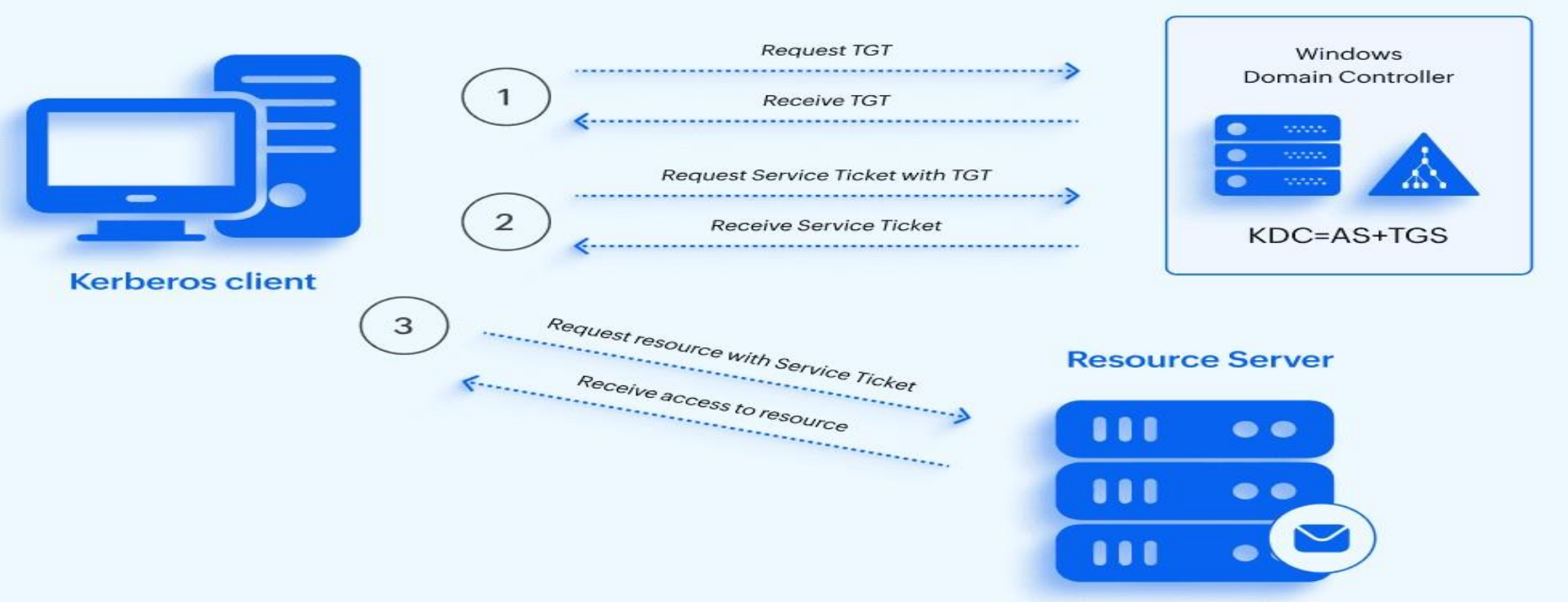
Unit – II (Authentication Applications)

Authentication Application

- Kerveros
- X.509
- Directory Authentication Service
- Pretty Good Privacy
- S/Mime

Kerberos – Applications

Kerberos is a **secure network authentication protocol** that uses **tickets** and **secret keys** to verify users and services without sending passwords over the network.



KDS= (Key Distribution Center)
AS=(Authentication Server)
TGS=(Ticket Granting Server)

Kerberos Authentication Process

This diagram shows **how Kerberos works** to securely authenticate a user and give access to a service **without sending the password again and again**.

There are **three main parts**:

- **Kerberos Client** → User's computer
- **KDC (Key Distribution Center)** → AS + TGS (inside Windows Domain Controller)
- **Resource Server** → File server, mail server, database, etc.

Step 1: Request TGT (Login Step)
Client → Authentication Server (AS)

- User logs in with **username & password**
- Client requests a **Ticket Granting Ticket (TGT)** from AS
- Password is **not sent directly**
- AS verifies the user

AS sends TGT back to the client
(TGT proves the user is authenticated)

Step 2: Request Service Ticket

- **Client → Ticket Granting Server (TGS)**
- Client sends **TGT** to TGS
- Requests a **Service Ticket** for a specific service (file server, mail server)

TGS sends Service Ticket
(Service Ticket allows access to that service)

Step 3: Access Resource Server

- **Client → Resource Server**
- Client sends **Service Ticket** to the Resource Server
- Server verifies the ticket
- **Access is granted**
  User can now use the service (files, emails, database)

Drawbacks of Kerberos

- **Single Point of Failure**
  - If the **KDC (Key Distribution Center)** fails, authentication stops for all users.
- **Time Synchronization Required**
  - All systems must have **same time** (clock skew causes login failure).
- **Complex Setup**
  - Installation and configuration are **difficult**, especially in large networks.
- **Not Suitable for Small Networks**
  - Overhead is high for small or simple systems.
- **Password Dependency**
  - Weak user passwords can reduce security.

Types (Versions) of Kerberos

Kerberos has evolved over time. The main **versions of Kerberos** are:

1. Kerberos Version 4 (V4)

•One of the **earliest versions**
•Supported only **single domain**
•Had security and scalability issues
•**Now obsolete (not used)**

Limitations:

•Weak encryption
•No support for cross-realm authentication
•Platform dependent

2. Kerberos Version 5 (V5)

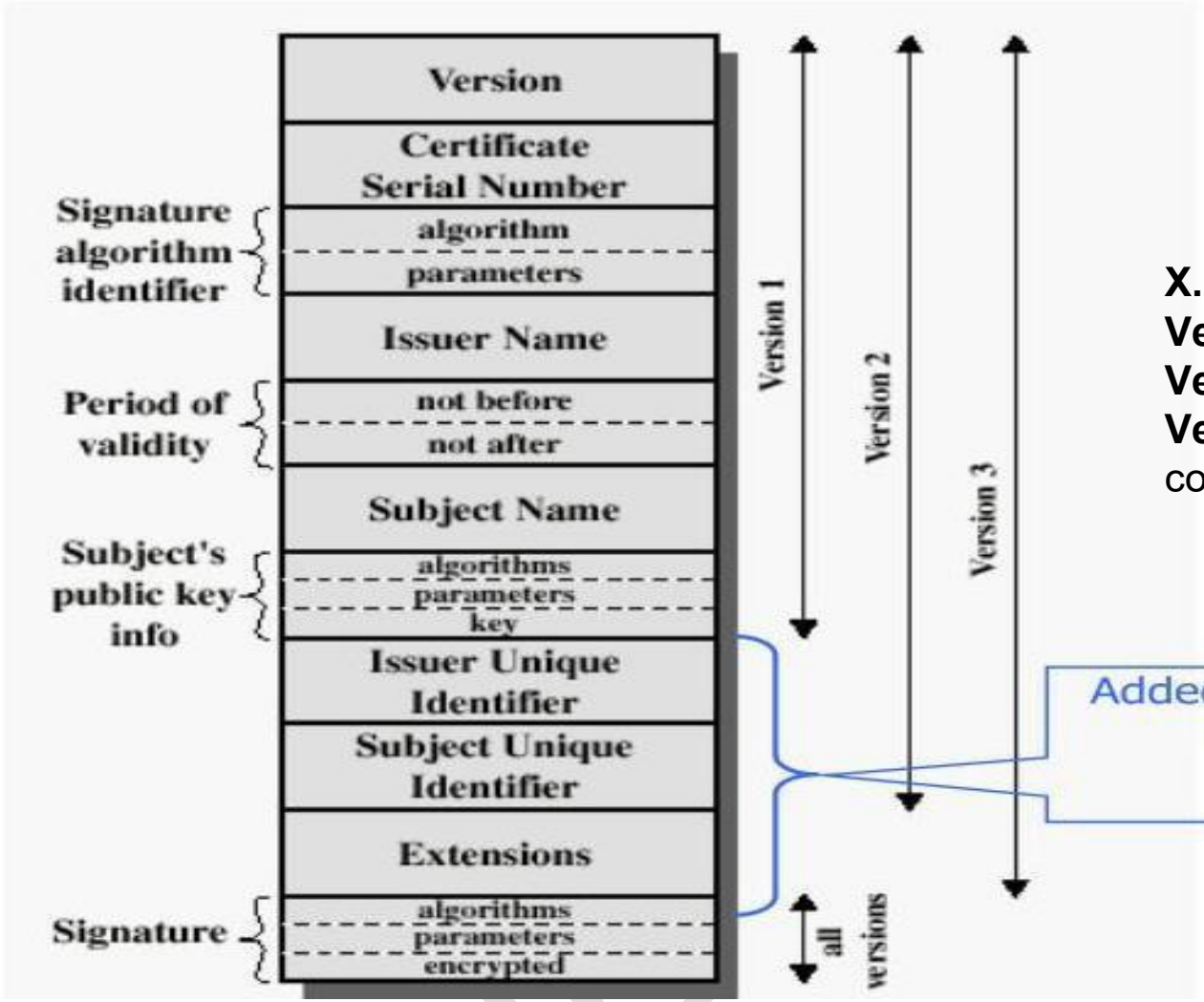
•**Improved and widely used version**
•Supports **multiple encryption algorithms**
•Allows **cross-realm authentication**
•Better security and flexibility
•Used in **Windows Active Directory**, UNIX, Linux

Advantages:

•Stronger security
•Better scalability
•Time-based tickets
•Platform independent

Feature	Kerberos V4	Kerberos V5
Release	Developed in late 1980s	Introduced in 1993 as improved version
Encryption	Uses **DES only** (weak today)	Supports **multiple algorithms** like AES, 3DES, RC4
Network Protocol	Works mainly with **IPv4 / TCP-IP**	Supports **multiple network protocols and addresses**
Ticket Lifetime	Fixed lifetime (max about 21 hours)	Flexible: **renewable, forwardable, post-dated tickets**
Ticket Structure	Simple and limited	**Flexible and extensible ticket format**
Encoding	Uses **ad-hoc encoding**	Uses **ASN.1 encoding standard**
Cross-Realm Authentication	Requires direct relationship between every realm	Supports **hierarchical cross-realm authentication**
Delegation / Forwarding	Not supported	**Supported**
Security	Less secure	**More secure with better cryptography and features**
Status	Now **obsolete / deprecated**	**Current standard used in modern systems**

X.509 Certificate



X.509 Versions
Version 1:- Basic fields only.
Version 2:- Added **unique identifiers**.
Version 3:- Added **extensions** (most commonly used today).

X.509 Certificate

An **X.509 certificate** is a digital certificate used to **prove identity** and **share a public key securely** on the internet (used in HTTPS, email security, digital signatures, etc.).

Parts of the X.509 Certificate

1. Version

1. Tells which version of X.509 is used (v1, v2, or v3).
2. Newer versions add more security features.

2. Certificate Serial Number

1. A unique number given by the **Certificate Authority (CA)**.
2. Helps identify and revoke a certificate if needed.

3. Signature Algorithm Identifier

1. Shows which algorithm the CA used to sign the certificate (example: RSA etc).

4. **Issuer Name**
   - The name of the **CA** that issued the certificate (e.g., VeriSign, DigiCert).

5. **Period of Validity**
   - **Not Before**: Certificate start date
   - **Not After**: Certificate expiry date
   - Outside this period, the certificate is invalid.

6. **Subject Name**
   - The owner of the certificate (person, organization, or website like

7. **Subject's Public Key Information**

   Contains:
   - Public key
   - Key algorithm
   - Used for encryption and digital signature verification

8. **Issuer Unique Identifier** *(v2 & v3)*
    - Helps uniquely identify the issuer if names are repeated.

9. **Subject Unique Identifier** *(v2 & v3)*
    - Helps uniquely identify the subject.

10. **Extensions** *(v3 only – very important)*

•Add extra features like:
    - Key usage (encryption, signing)
    - Subject Alternative Name (SAN)
    - CA or non-CA information

•Improves **security and usability**.

11. **Signature**
    - •The CA's digital signature on the certificate.
    - •Ensures the certificate is **authentic and not modified**.

X.509 Authentication Methods
(One-Way, Two-Way, Three-Way Authentication)

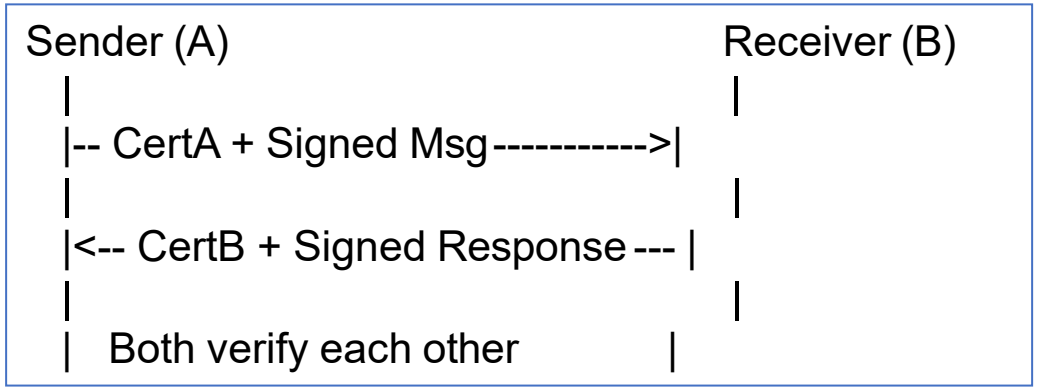
1. **One-way authentication:**
   Only the **sender** is authenticated.
   Example: A website proves its identity to a user in **HTTPS**.

2. **Two-way authentication:**
   Both sender and receiver authenticate each other.
   Example: Client–server login using digital certificates (VPN).

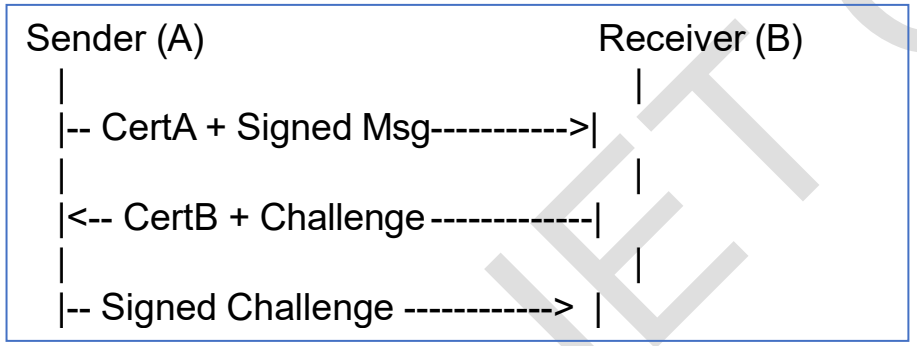
3. **Three-way authentication:**
   Mutual authentication with a **challenge–response** to stop replay attacks.
   Example: High-security network systems using nonce/timestamp.

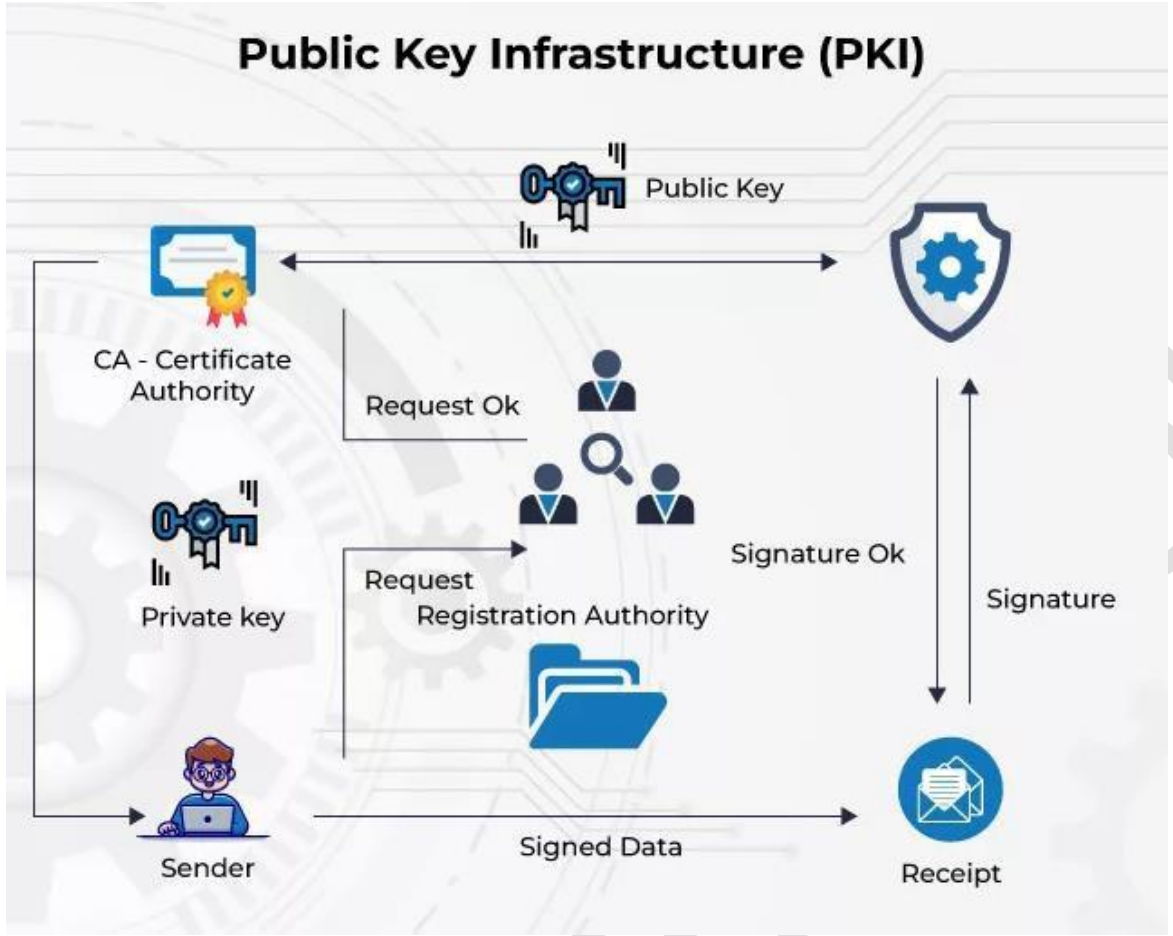
1 One-Way Authentication Diagram Only
Sender A is authenticated

2 Two-Way (Mutual) Authentication Diagram
Both A and B are authenticated



3 Three-Way Authentication Diagram
Mutual authentication Protection against **replay attack**





PKI (Public Key Infrastructure)
User creates **public–private key pair**.
•**RA** verifies user identity.
•**CA** issues and signs the **digital certificate**.
•Sender signs data using **private key**.
•Receiver verifies signature using **public key** and CA certificate.
Ensures **authentication, integrity, and trust**.

Elements of PKIX Model

1. **End Entity**
    1. The **user, device, or server** that uses PKI.
    2. Can be a **certificate holder** or a **certificate user**.
    3. Example: Website, email user, client, server.

2.Public Key Certificate

1. A **digital certificate (X.509)** that binds:
    - Identity of end entity
    - Public key
2. Issued and signed by a **Certification Authority (CA)**.

3.Certification Authority (CA)

1. A **trusted organization** that:
    - Issues digital certificates
    - Signs certificates using its private key
2. Example: DigiCert, GlobalSign.

4.Certificate Repository (CR)

1. A **database** that stores:
    - Digital certificates
    - Certificate Revocation Lists (CRLs)
2. Allows users to **retrieve and verify certificates**.

Email Security and IP Security

Email Security

Email security protects emails from **unauthorized access, modification, and impersonation**.

How it works

•Uses **encryption** and **digital signatures**

•Common standards:

- **PGP (Pretty Good Privacy)**
- **S/MIME**

Provides

•**Confidentiality** – only receiver can read

•**Authentication** – sender identity verified

•**Integrity** – message not changed

•**Non-repudiation** – sender cannot deny

Example

•Secure email with **PGP / S-MIME**

IP Security (IPsec)

IP security protects data at the **network (IP) layer**.

How it works

•Secures **all IP packets**

•Uses:

- **Authentication Header (AH)**
- **Encapsulating Security Payload (ESP)**

Modes

•**Transport mode** – protects payload

•**Tunnel mode** – protects whole packet

Provides

•Data confidentiality

•Authentication

•Integrity

•Anti-replay protection

Example

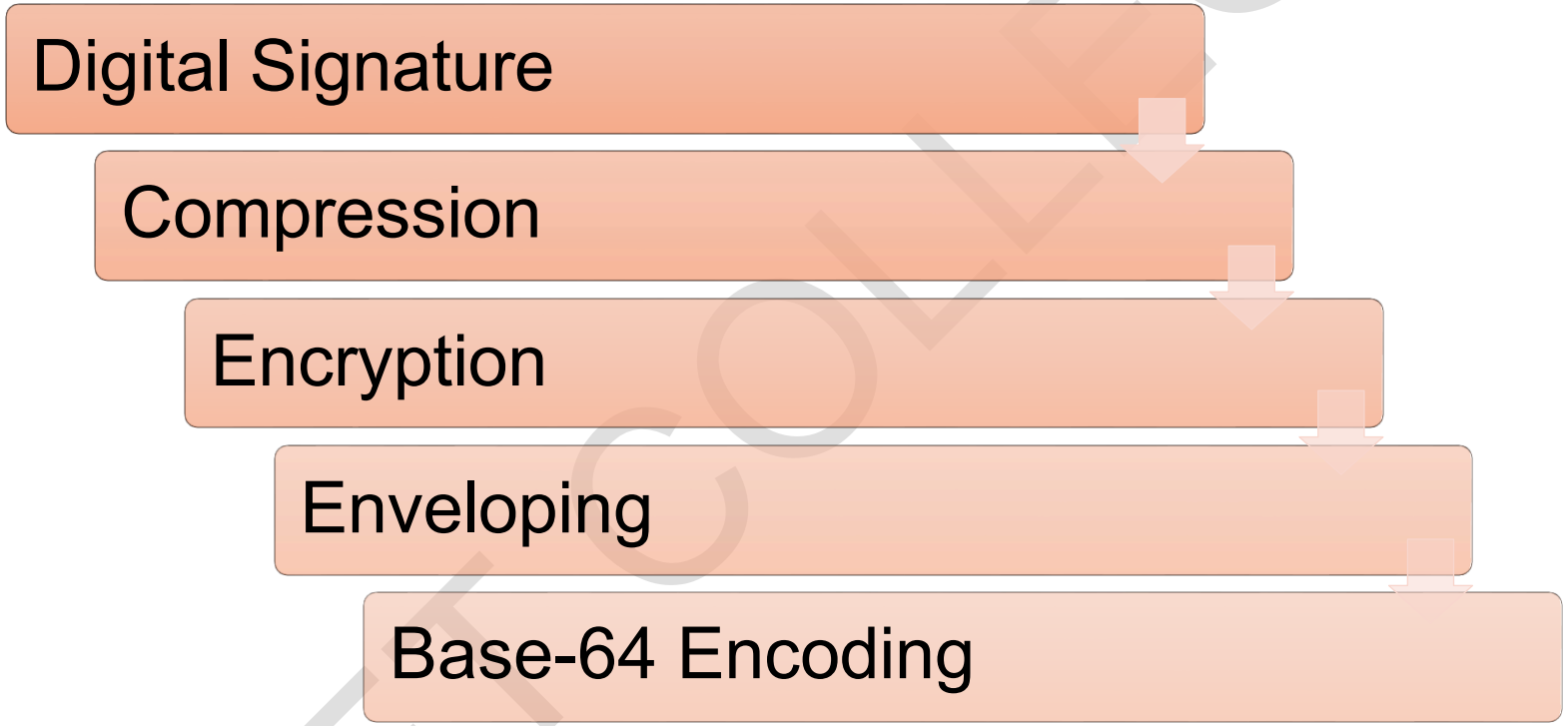
•**VPN (Virtual Private Network)**

PGP (Pretty Good Privacy)
PGP is an email security system used to **encrypt and digitally sign emails**.

Functions of PGP
- **Confidentiality** – encrypts message
- **Authentication** – verifies sender
- **Integrity** – ensures message not changed
- **Non-repudiation** – sender cannot deny

How PGP Works
Message is **compressed**.
1. Message is **encrypted using a session key** (symmetric).
2. Session key is **encrypted using receiver's public key**.
3. Sender **signs message** using own private key.
4. Receiver:
    1. Decrypts session key using private key
    2. Verifies signature using sender's public key

Working of PGP



PGP Operations

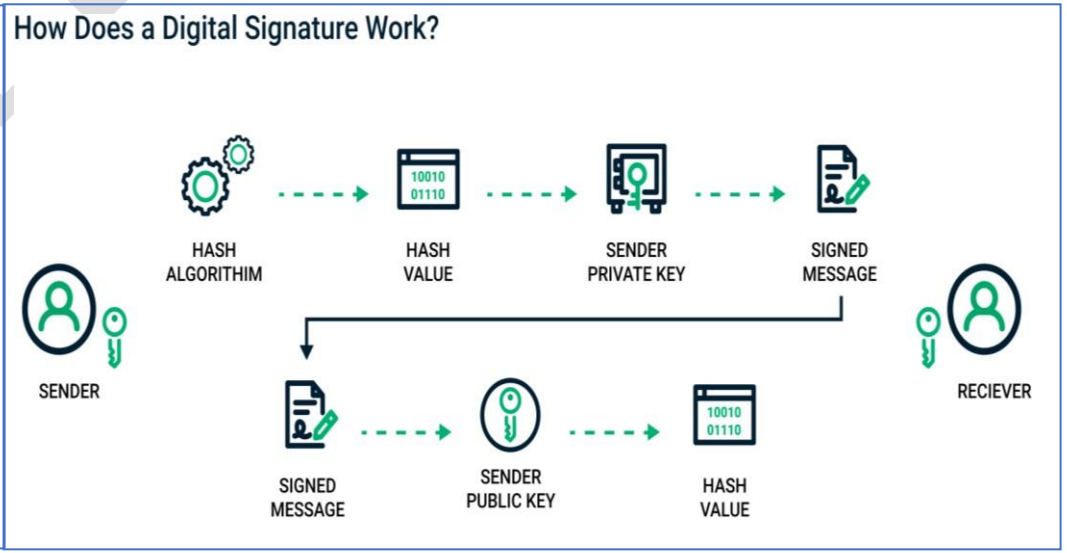
1. Digital Signature

•Creates a **hash** of the message.
•Hash is encrypted using **sender's private key**.
•Ensures:

- **Authentication**
- **Integrity**

•Sender side:
•Message → Hash → Encrypt hash with private key → Send message + digital signature.

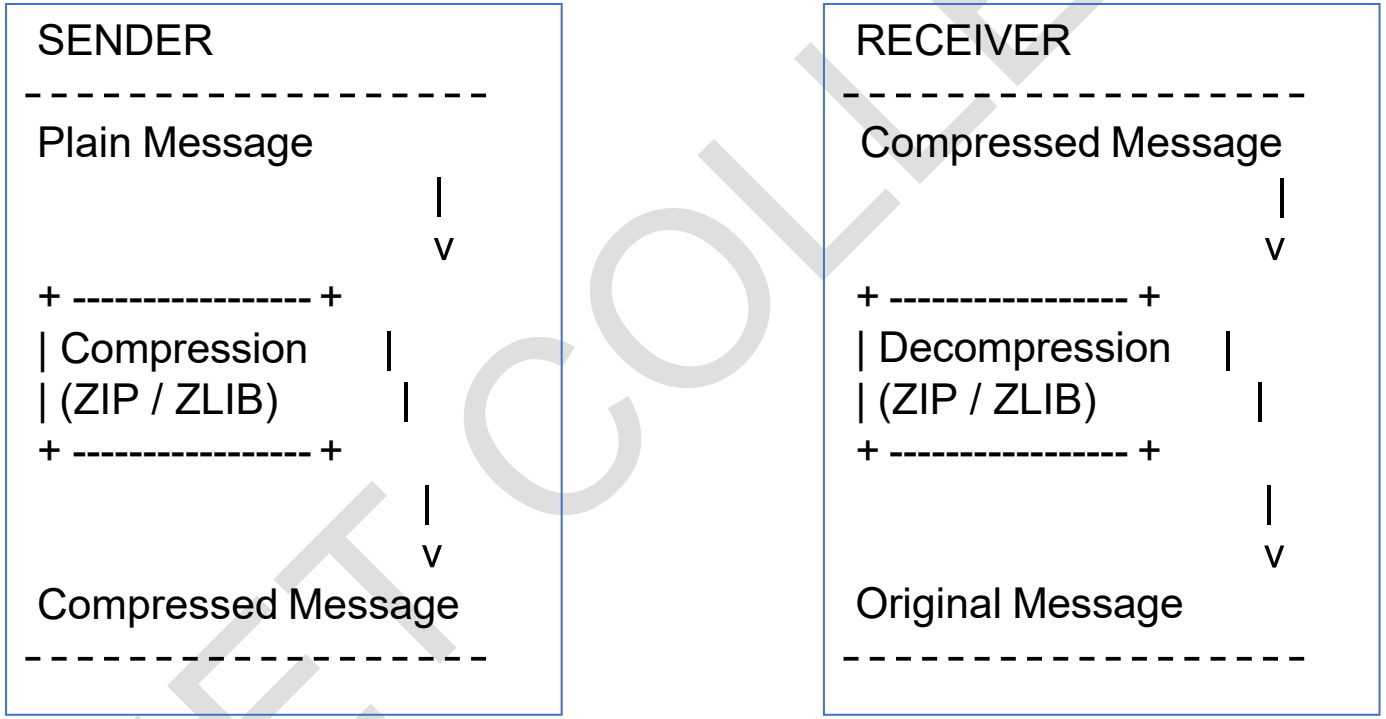
•Receiver side:
•Receive message + signature → Decrypt signature with sender's public key → Get original hash → Hash received message → Compare hashes.



2. Compression

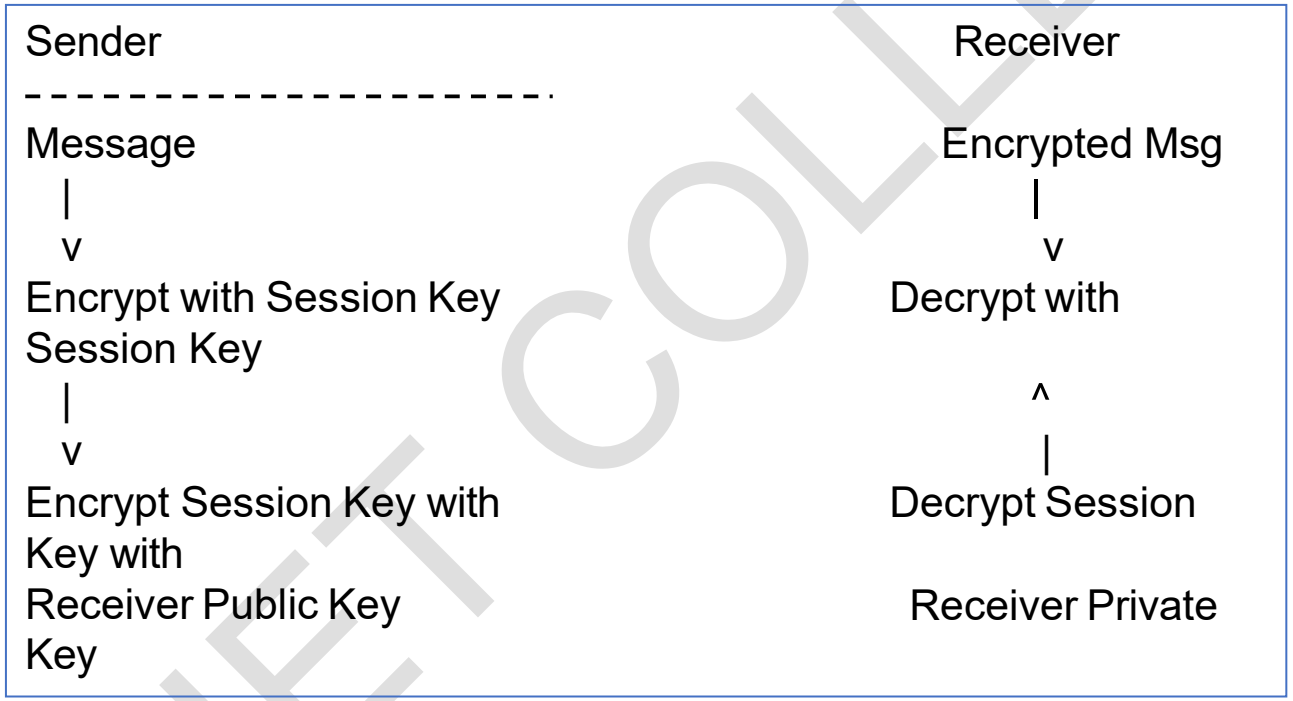
•Message and signature are **compressed** before encryption.

•Saves bandwidth and improves security.



3. Encryption

•Message is encrypted using a **session key** (symmetric encryption).
•Session key is encrypted using **receiver's public key**.
•Provides **confidentiality**.

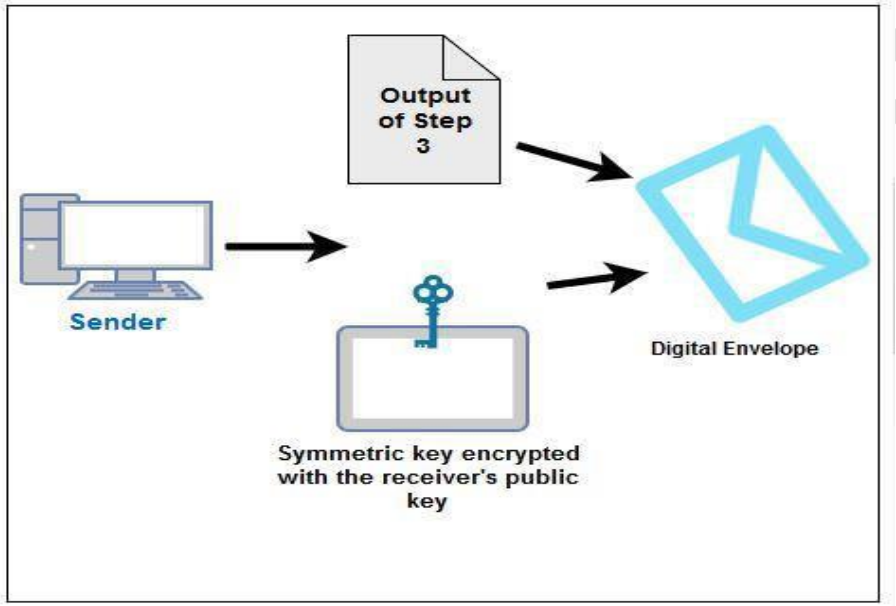


4. Enveloping

•Encrypted message + encrypted session key are combined.

•Forms a **digital envelope**.

•Securely sends data and key together.

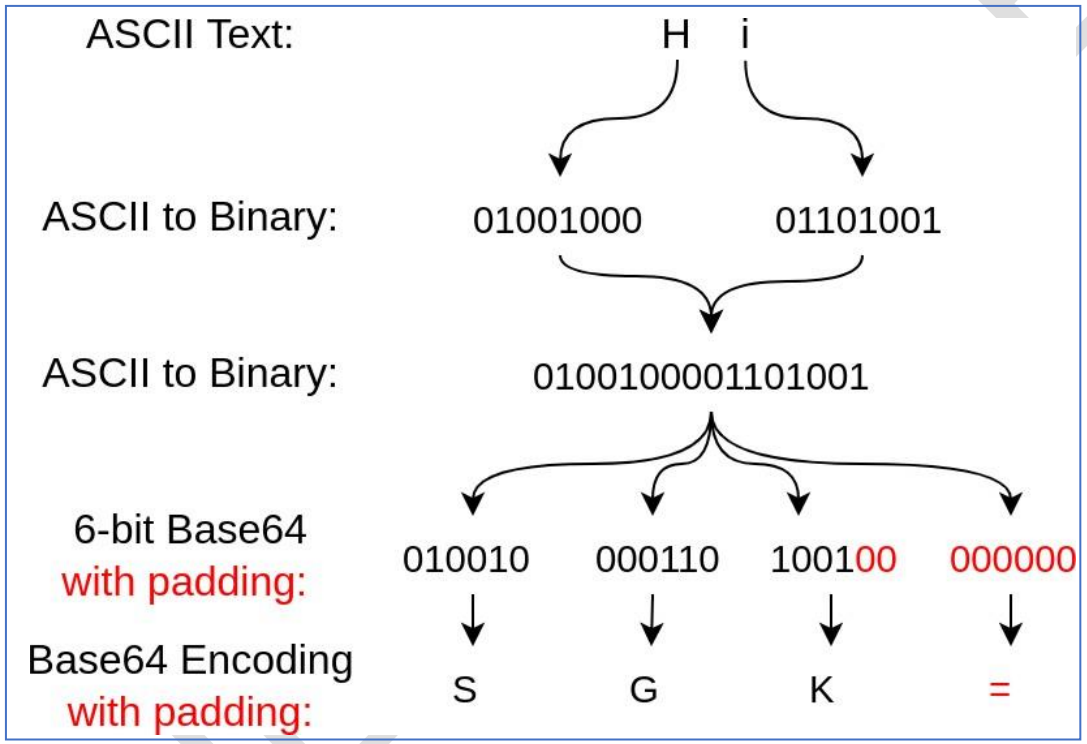


Formation of digital envelope

5. Base-64 Encoding

•Converts binary encrypted data into **ASCII text**.

•Makes email **safe for transmission**.



S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard used to **secure email messages** using **encryption and digital signatures**.

Message consists of two parts

An **email/message** is divided into **two main parts**:

1. **Header**
    1. Contains control information
    2. Examples: **From, To, Subject, Date**
    3. Used for **routing and delivery**
    4. **Not encrypted** (usually)
2. **Body**
    1. Contains the **actual message content**
    2. Text, attachments, etc.
    3. Can be **encrypted and signed** (in PGP / S-MIME)

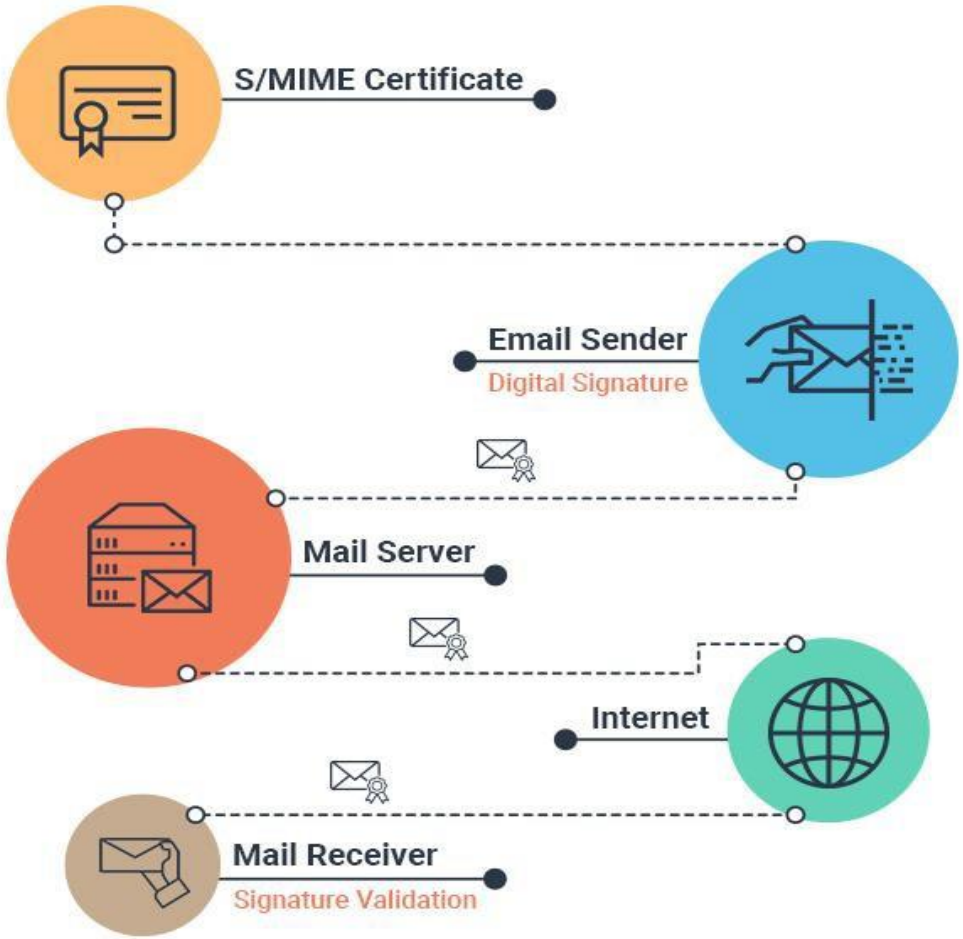
S/MIME Functionality
S/MIME provides **email security** using three main functions:

1. Enveloped Data
•Used for **encryption**

•Message is encrypted using a **session key**
•Session key is encrypted with **receiver's public key**
•Provides **confidentiality**
Only the intended receiver can read the message.

2. Signed Data
•Used for **digital signature**
•Message is hashed and encrypted with **sender's private key**
•Signature is sent **along with the message**
•Provides **authentication, integrity, and non-repudiation**
Receiver verifies using sender's public key.

3. Clear Signing
•Message is **not encrypted**
•Only the **digital signature** is attached
•Message remains readable by everyone
•Provides **authentication and integrity**, but **no confidentiality**
Used when privacy is not required.



•Sender uses **S/MIME certificate** to **digitally sign** the email with their **private key**.
•Email is sent through **mail server and internet**.
•Receiver uses **sender's public key** to **verify the signature**.

Very Short Answer Questions

1. What is authentication?
2. What is Kerberos?
3. What does X.509 define?
4. What is a digital certificate?
5. Expand PGP.
6. What is S/MIME used for?
7. What is a public key?
8. What is a private key?
9. What is Directory Authentication Service?
10. What is the role of a Certification Authority (CA)?

Short Answer Questions

1. Explain Kerberos authentication in brief.
2. What is X.509 certificate? Write its importance.
3. Explain Pretty Good Privacy (PGP).
4. What is S/MIME? Mention its use.
5. Explain Directory Authentication Service with one example.

Long Answer Questions

1. Explain **Kerberos authentication system** with working and advantages.
2. Describe **X.509 authentication framework** in detail.
3. Explain **Pretty Good Privacy (PGP)** with its services and working.
4. Explain **S/MIME** architecture and its applications in secure email.
5. What is **Directory Authentication Service**? Explain its role in network security.