| Term 1 | Term 2 | Term 3 | Term 4 |
|---|---|---|---|
| **12.1A Artificial intelligence**<br>• Artificial intelligence<br>• Virtual and augmented reality | **12.2A Information security**<br>• Data protection measures<br>• Methods of information systems protection<br>• Methods of intellectual property protection | **12.3A Computer systems**<br>• OS types<br>• CPU architectures<br>• Memory addressing principle<br>• System bus<br>• Fetch-execute cycle<br>• Boolean logic | **12.4AREVISION** |
| **12.1B Programming paradigms**<br>• Declarative and imperative programming languages<br>• Expert systems<br>• Program compilation stages | **12.2B Creating documentation**<br>• Making a text document<br>• Formatting a text document<br>• User e-sources to check for plagiarism | **12.3B Data presentation**<br>• Number representation methods<br>• Addition and multiplication of binary numbers<br>• Stacks and queues<br>• Binary tree | |
| **12.1C System testing**<br>• Types of test data<br>• Types of errors | **12.2C System implementation**<br>• Methods of system implementation<br>• New system implementation | **12.3CCommunication and networks**<br>• Internet and the World Wide Web<br>• OSI models<br>• Channel switching and packet switching<br>• Packet routing | |


# CLASS DISCUSSION

In our daily lives we find ourselves working with massive amounts of data, either on personal level or business/organizations.

In what ways, do we protect data?

# *Ways we protect data.*

- Install an Antivirus
- Take Regular Backup of Your Data
- Install a Firewall
- Use Complex Passwords
- Biometrics
- Use Encryption Software
- Update Your Software
- Secure Mobile Devices
- Protect Wireless Networks
- Disk mirroring
- Keep an Eye on Suspicious Activity
- Educate Your Team
- Physical protection

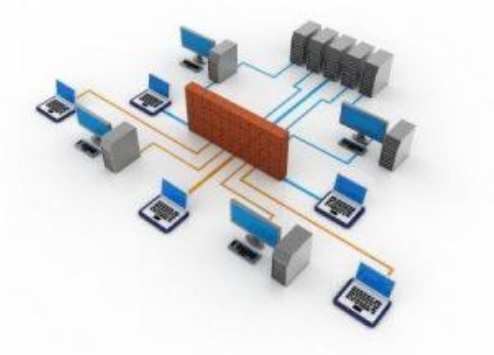
# Data protection measures



**Lesson objective:**

Understand and be able to explain a range of security measures, including:

- **Physical risks,**
- **Inter-network screens**,
- **Biometrics**


# Introduction to Data Protection

- **Why Data Protection Matters**: Protects sensitive information (e.g., personal data, financial records) from unauthorized access, loss, or damage.
- **Relevance**: Increasing cyber threats, legal requirements (e.g., GDPR), and organizational trust.
- **Key Measures**: Physical security, inter-network screens, encryption, biometrics, virus protection.

# Physical risks

- Threats to hardware and data from physical events.

Theft, fire, floods, power surges, unauthorized physical access.

Protection Measures:

- Secure server rooms with locks and alarms.
- Fireproof safes for backups.
- Uninterruptible Power Supplies (UPS) for power stability.

# Pair Activity

How do the following affect the data and how do we mitigate them

1. Scratches on the hard disk
2. Theft of equipment
3. Fire, floods and lightning damage

# Physical risks

1. Scratches on the hard disk
- Platters spin rapidly with a "head" reading data.
- Improper shutdown may cause head crashes and scratches.
- Scratches can damage data, making it inaccessible.

Protect measures:

- Shut down properly to avoid head crashes.
- Handle drives carefully, avoiding shocks.
- Back up data to external or cloud storage.

**2. Theft of equipment**

- Computers are valuable and theft targets.
- Stolen devices without backups lose all data.

Protect measures:

- Use locks or safes to secure devices.
- Keep devices hidden in public.
- Back up data off-site or to the cloud; use encryption.

## 3. Fire, floods and lightning damage

- Can severely damage or destroy equipment.
- Backups kept onsite may also be lost.
- Fire, flood, or lightning can damage backups too.

Protect measures:

- Store backups off-site or in the cloud.

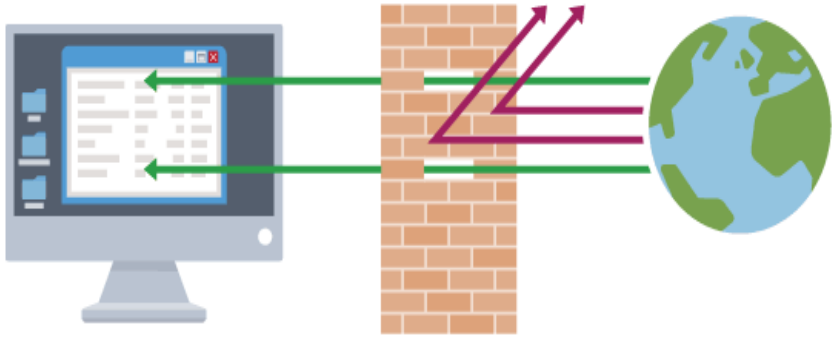
- Use surge protectors against lightning.

- Install fire/water detection; use fireproof storage.

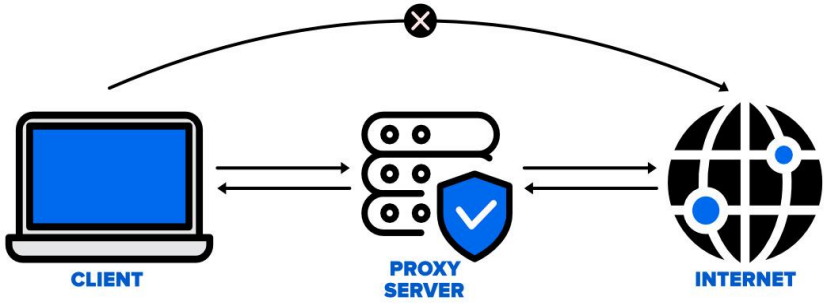
- Test and update backup plans regularly.

# DATA SECURITY MEASURE

- Firewall

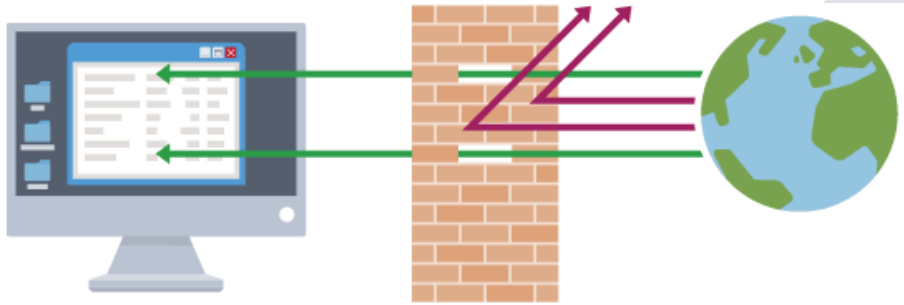


- Proxy server




- Biometrics

# FIREWALL



* A firewall is a hardware or software program that protects a computer network by **monitoring and controlling incoming and outgoing data**. **OR**

* Software or hardware that **filters** network traffic to prevent unauthorized access.

Types include Packet-filtering, stateful inspection, proxy firewalls.

How They Work: Monitor incoming/outgoing traffic based on **predefined rules.**

Blocking malicious IP addresses attempting to access a network.

# Activity (group work)

Research on the following: Create a Poster

Group 1 - Firewall
Principle of Operation
Advantages (4)

Group 2 – Firewall
Principle of Operation
Disadvantages (4)

Group 3 – Proxy-server
Principle of Operation
Advantages (4)

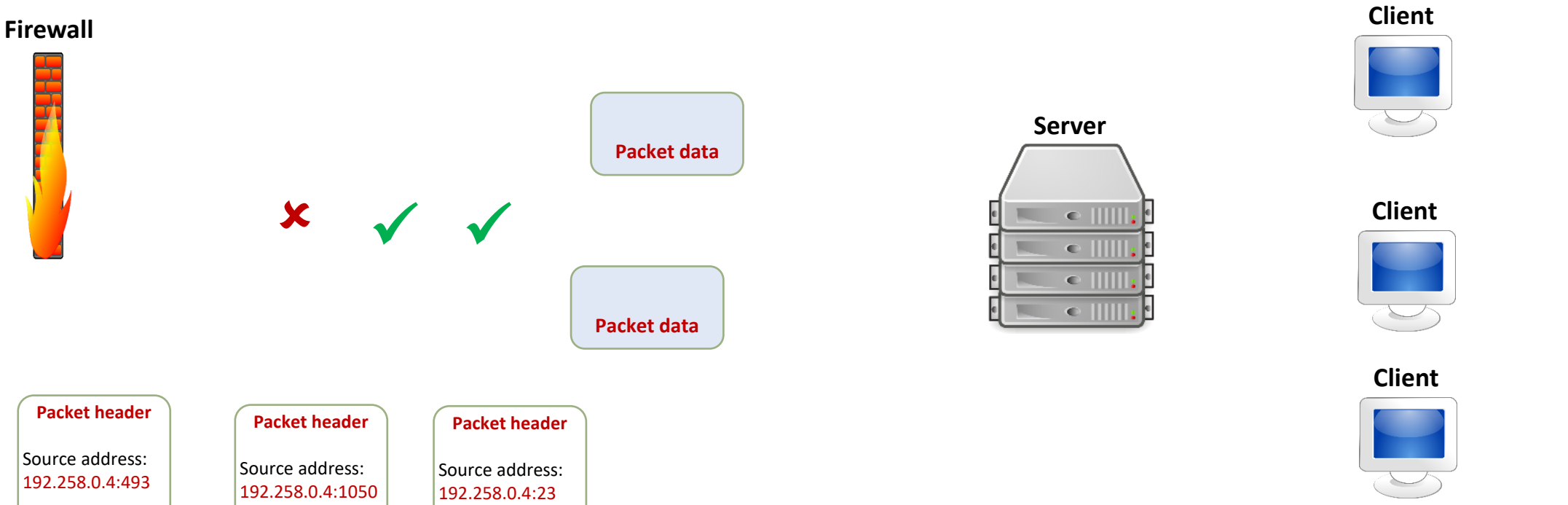
Group 4 – Proxy-server
Principle of Operation
Disadvantages (4)

**success criteria**

Understand how a firewall works (packet filtering, proxy server, stateful inspection)

1. Construct a diagram using the following, adding any additional arrows, annotations etc. you feel are needed to explain the following concept:

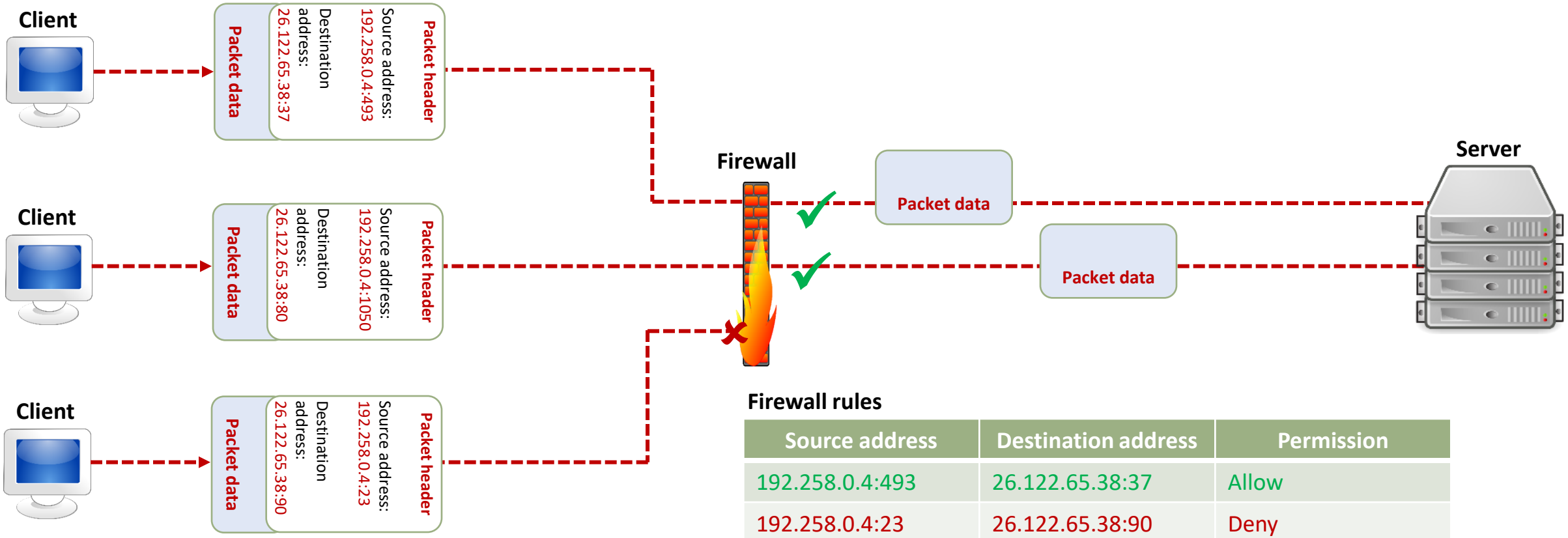
## Packet filtering




| Source address | Destination address | Permission |
|---|---|---|
| 192.258.0.4:493 | 26.122.65.38:37 | Allow |
| 192.258.0.4:23 | 26.122.65.38:90 | Deny |
| 192.258.0.4:1050 | 26.122.65.38:80 | Allow |

1. Construct a diagram using the following, adding any additional arrows, annotations etc. you feel are needed to explain the following concept:

## Packet filtering




**Firewall rules**

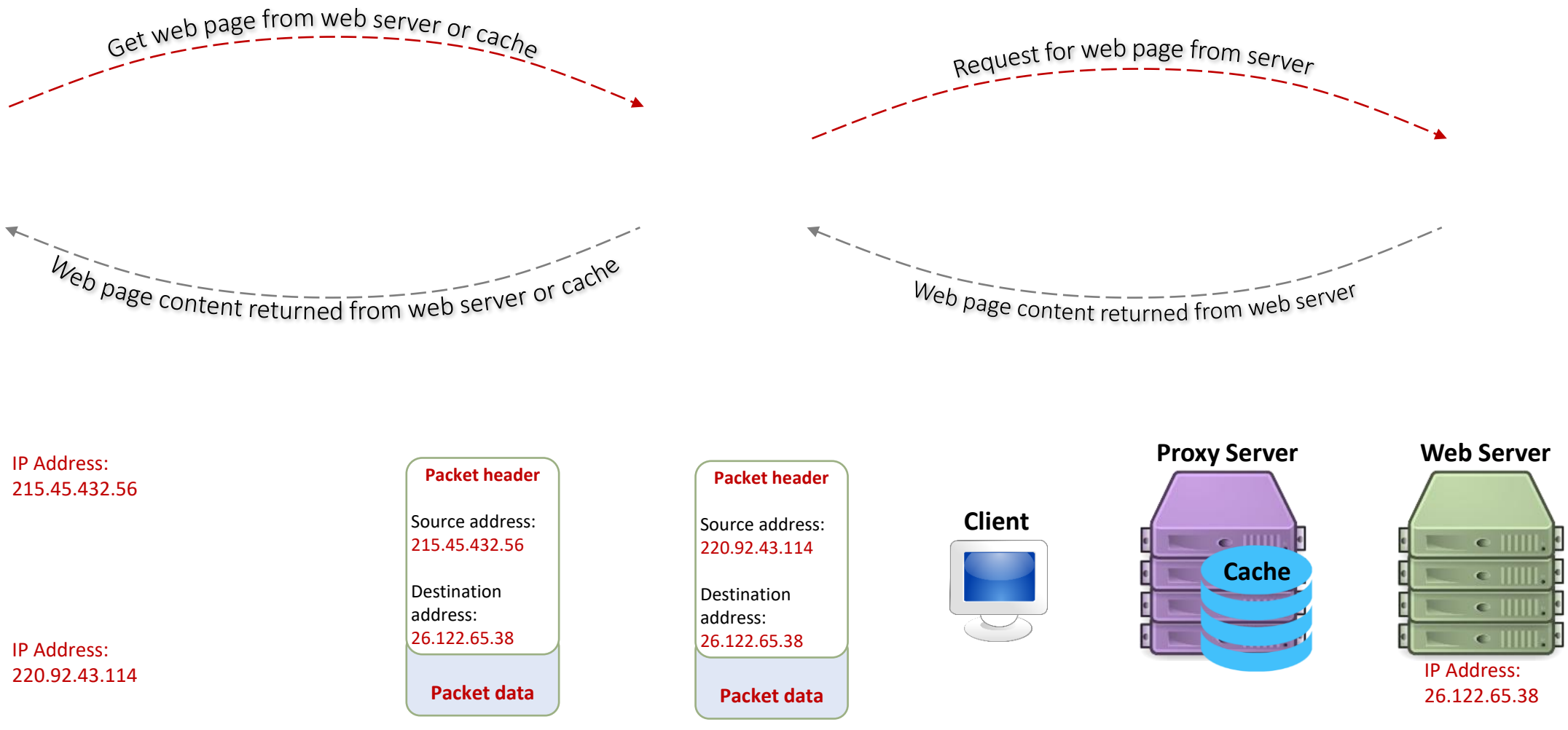
| Source address | Destination address | Permission |
|---|---|---|
| 192.258.0.4:493 | 26.122.65.38:37 | Allow |
| 192.258.0.4:23 | 26.122.65.38:90 | Deny |
| 192.258.0.4:1050 | 26.122.65.38:80 | Allow |

**success criteria**

Understand how a firewall works (packet filtering, proxy server, stateful inspection)

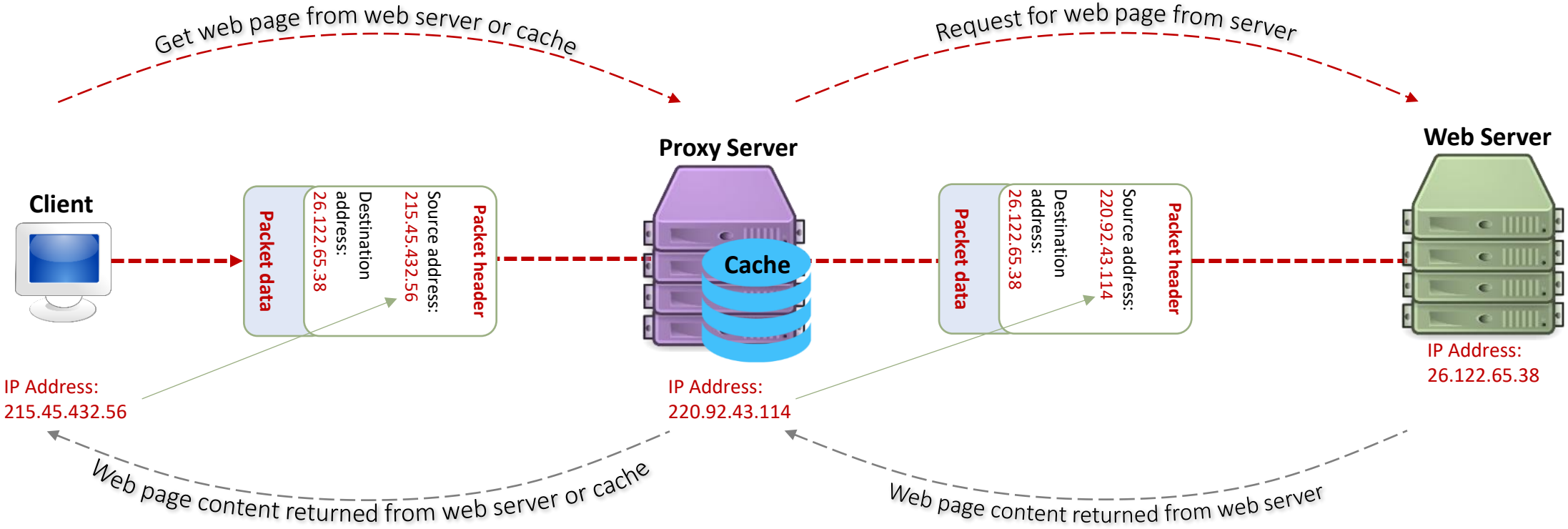
2. Construct a diagram using the following, adding any additional arrows, annotations etc. you feel are needed to explain the following concept:

## Proxy servers



2. Construct a diagram using the following, adding any additional arrows, annotations etc. you feel are needed to explain the following concept:

# Proxy servers

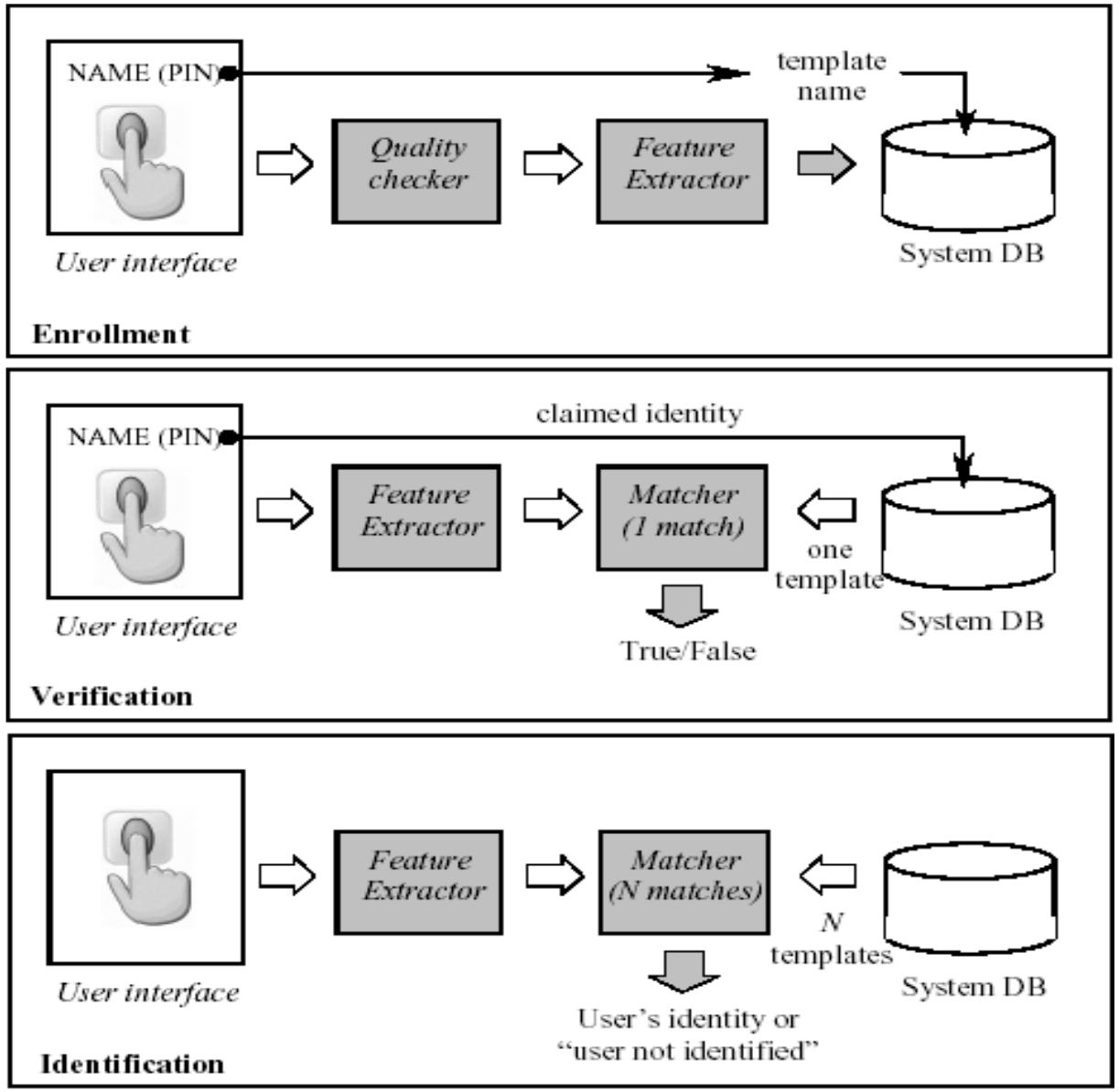


# BIOMETRICS

Biometrics use **unique** physical or behavioral characteristics—like fingerprints, face, voice, or iris patterns—to recognize individuals.

- Ensure Enhanced security and safety
- Identify an Individual Uniquely
- Verify the identity of an individual who he claims to be
- Provide access to high security zones/areas to authorized individuals
- Identify criminals and prove them guilty beyond doubt

# How a biometric works?




**Enrollment:**

The biometric system scans or captures a unique trait (e.g., a fingerprint) and creates a **digital template**. This template is a mathematical model, not a direct image, of the biometric data and saved into a **secure database**.

**Verification:**

The system checks if a person is who they claim to be by comparing their live biometric data with the stored template. Use of smart phones (*one-to-one* comparison).

**Identification:**

The system searches the entire database to find a matching template **without knowing** the person's identity upfront. Thief identification / airports-ins (*one-to-many* comparison).

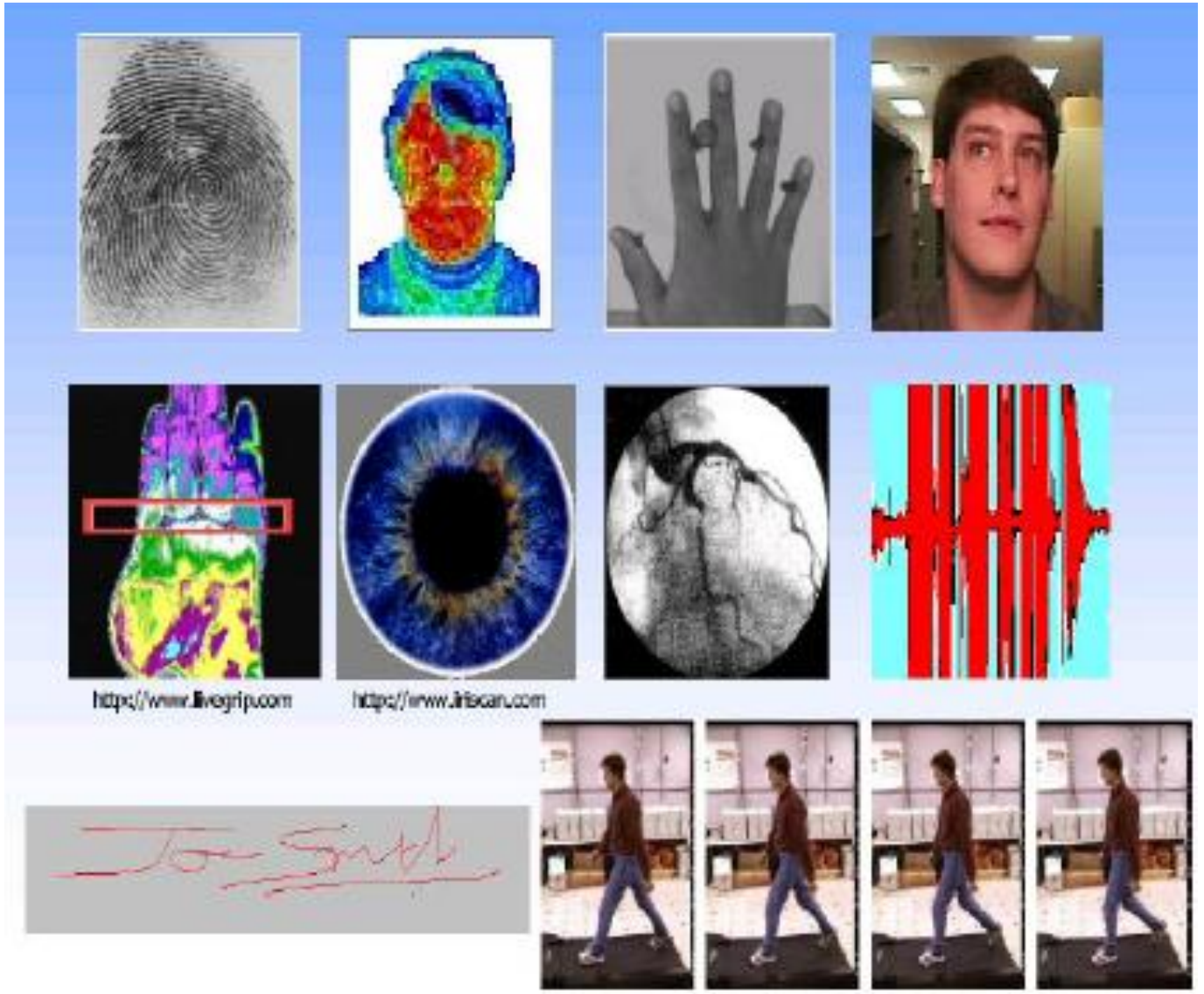
# Types of Biometrics

**Physical:**

- Fingerprints
- Hand Geometry
- Retina Scanning
- Iris Scanning
- Facial Recognition
- DNA Matching
- Ear Shape Recognition

**Behavioural:**

- Signature  recognition
- Voice Recognition
- Key Stroke Pattern
- Gait(Body Dynamics)



# Face Recognition – Strengths & Weaknesses

Based on Relative position and shape of nose, position of cheekbones…

## Strengths

- It's contactless and quick, requiring only a glance, making it easy for users.
- Face recognition can work from a distance, making it suitable for public spaces like airports.
- It can be used in various scenarios, from unlocking phones to law enforcement

## Weaknesses

- Low accuracy
- Very sensitive to light changes, angles and image quality
- Faces change with age
- Facial Appearances can be changed
- Storing biometric data poses a security risk

# Research Task. Work in pairs.

## Define strengths & weaknesses of the following types of Biometrics

- **Iris Recognition**
- **Retinal Scanning**
- **Hand Geometry**
- **DNA**
- **Voice Recognition**
- **Fingerprints**

# Computer Security

Encryption and Data Backup

# Decipher the following coded message

1st word

5 14 3 18 25 16 20 9 15 14

2nd word

1 14 4

3rd word

4 1 20 1 12 15 19 19

4th word

12 5 19 19 15 14

# Objectives

At the end of the lesson students should be able to

- Define the term encryption
- State the purpose of encryption
- Describe the two types of encryption keys
- Describe what is a digital signature
- Explain in detail the concepts of digital certificate
- Describe data protection measures such as data backup and disk mirroring

# Encryption


Process of converting readable data into unreadable characters so that only authorized parties can read or access the data

The unencrypted, readable text is called **plain text**.

The encrypted (scrambled) data is called **cipher text**.

It uses **complex algorithms** to scramble the data being sent.

The security effectiveness is determined by the **strength** of the algorithm and the **length** of the key.

Encryption makes information unreadable to an unauthorized party therefore the information remains private and confidential, whether being **transmitted** or **stored** on a system.


Encryption technology can provide assurance of data integrity as some algorithms offer protection against forgery and tampering.

The ability of the technology to protect the information requires that the encryption and decryption keys be properly managed by authorized parties.

# Activity 1 – 20 min

In groups research on the following concepts

- Asymmetric key Encryption
- Symmetric Key Encryption
- Digital Signature
- Digital Certificate

Outlines the
- ✓ Process
- ✓ Advantages and disadvantages
- ✓ Give examples of how each is used (Use provided keys for demonstration)

Outlines
- ✓ What it is
- ✓ Purpose of DS/DC
- ✓ what information is contained in each document

(Demonstrate the process when sending message)

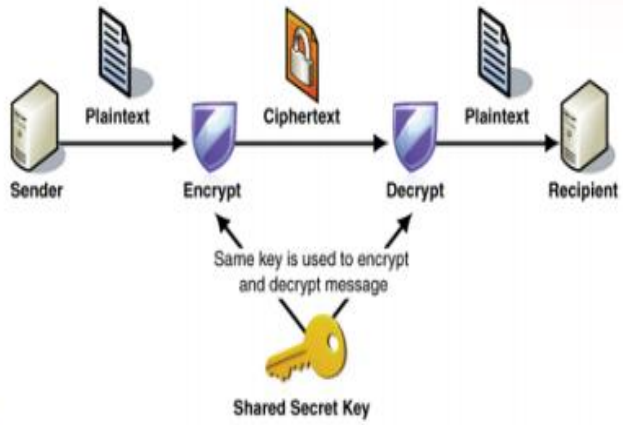
Present your findings by creating a PPT of not more than 5 slides

# Presentation
# Encryption keys

# Two types of Encryption

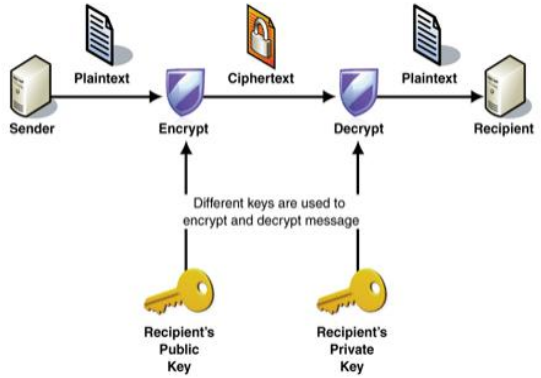
## Private key also called Symmetric Key Encryption

- Both the originator and the recipient use the **same secret key** to **encrypt** and **decrypt** the data.
- One key is needed to encrypt a message and same key is needed to decrypt a message.
- Key distribution is a security problem The sender has to supply the key to the recipient which can be intercepted by a hacker



## Public key Encryption, also called Asymmetric key


- Uses two encryption keys: a public key and a private key.
- Public key encryption software generates both *the private key and the public key*.




- A message encrypted with a public key can be decrypted only with the corresponding private key, and vice versa.
- The public key is made known to message originators and recipients but the private key is only known by the computer user.

# Presentation
# Digital Signature and Digital Certificate

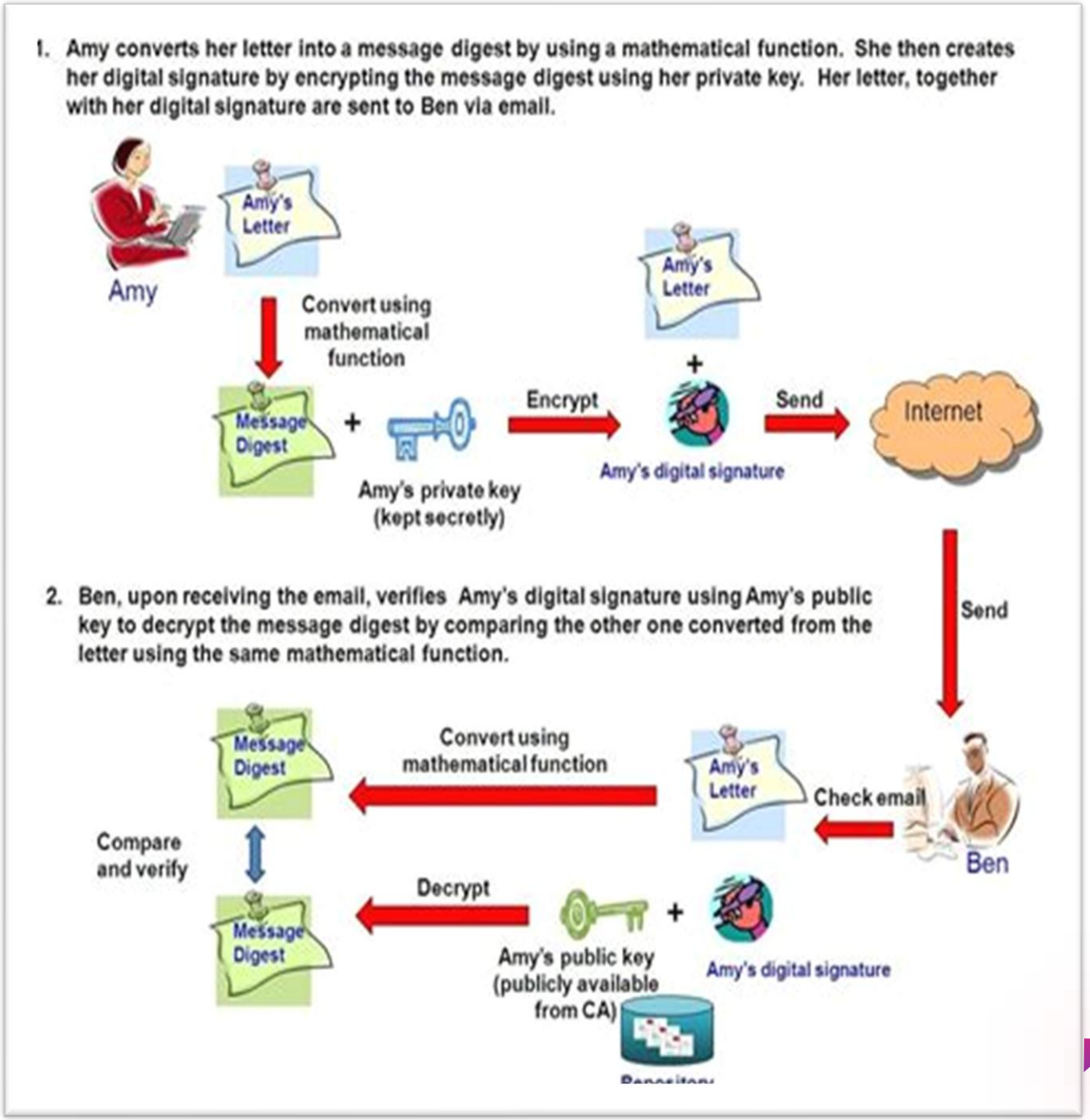
# Digital Signatures


**A digital signature is a** specific type of electronic **signature** that requires the signer to authenticate their identity using a certificate-based **digital** ID.

The **digital certificate** is generally issued by an independent Certificate Authority (CA), which verifies the identity of the signer before issuing the certificate.

It is an encrypted code that a person, web site, or organization attaches to an electronic message to verify the identity of the message sender.

**A digital signature is used to verify that the content of a message has not changed.**




# Digital Signatures

The code usually consists of the user's name and a hash of all or part of the message.

Receivers of the message decrypt the digital signature by generating a new hash of the received message and compares it with one in the digital signature to ensure they match. Digital signatures often are used to ensure that an impostor is not participating in an Internet transaction. That is, digital signatures help to prevent e-mail forgery.

# Digital Certificate

is an electronic "password" that allows a person, organizaion to exchange data securely over the Internet using the public key infrastructure (PKI).


Digital Certificate is also known as a **public key certificate** or **identity certificate.**

# Digital Certificate Characteristics

- **Identification / Authentication:** The person who we are communicating with are who they are
- **Confidentiality:** The information within the message or transaction is kept confidential. It may only be read and understood by the intended sender and receiver
- **Integrity:** The information within the message or transaction is not tampered accidentally or deliberately with en-route without all parties involved being aware of the tampering
- **Non-Repudiation:** The sender cannot deny sending the message or transaction, and the receiver cannot deny receiving it
- **Access Control:** Access to the protected information is only realized by the intended person or entity

# Contents of a  Digital Certificate

- **Subject Name** - "subject" refers to the site represented by the cert.
- **Information about the certificate issuer/certificate authority (CA)** - The CA is the body that issued and signed the certificate.
- **Serial number** - this is the serial number assigned by the issuer to this certificate. Each issuer must make sure each certificate it issues has a unique serial number.
- **Validity period** - certificates aren't meant to last forever. The validity period defines the period over which the certificate can still be deemed trustworthy.
- **Signature** -  This is the digital signature of the entire digital certificate, generated using the certificate issuer's private key
- **Signature algorithm** - The cryptographic signature algorithm used to generate the digital signature (e.g. SHA-1 with RSA Encryption)
- **Public key information** - Information about the subject's public key. This includes:
  - the algorithm (e.g. Elliptic Curve Public Key),
  - the key size (e.g. 256 bits),
  - the key usage (e.g. can encrypt, verify, derive), and
  - the public key itself