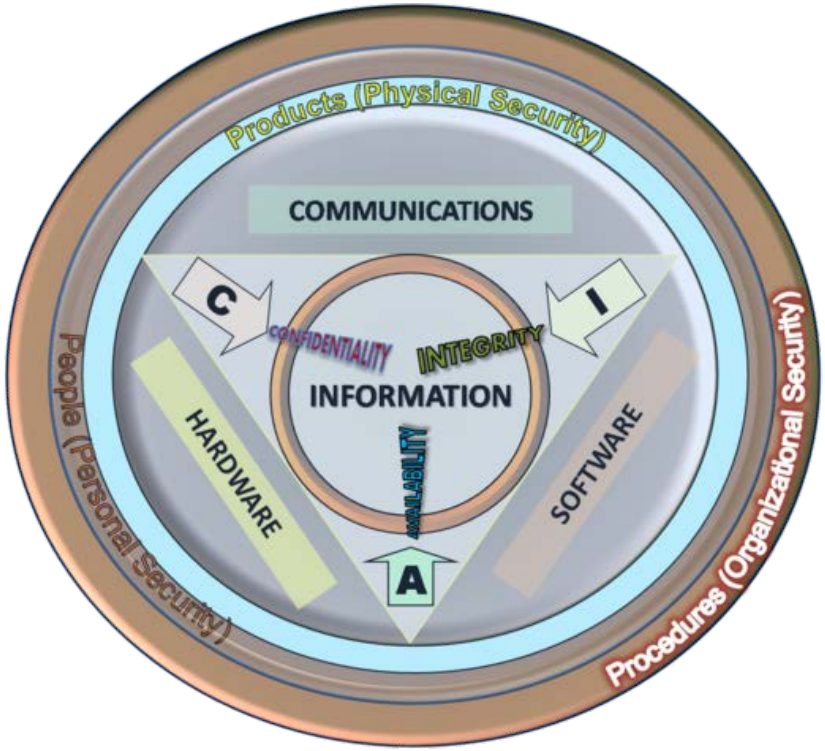
Threats

- Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks
- Intellectual property is the ownership of property usually consisting of some form of protection
- Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information

Threats

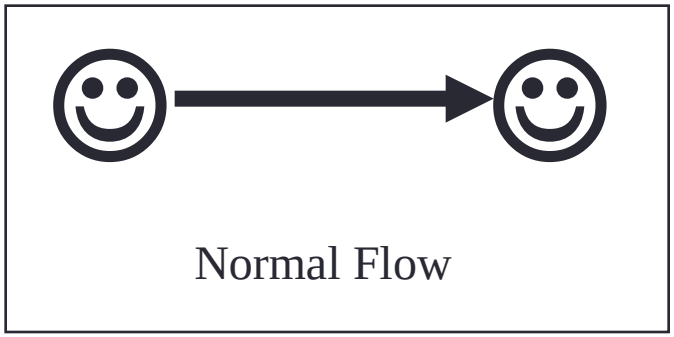
- Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile.
- Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases
- Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence to its customers
- Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner

Basic Principles

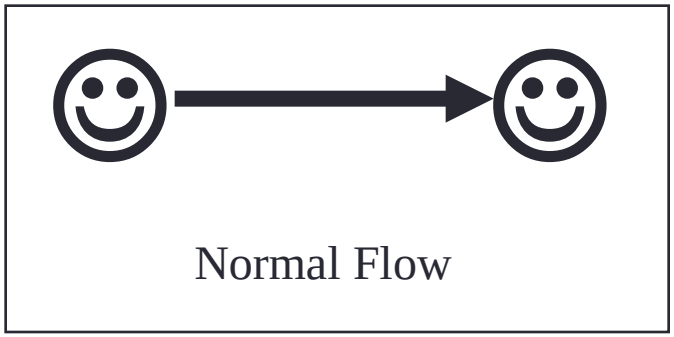


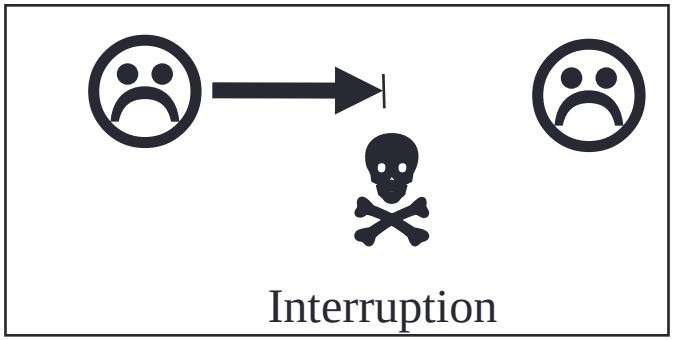
The CIA triad of **confidentiality**, **integrity**, and **availability** is at the heart of information security

Network Security Issues

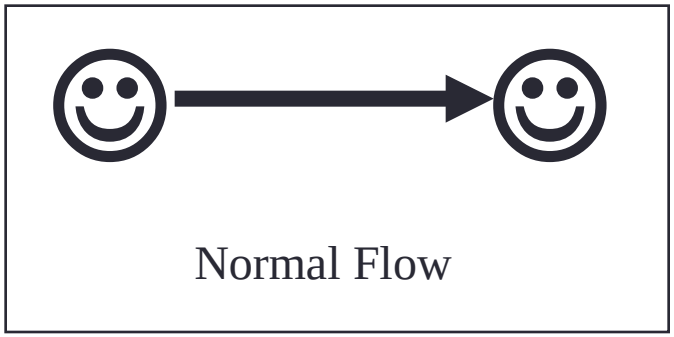


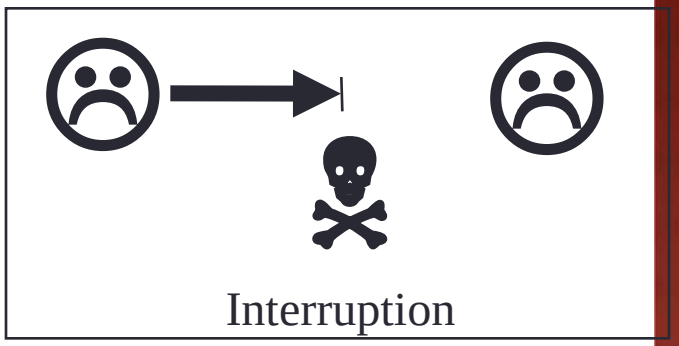
Network Security Issues

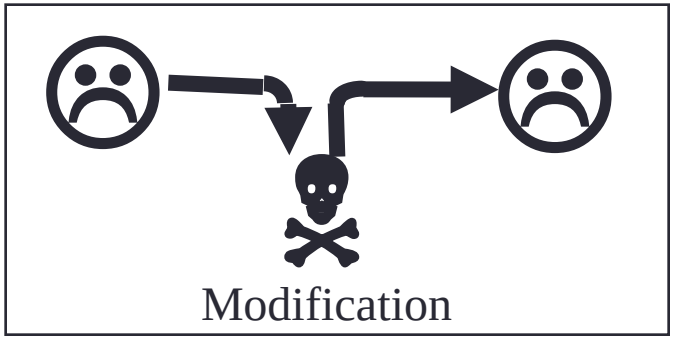




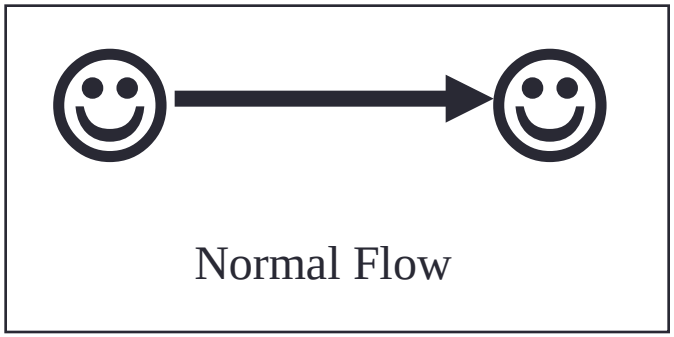
Network Security Issues

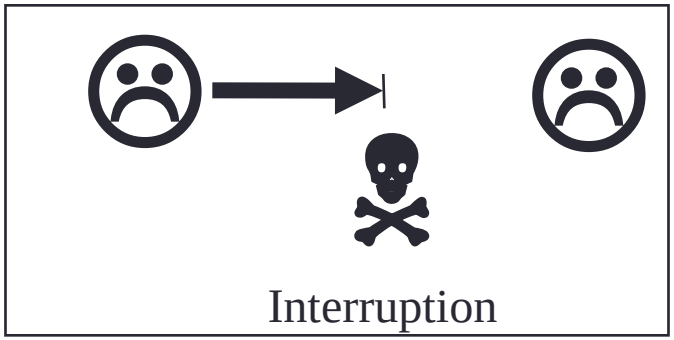


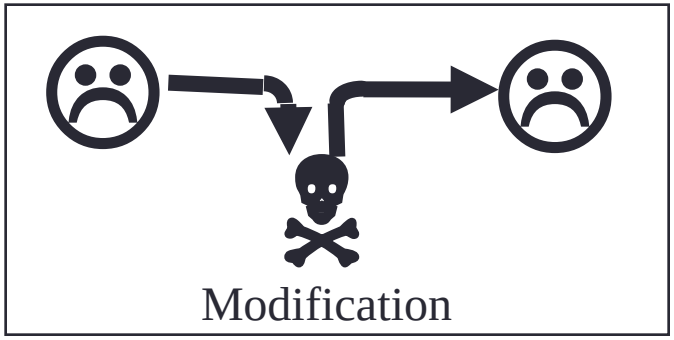


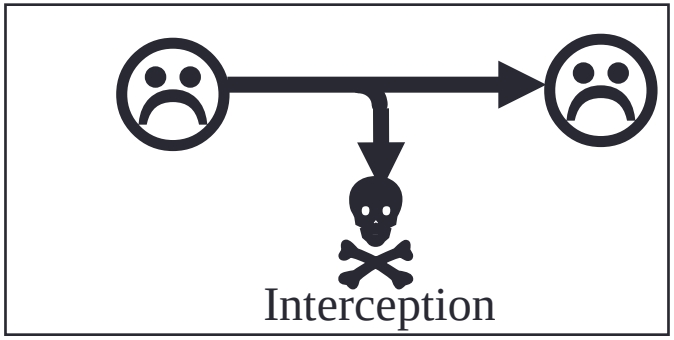


Network Security Issues

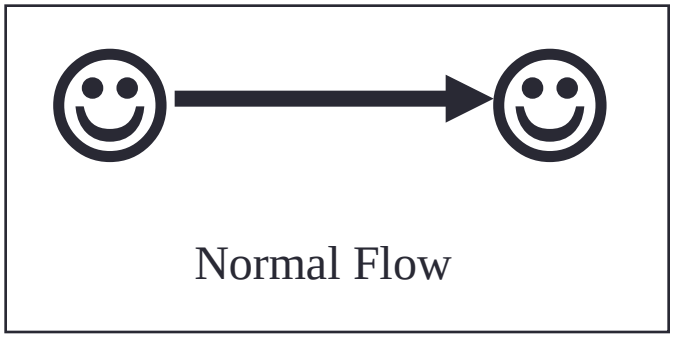


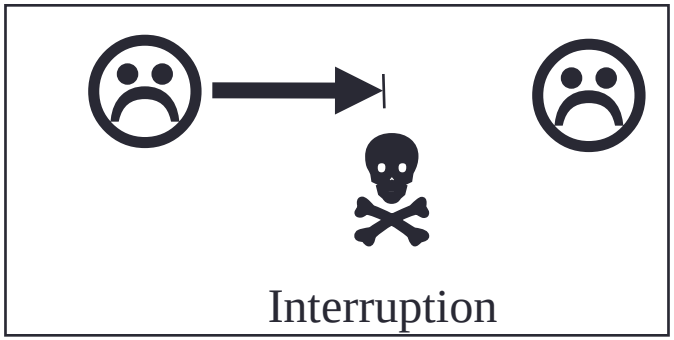


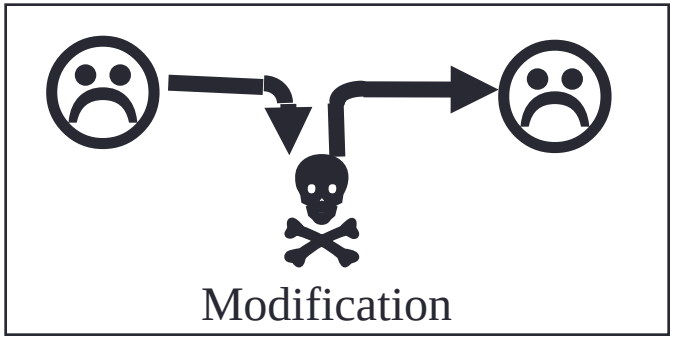


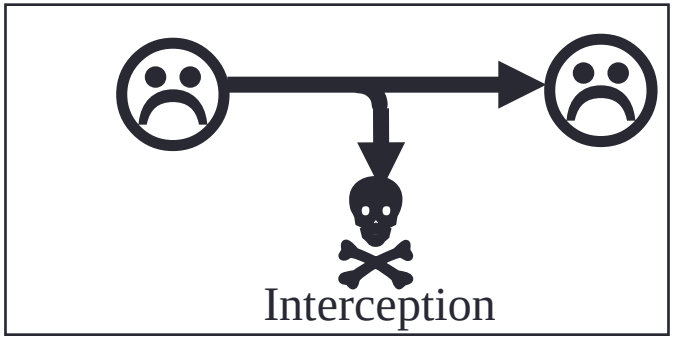


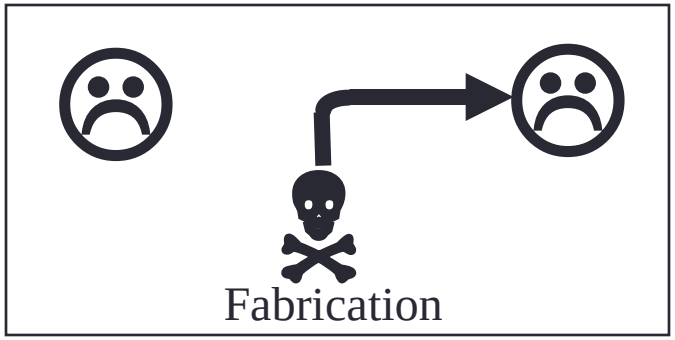
Network Security Issues



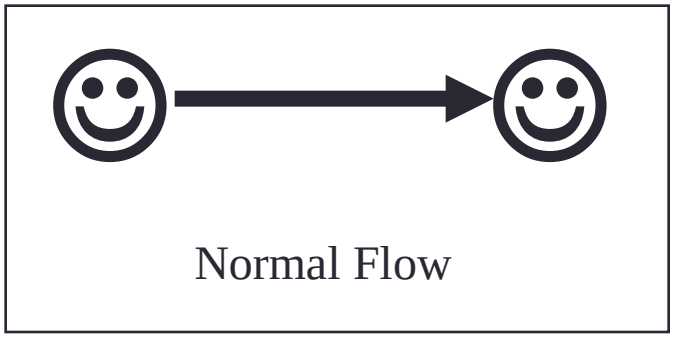


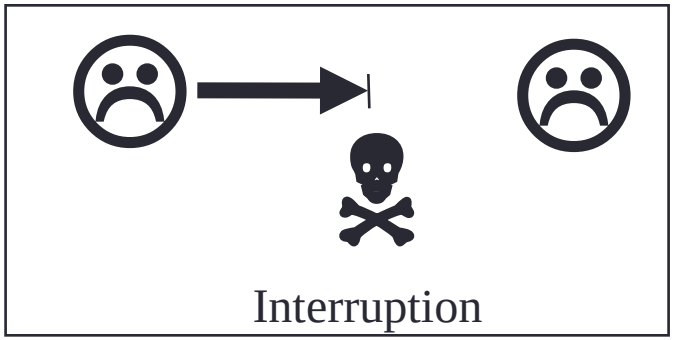


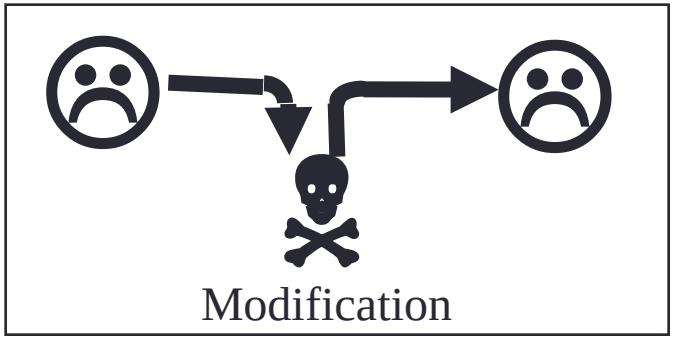


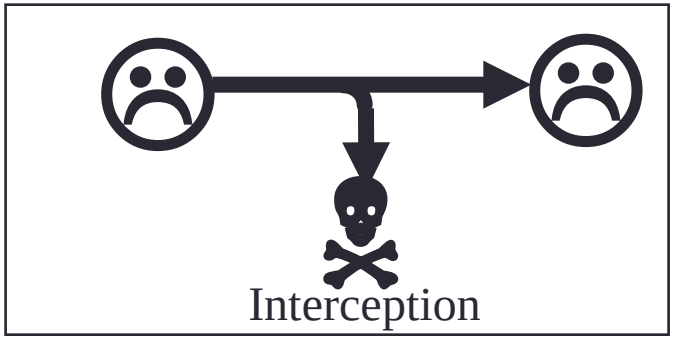


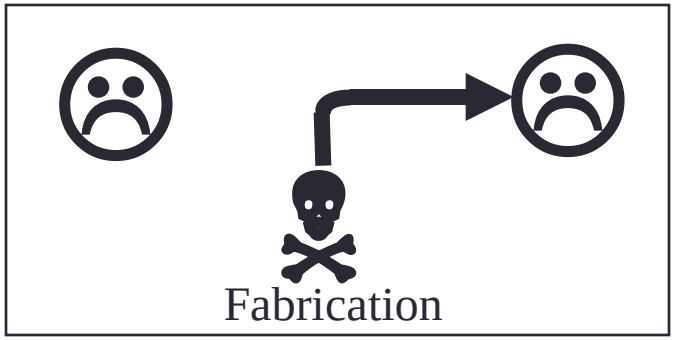
Network Security Issues

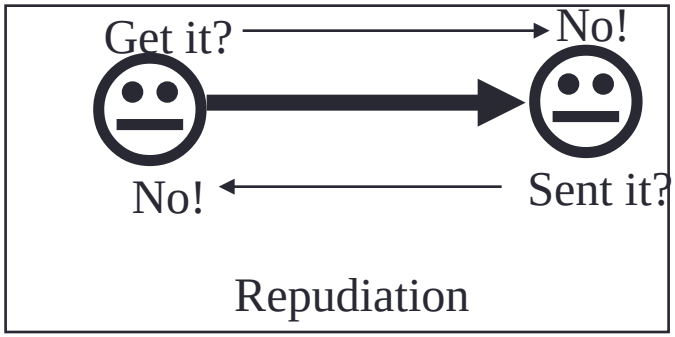




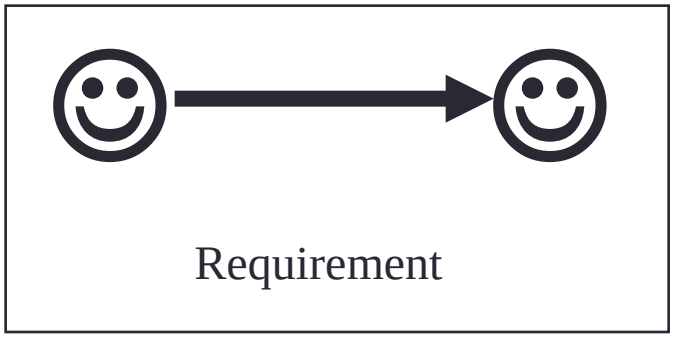




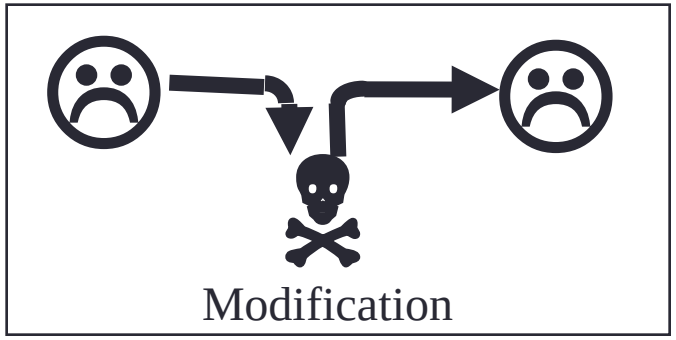


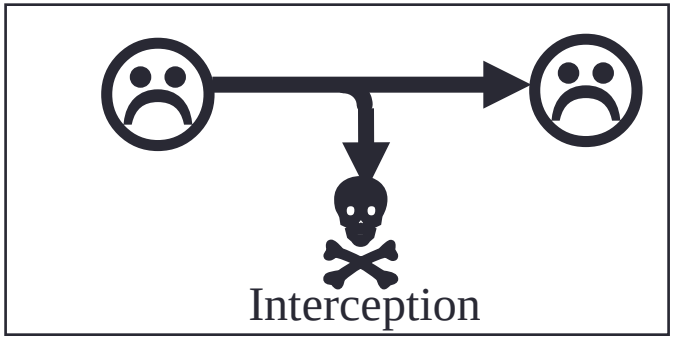


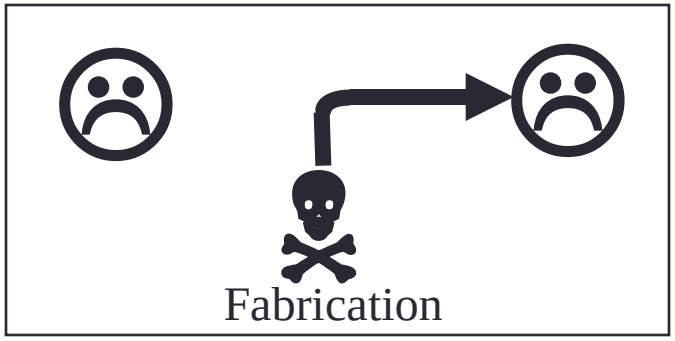
Network Security Services

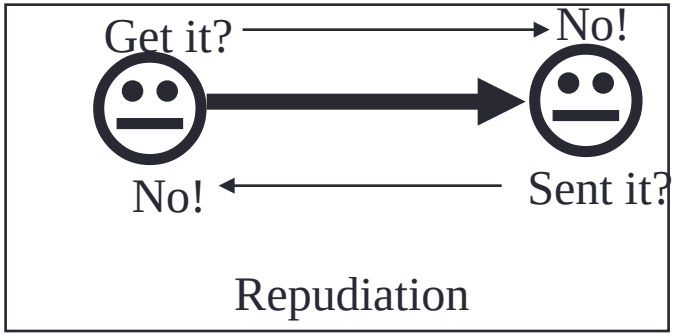


Availability

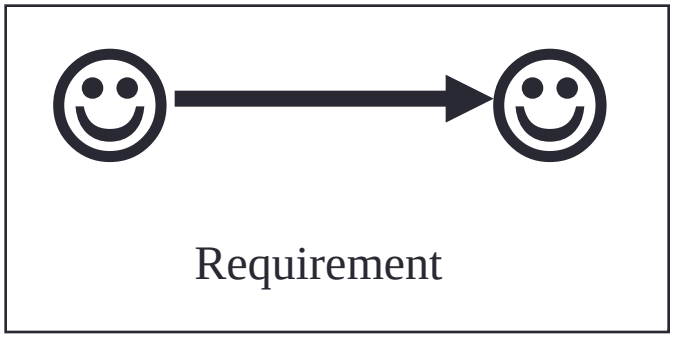






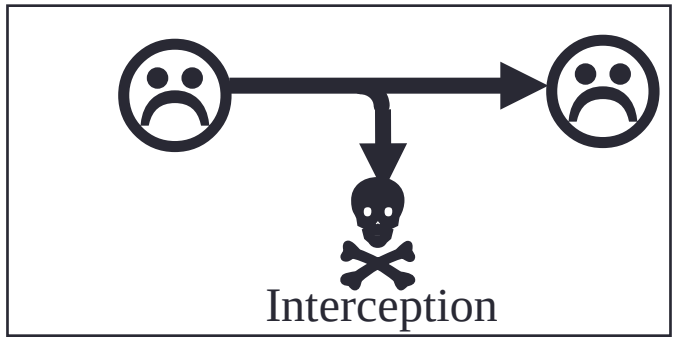


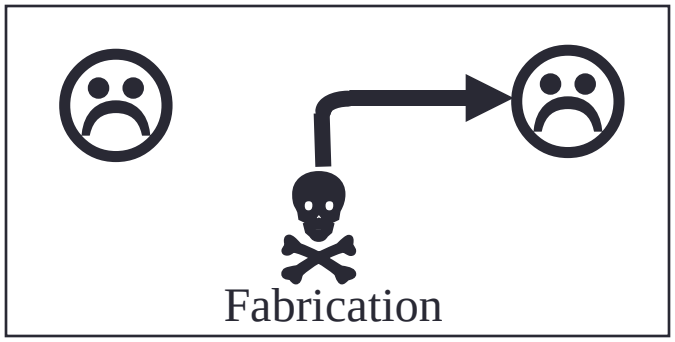
Network Security Services

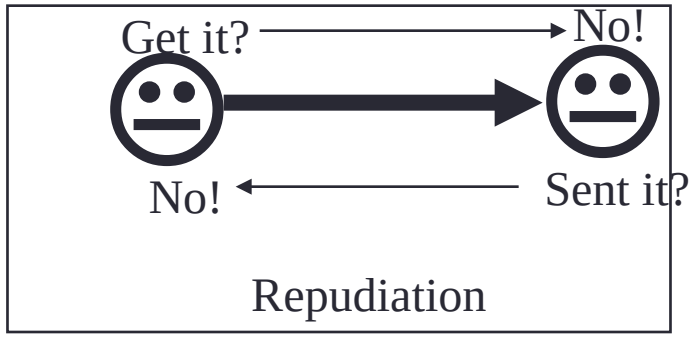


Availability

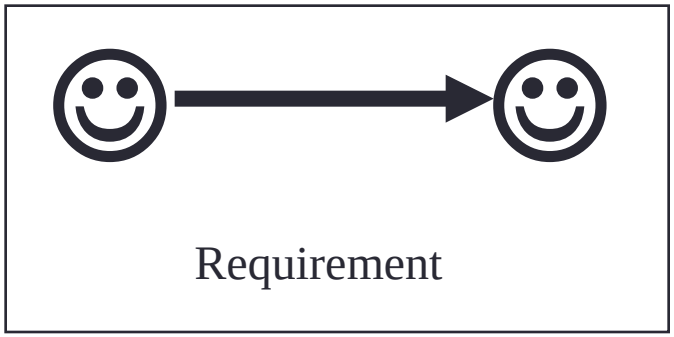
Integrity







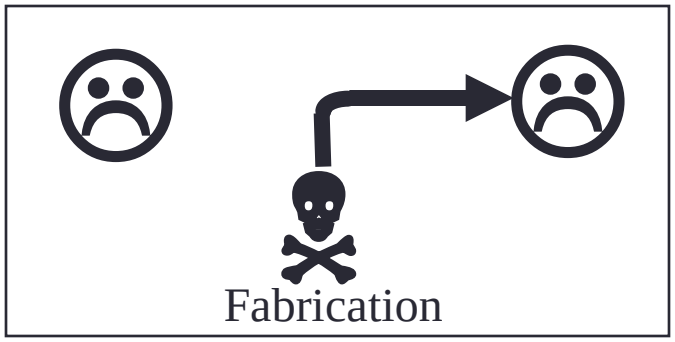
Network Security Services

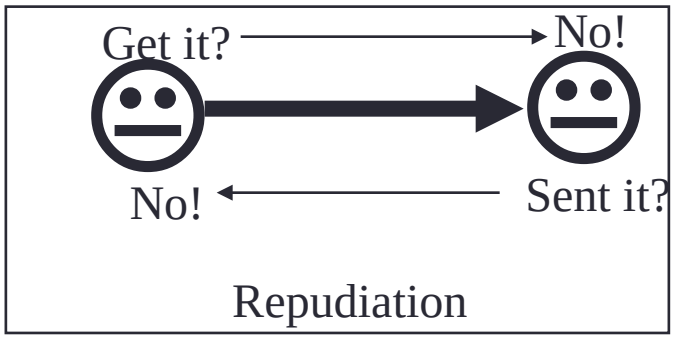


Availability

Integrity

Confidentiality





Network Security Services

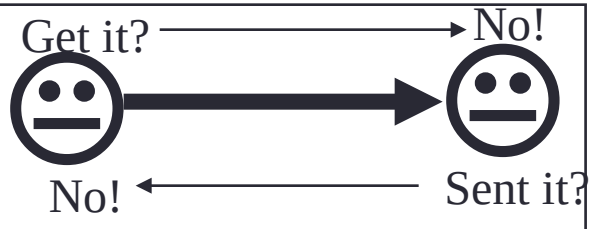
Requirement

Availability

Integrity

Confidentiality

Authenticity



Repudiation

Network Security Services

Requirement

Availability

Integrity

Confidentiality

Authenticity

Non Repudiation

Security Mechanisms

- Confidentiality - Encryption
- Integrity - Hashing
- Authentication - Digital Certificates
- Non-Repudiation - Digital Signatures

Basic Terminology

Cryptology

Branch of maths that studies the mathematical foundation of cryptographic methods

Cryptography

Art of secret (crypto) writing (-graphy)

Cryptanalysis

Art of breaking ciphers

Basic Cryptography Terminology

- **Plaintext** - the original message
- **Ciphertext** - the coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering plaintext from ciphertext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (code breaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **Cryptology** - the field of both cryptography and cryptanalysis

Cryptographic Algorithms

- Types of Cryptographic algorithms
  - Secret key cryptography or Symmetric Key
  - Public key cryptography or Asymmetric Key
  - Hash functions

Types of Cryptosystems

- Secret Key or Symmetric Cryptography

  DES, IDEA, AES etc.

Advantages: *fast, cipher text secure*

Disadvantages: *must distribute key in advance, key must not be divulged*

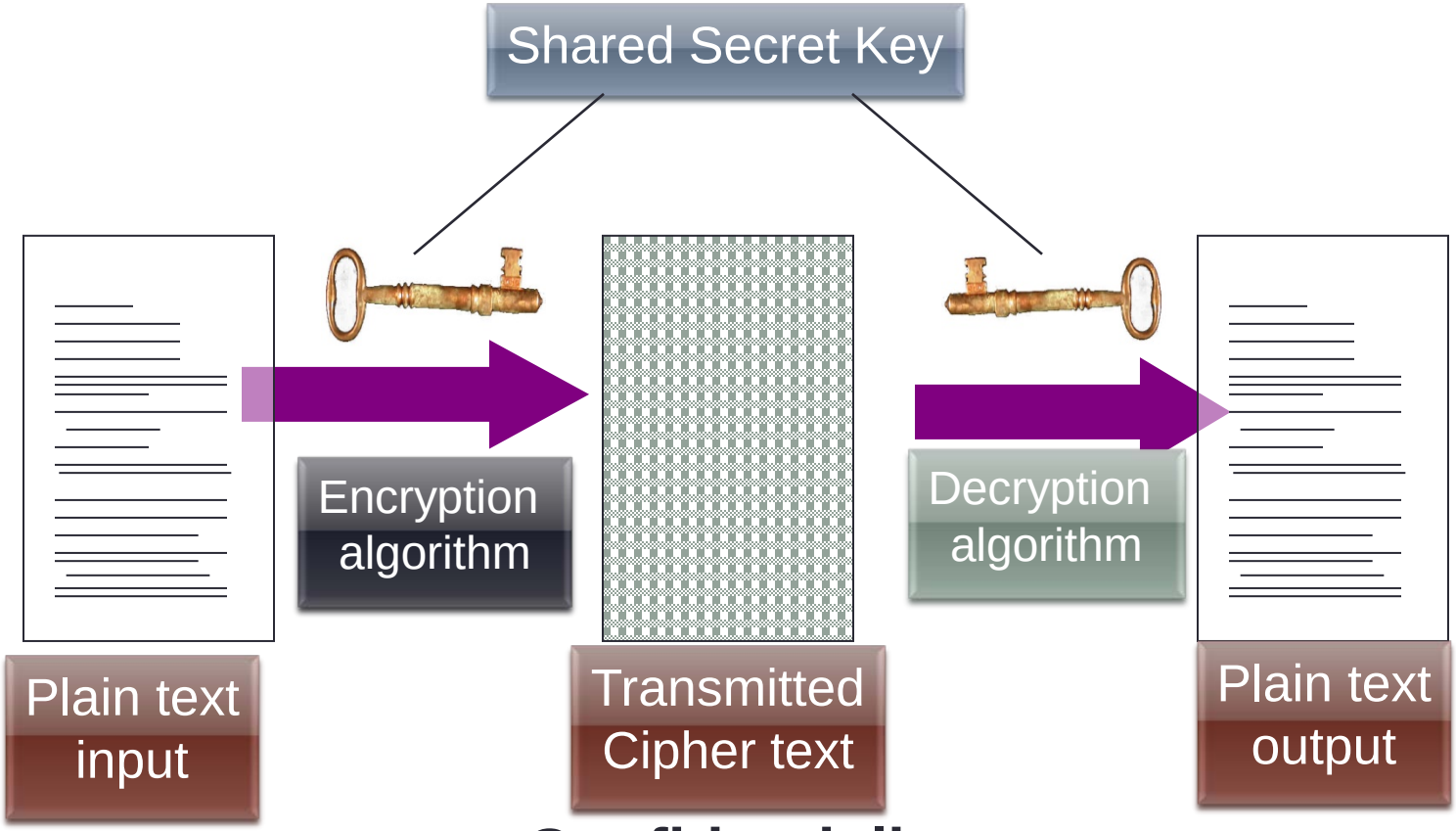
- Public-key or Asymmetric Cryptography

  RSA, Diffie-Hellman key agreement protocol

Advantages: *public key widely distributable, does digital signatures*

Disadvantages: *slow*

Secret Key Algorithms

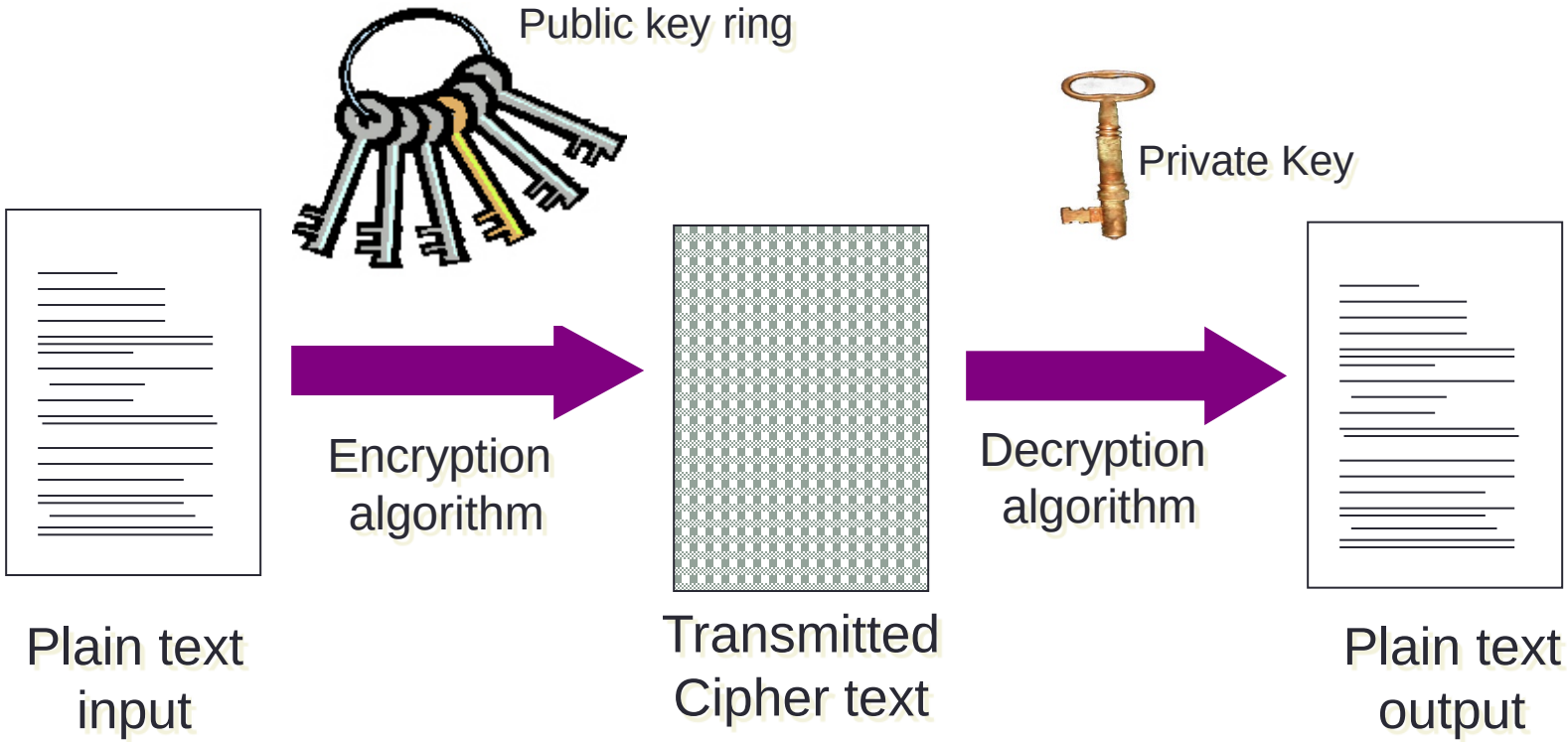


Confidentiality

Key Distribution

- Symmetric schemes require both parties to share a common secret key
- Issue is how to securely distribute this key
- Often secure system failure due to a break in the key distribution scheme

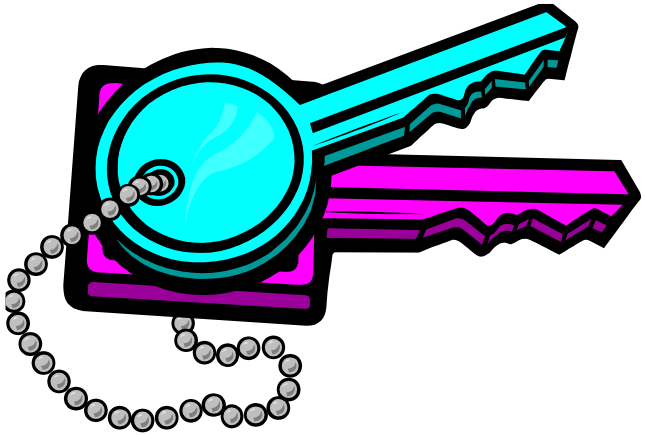
Public Key Algorithms



Confidentiality

Public Key Cryptography

- Uses two keys: private & public
- Used for
  - Confidentiality
  - Authentication
  - Key distribution

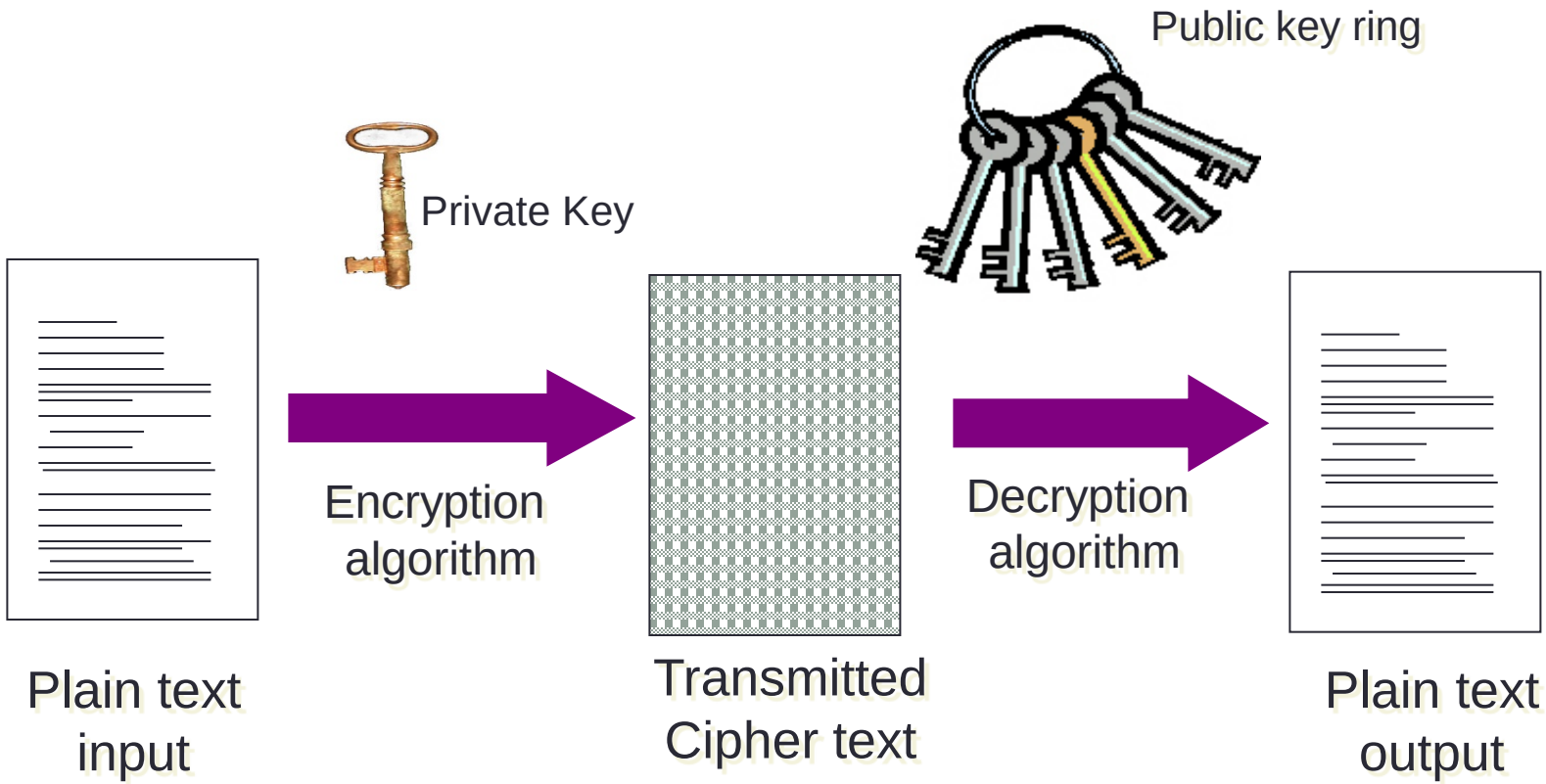


Public Key Cryptography

Confidentiality

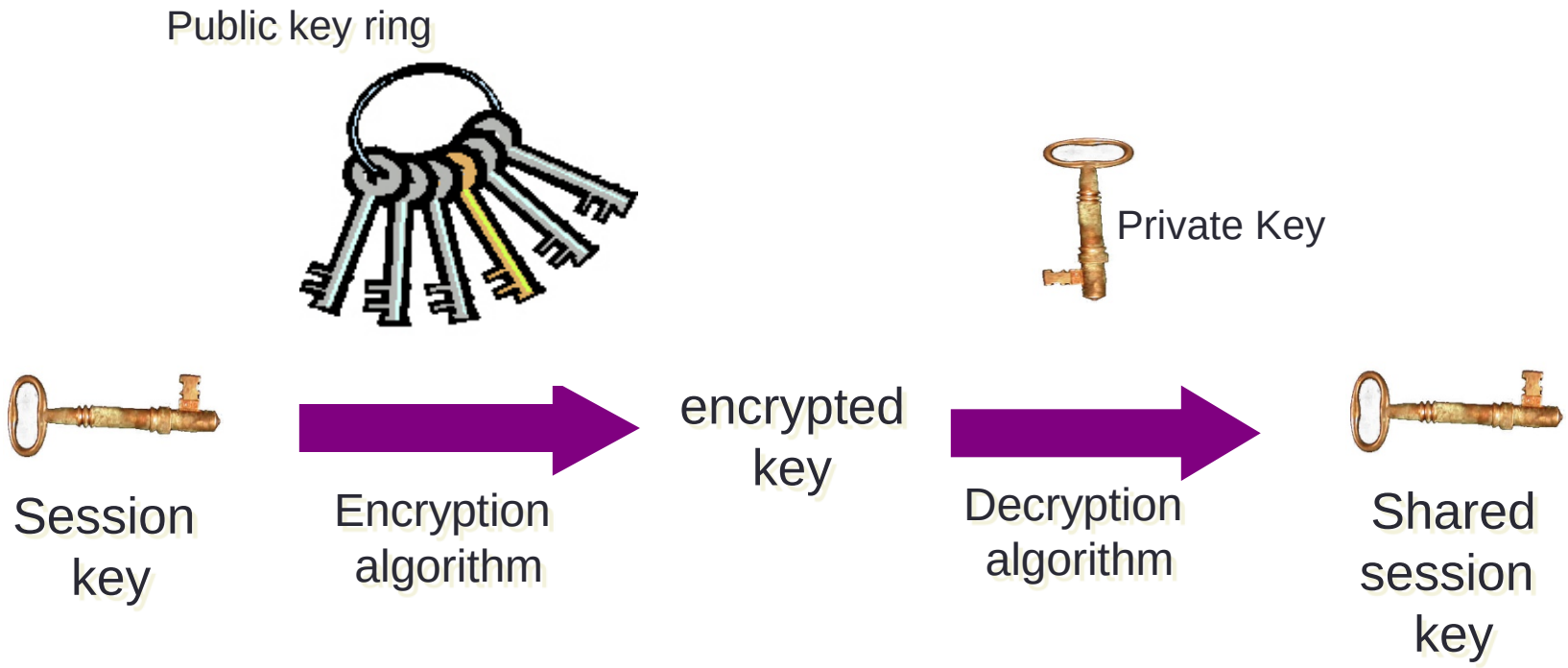
- The sender encrypts using public key of receiver
- Only the receiver can decrypt the cipher message with his private key

Public Key Algorithms



Authentication

Public Key Algorithms



Key Exchange

Integrity

- Encryption protects only against passive attack.
- Integrity
  - A message digest is computed which is appended to message using hash functions.

Hash Functions

A public function that maps a plaintext message of any length into a fixed length hash value used as the authenticator

- Pros
  - One way transformation
  - Offers integrity without the cost of encryption
  - Message can be read when authentication is unnecessary
- Cons
  - No Confidentiality
  - Can be altered by attackers to match altered message

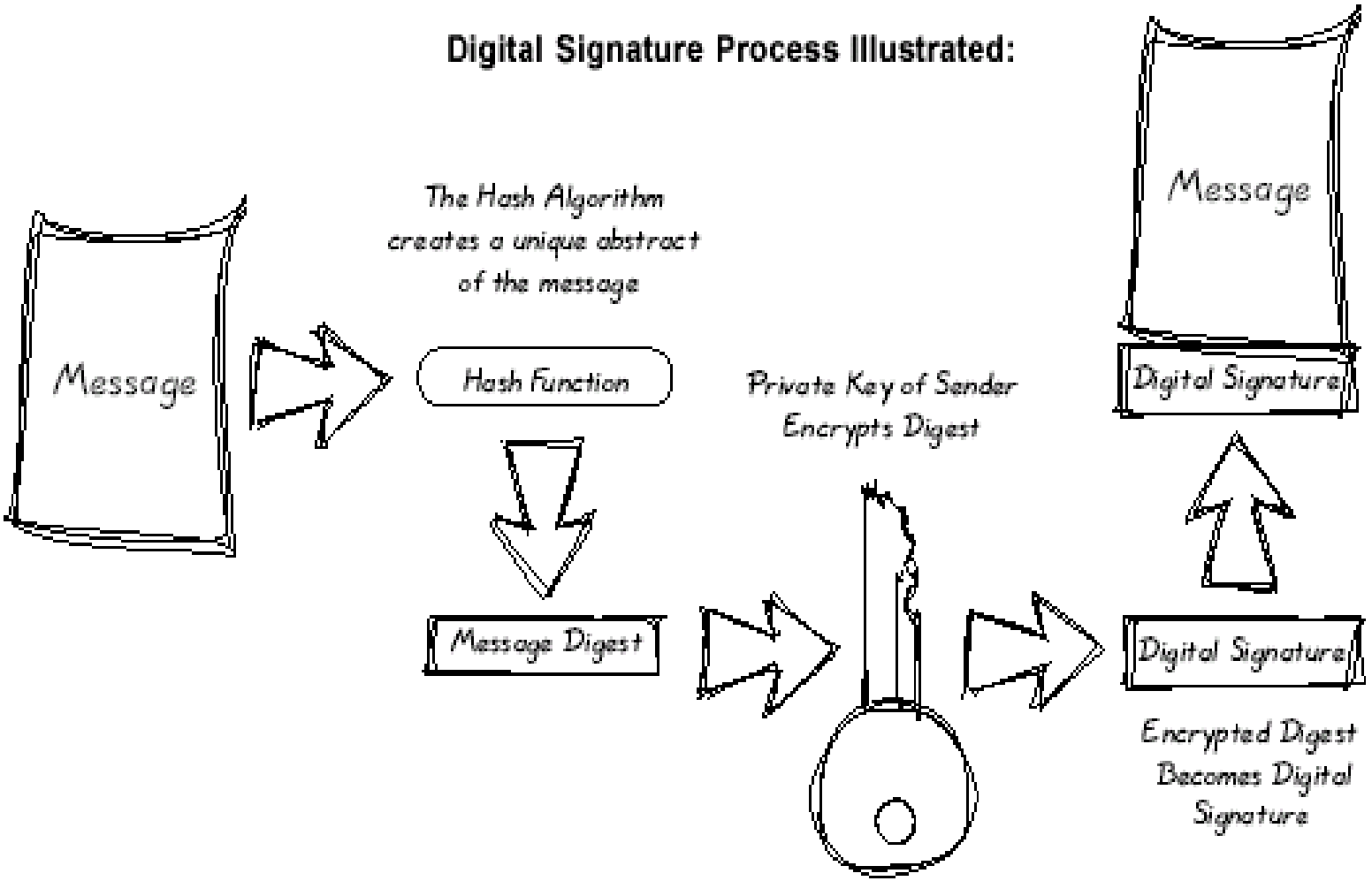
Authentication

Digital Signatures

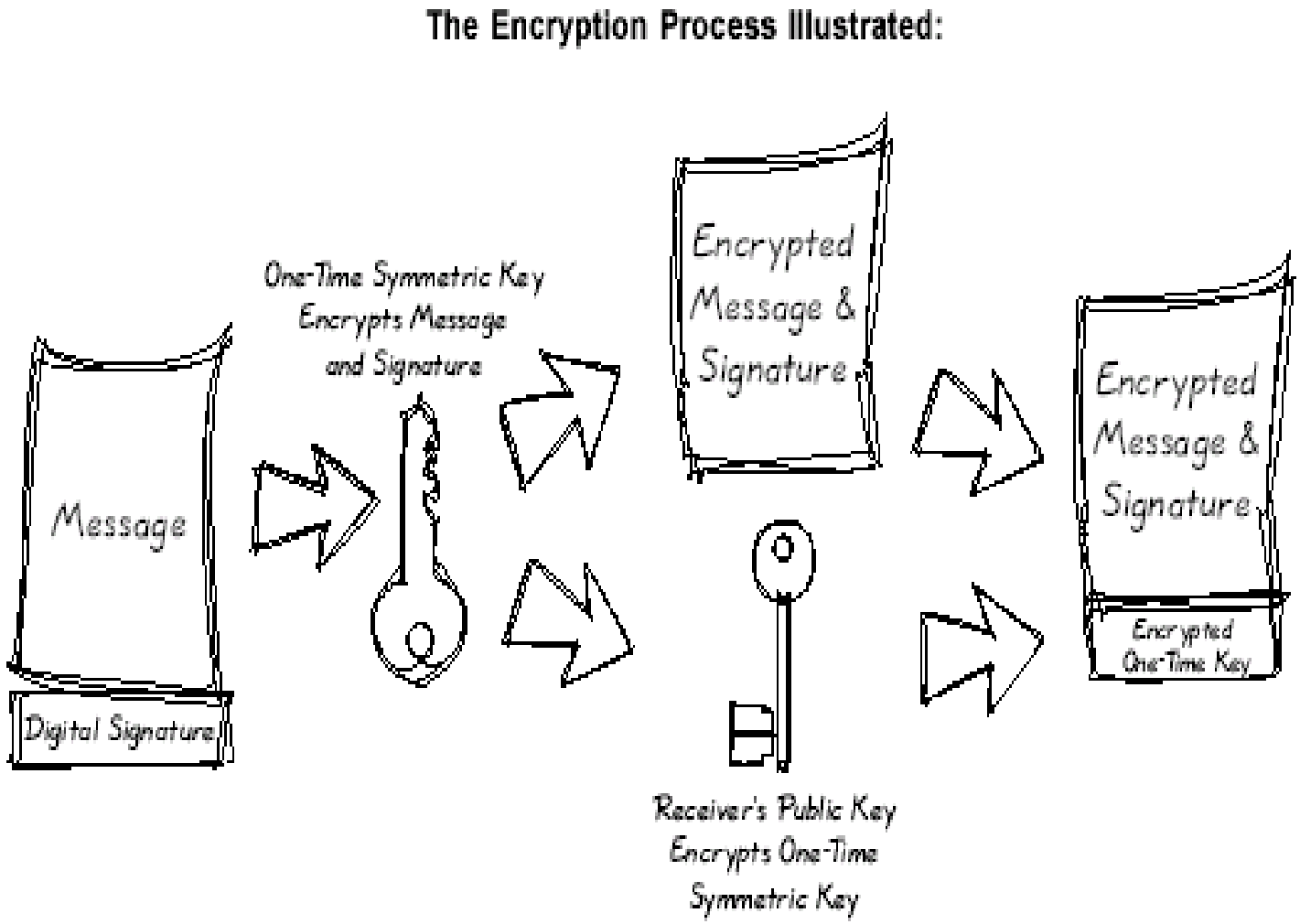
- An authentication mechanism which enables the creator of a message to attach a code that acts as a signature

  - Encrypt a small block of bits that is a function of the document (authenticator), using sender's private key.
  - This serves as signature that verifies origin and content.

Digital Signature Process Illustration



Encryption Process Illustration



Digital Certificates

- An answer to Internet trust problem
- Trusted 3rd parties issue certificates to people or companies who prove their ID

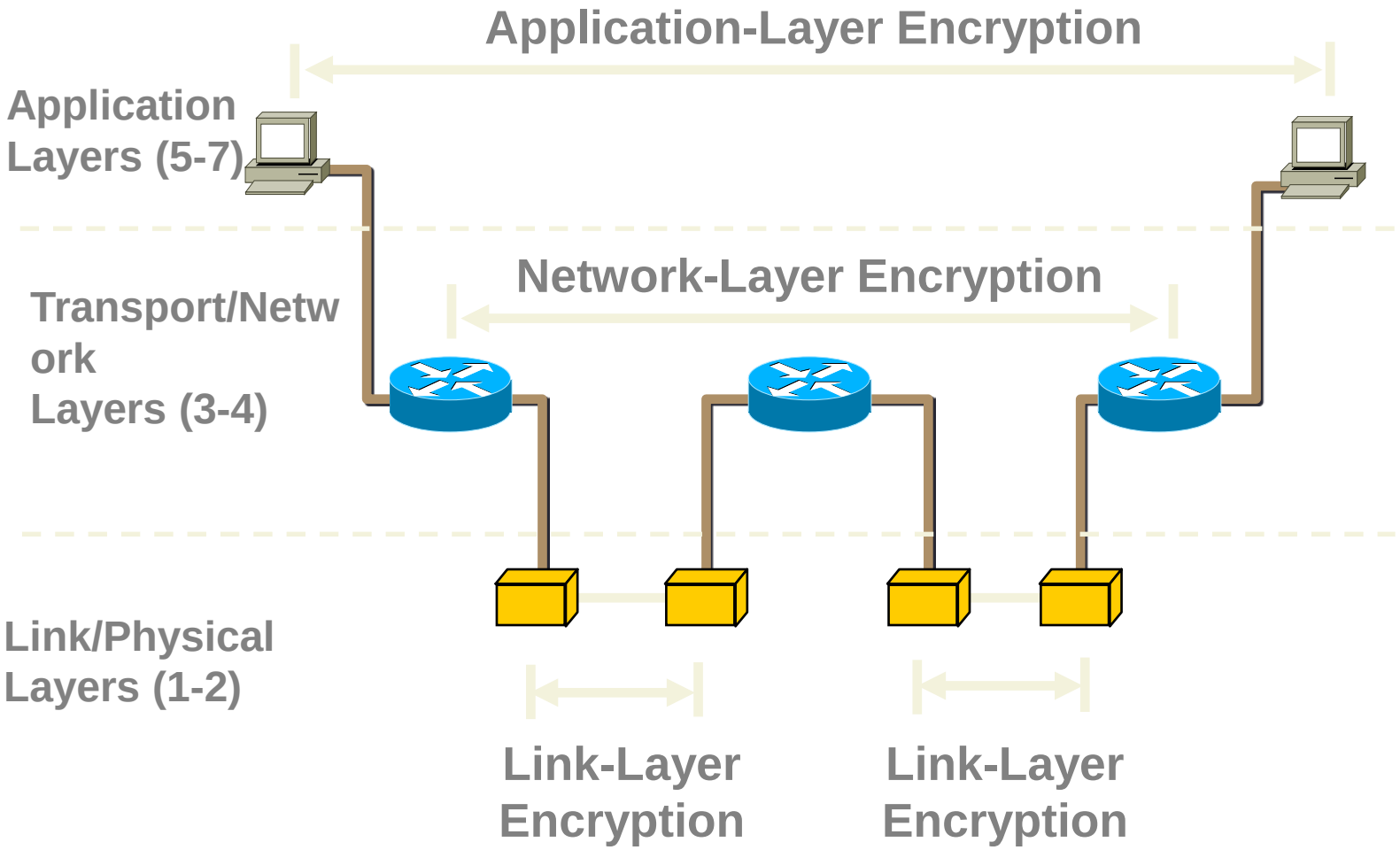
Digital Certificates – Manage key

- Used for distribution of public keys.
- Public key certificate consisting of public key and user ID of key owner is signed by a trusted third party.
- The third party is called Certificate Authority (CA).

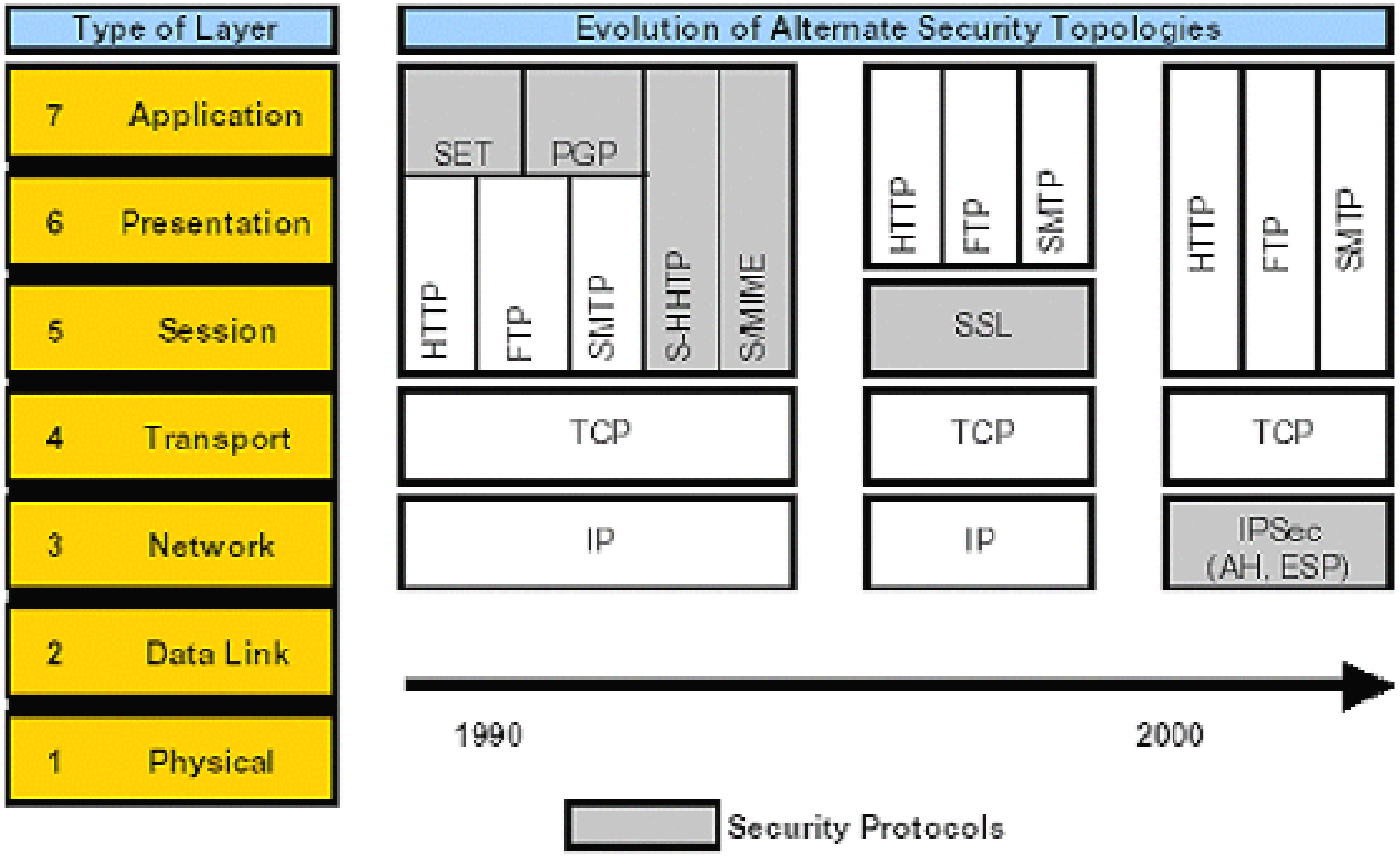
Digital Certificates

- A Digital Certificate typically contains
  - Owner's public key
  - Owner's name
  - Expiration date of the public key
  - Name of the issuer (CA that issued the Digital ID)
  - Serial number of the Digital ID
  - Digital signature of the issuer
  - X.509

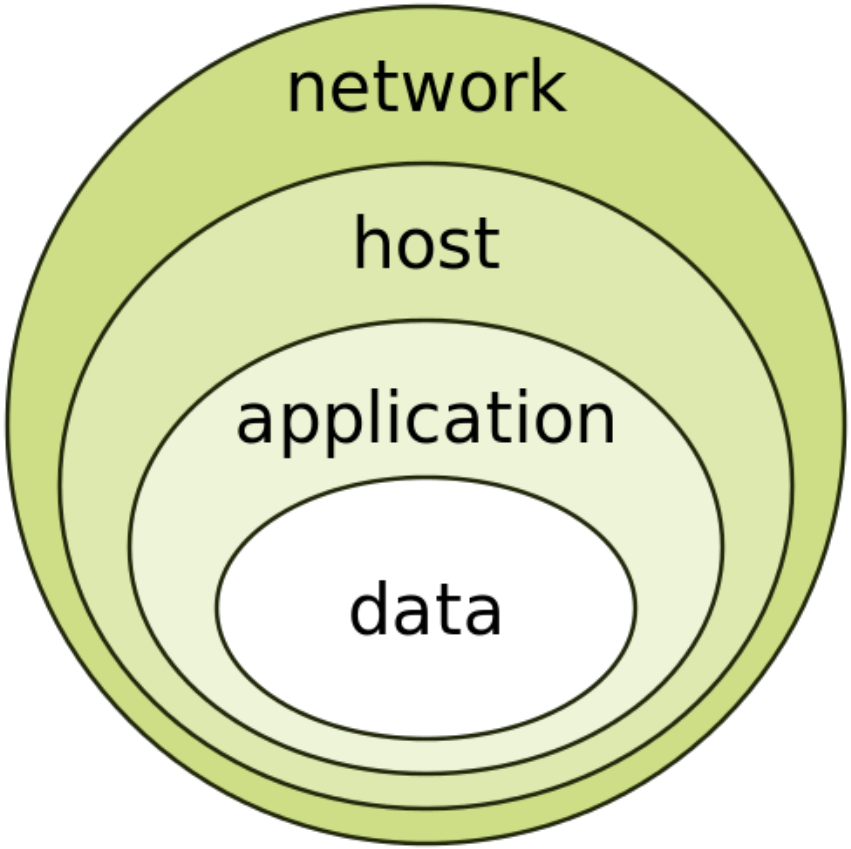
Deployment of Cryptography



Evolution of Security Protocols



Defense in Depth



The onion model of defense in depth

Defense in Depth

- It is protecting information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information
- The information must be protected while in motion and while at rest
- During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems

Defense in Depth

- To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms
- The building up, layering on and overlapping of security measures is called defense in depth

Business Continuity Planning

- It is a process that helps company to recover one of its systems that does not work

- It involves risk assessments and drawing plans, policies and procedures to lessen the impact when a disaster is prominent to the organization IT infrastructure

What are the Disasters that Interrupt Business Operation?

Earthquake

Fire Accident

Tornado

Bomb Exploding

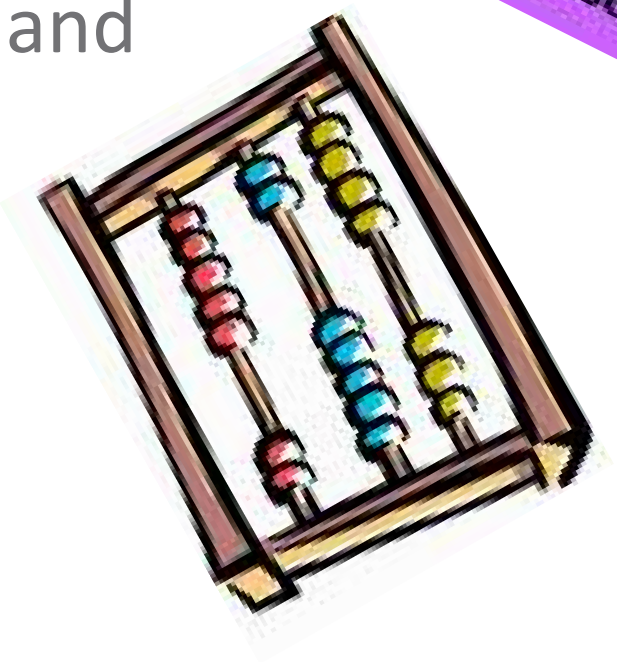
Why it is Needed?

- To reduce the operational risks like
  - System failure
  - Internal or External Threats
  - Ability to meet the services

Who is Responsible for BCP?

Where Did it Come From?

- Evolved from data centres
- From centralized processors and platforms



Examples – Business Continuity

- Staff wages

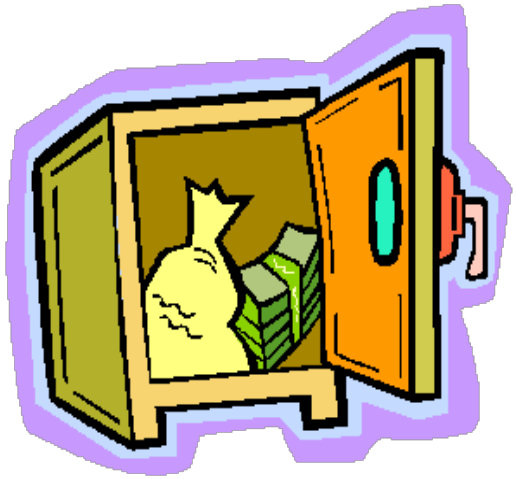
- Call Centre

- Sales

- Manufacture

Business Costs of Data

- The value of data varies among industries like
  - Size of Industry
  - Application and firms of the company



Costs for Data Protection

- Acquisition Cost
- Operational Cost

BCP Goals

- Protect Your
  - People
  - Data
  - vital communications
  - Assets
  - brand and reputation.
- Minimize threats, impacts and downtime.
- Mitigate any losses

What is BCP?

- The continuous businesses / Services
- The process and procedures
- Maintenance of various Operations
- Fight against disasters
- To minimize the loss

Benefits

- Protect from natural and man-made disasters
- Prevent the damages

Features

- Identify critical business processes
- Receive assessment of current threats
- To meet specific needs
- Put effective disaster response in place

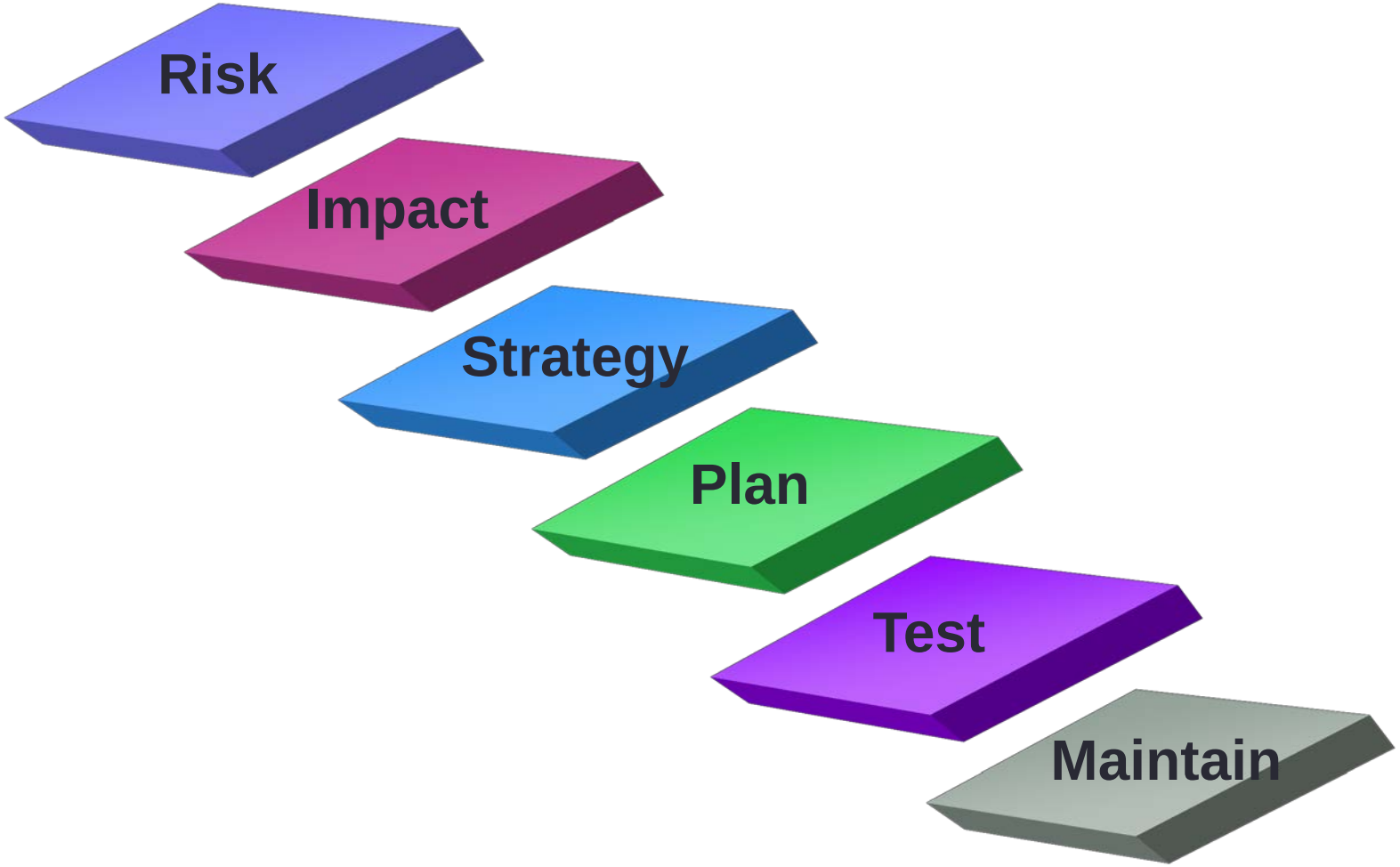
BCP Challenges

- Planning
- Testing
- Modifying
- Approving

Business Continuity Policies

- Determine the fundamental practices
  - values and culture throughout the enterprise
- Linked with information security policies
- Ensures stability and continuity

BCP Model



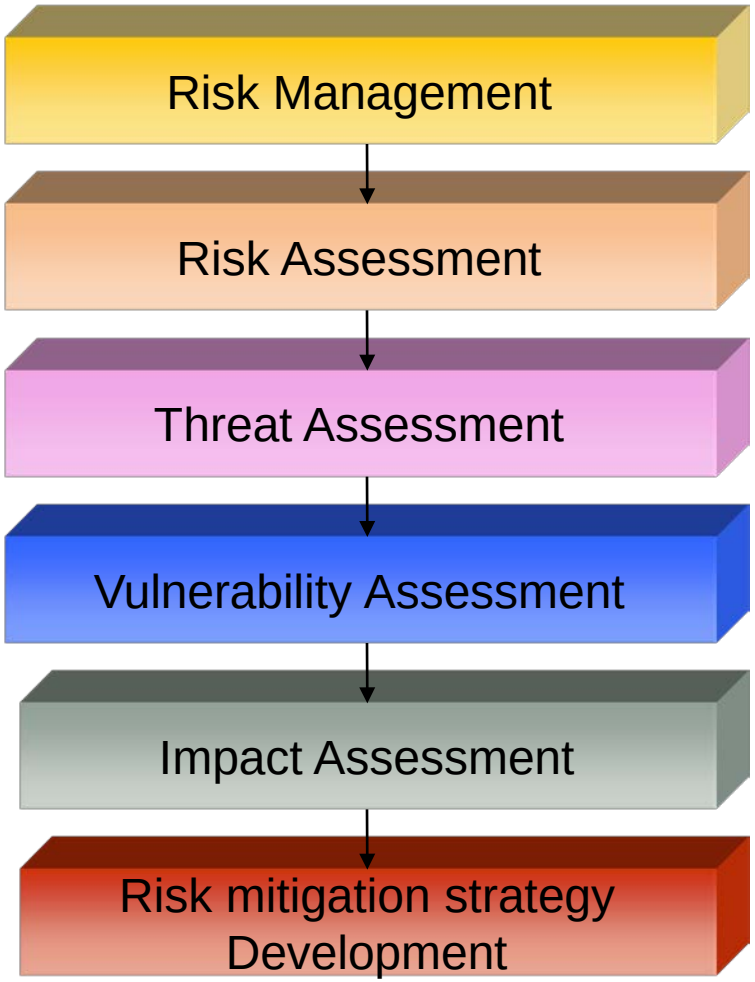
Project Management Initiation

- Establish the need for BCP
- Establish the Project management work Plan
- Prepare and present the initial report to the management
- Establish the members of the BCP Team
- Develop formal meeting schedules
- Prepare and present status reports

Risk Management Process

- How all risks are managed ?
- Thorough risk management plan

Risk Management Process Overview



Risk Management

- Process of
  - Understanding
  - Controlling
  - Minimize the impact of unfortunate events

Risk Assessment

- List assets that might be target
- Look at the vulnerabilities
- Communication countermeasures

Threat Assessment

- Undesired Impact
- Quantitative
- Qualitative

Vulnerability Assessment

- Exploit vulnerabilities
- Prioritize list of threats

Steps in vulnerability analysis

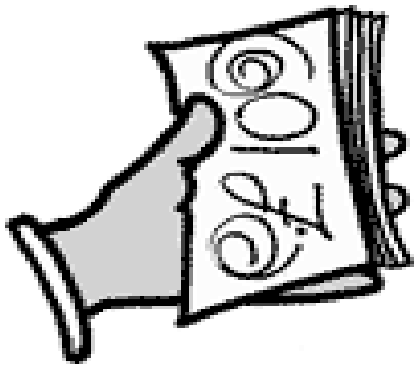
- Identifying and classifying network or system resources
- Prioritizing levels of importance of the resources
- Identifying potential threats to each resource
- Dealing the most serious potential problems first
- Taking steps to minimize the consequences if an attack occurs

Impact Assessment

- Impact on business due to disruption
- Indirect Impact
  - Upstream losses
  - Downstream losses

Risk Mitigation strategy

- Gather your recovery data
- Compare cost of each category
- Reduce adverse effects



Types of Risk Mitigation Strategy

- Risk Acceptance
- Risk avoidance
- Risk Limitation
- Risk Transference

Risk Acceptance

- Accepts Potential consequences
- It is a part of risk management

Risk Avoidance

- Completely avoids risk
- It is a kind of risk bearing
- Expensive strategy

Risk Limitation

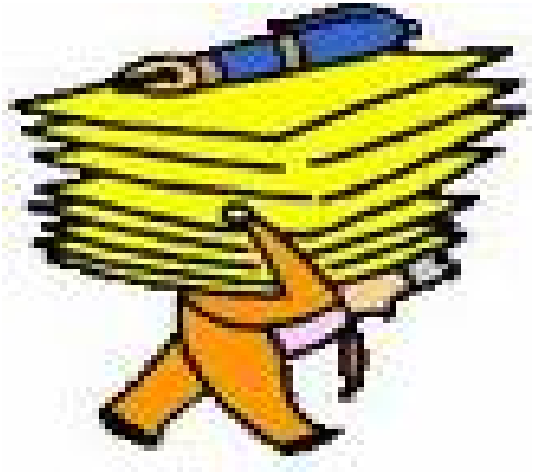
- Limit the risks
- Safe business
- Cost of Implementation is finite

Risk Reduction

- Minimising the effects of disasters
- Protect against earth quakes
- Reduce the likelihood of disaster occurring
- Bridging the gaps between ideas and audience

Risk Transfer

- Burden of risk to someone else
- Transfer of risk to another organization



Ways of Risk Transfer

- Insurance
- Contracts
- Warranties

Risk Evaluation

Prioritize threats

Identify Key Risks

Vulnerability analysis

Disaster Recovery Planning

- Precautions to be taken to minimize effects of
  - Natural calamities
  - Man-made Disaster
- Analysis on
  - Business process
  - Continuity needs

Creating DRP

- Step by step procedure that includes
  - Recovery procedure
  - List of required database
  - Backup details
  - Instructions that you define

Disasters in Varied Forms

Earthquake

Drought

Flood

Why Disaster Management Important?

- Sustainable Livelihoods
- Protection
- Long lasting

Disaster Management

- Disaster Management generally focus to
  - Reduce losses from hazards
  - Assure 100% assistance to victims
  - Achieve effective recovery

Data Storage

- IT recovery storage is done as follows
  - Offsite
  - Hot site
  - Warm site
  - Cold site

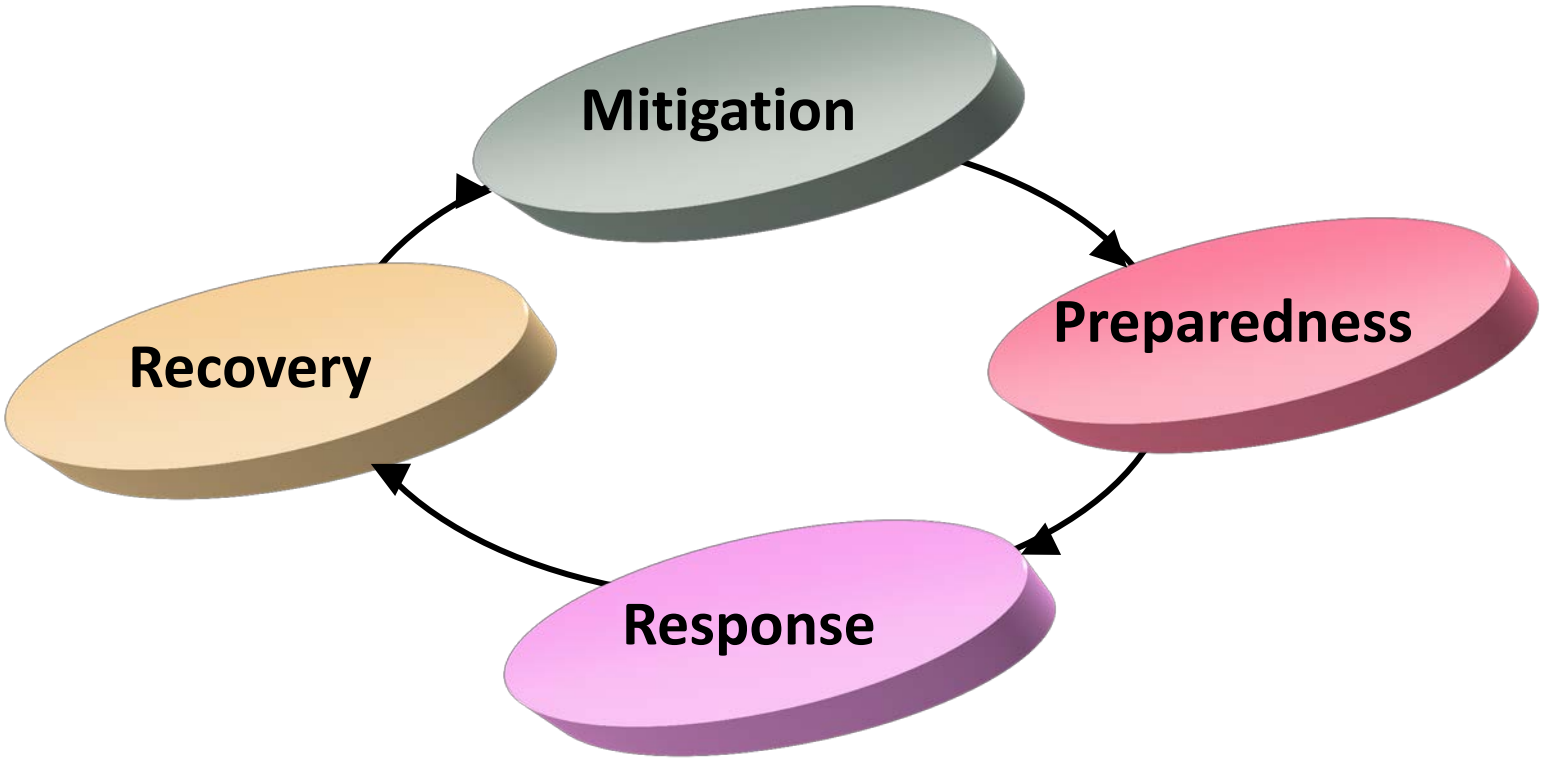
Reactive Disaster Management

- Background
- Objective
- Strategies
- Policy
- Program
- Expected Outcomes

Proactive Disaster Management

- By knowing which countries are most disaster-prone
- The poor are most vulnerable
- Cost of disasters
- Reducing the risk of disasters
- New thinking by governments

DM cycle



Mitigation

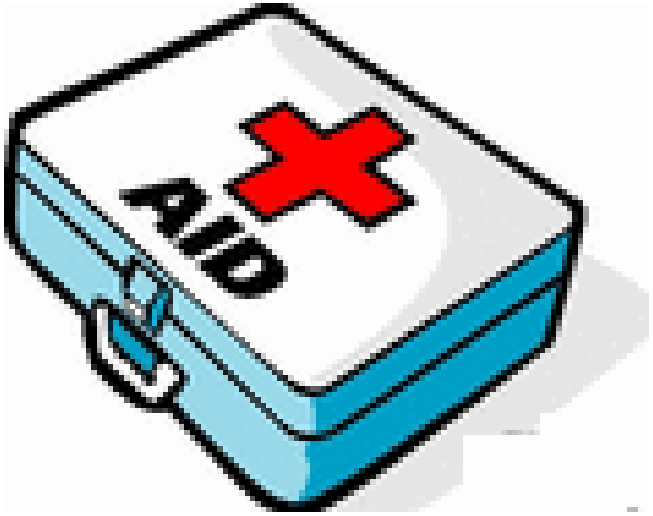
- Reduce the Disaster occurrence
- Vulnerability analysis
- Information on hazards

Preparedness

- Preparedness includes:
  - Emergency kits
  - Development of long term plan
  - Training and awareness

Response

- Response includes basic needs
  - First aid
  - Fire fighting
  - Temporary shelter



Recovery Plan

- Restore lives and infrastructure
- Recover of business
- Continue until normal operations

Disaster DM Team

- Early Warning team
- Event Organizing team
- First aid team
- Security Team

The Major Areas Concern

- Awareness if Disaster
- Disaster Management
- Safety from natural Hazards
- Preparation of Disaster Plans

Incident Response Plan

- Based on the underlying concepts
- When Problem occurs how to respond it
- How to overcome when incident occurs
- Function appropriately in a time of incident
- Should consider positive and negative steps for building proper incident response plan

Incident Response

- To provide immediate assistance
- Support the affected People
- Initials repairs to damaged Infrastructure

Determining your Recovery needs

- Determine the business needs
- Determine recovery Objective

How to Prevent Disasters

- Protecting the Equipment
- Providing continues Power supply
- Protecting Internet Access
- Practice the Disaster Plans
- Alternative Communication

Steps to Take Before Disaster

- Plan reinforced regularly in staff meetings
- Update at least annually.
- Reassign duties

Steps to Take When Disaster Looming

- Do not delay
- Confirm employees know their role
- Safety of employees and office

Contd

- Use your phone tree.
- Recorded message
- Backup number
- What staff should do if they are unable to meet their assignment

Steps to Take After Disaster

- Do an assessment
- Assist them as you can
- Alternative location