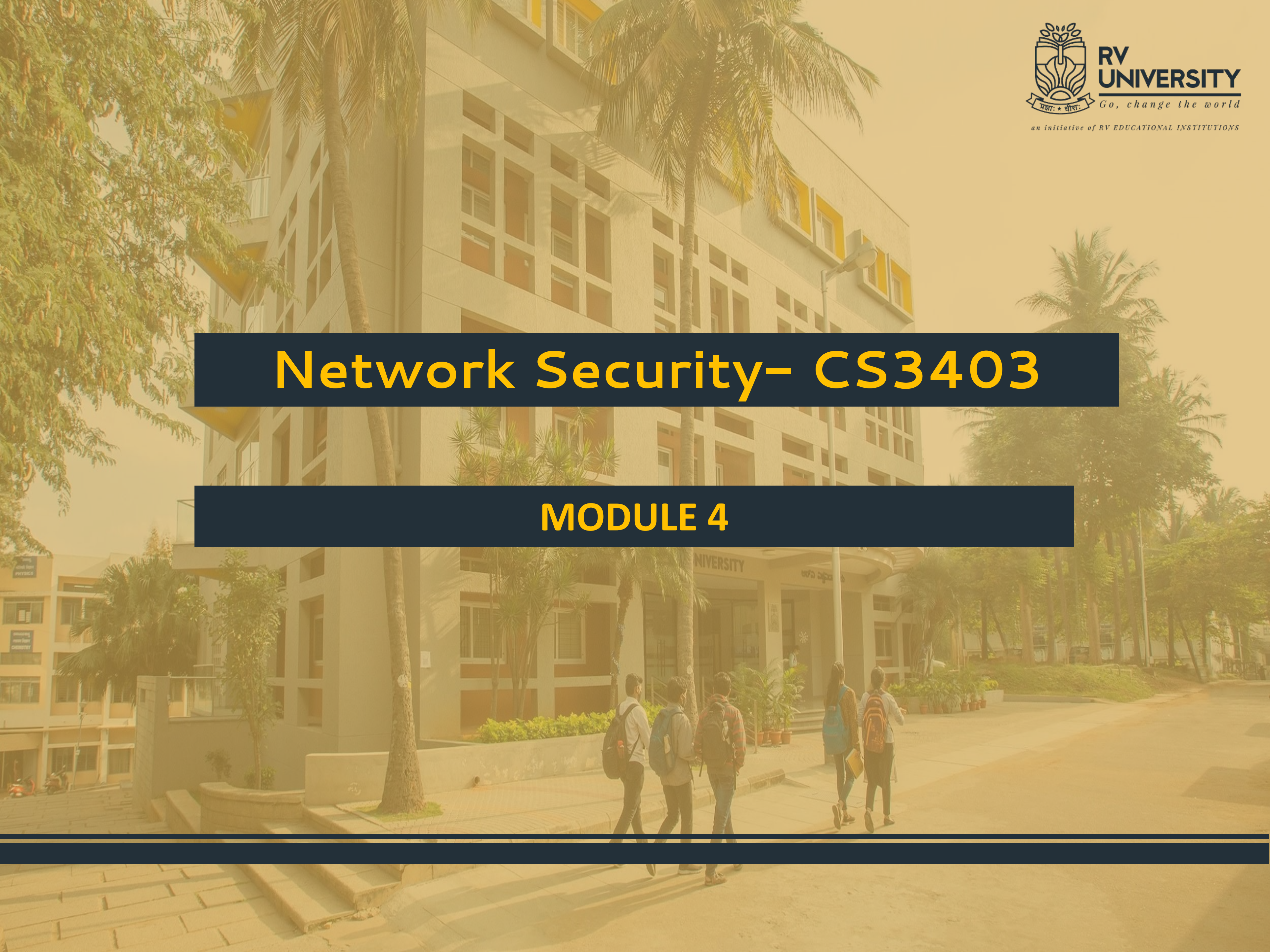


RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

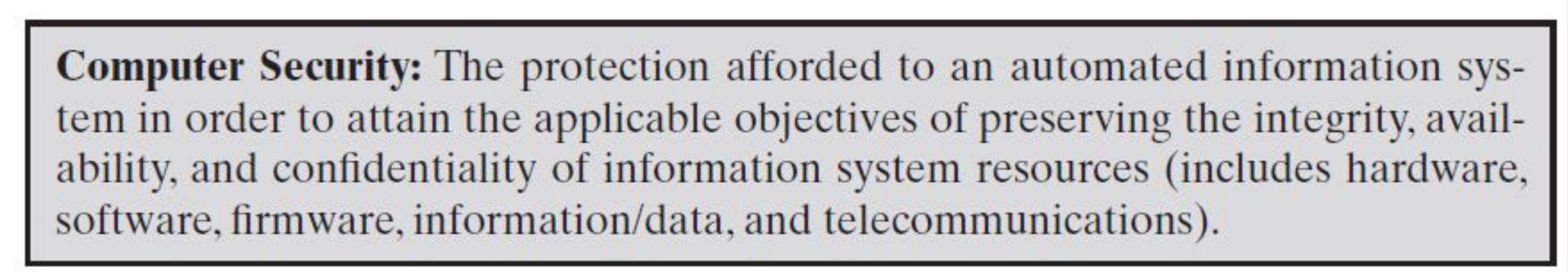
Network Security- CS3403

MODULE 4

Network Security- CS3403

MODULE 4

Computer Security



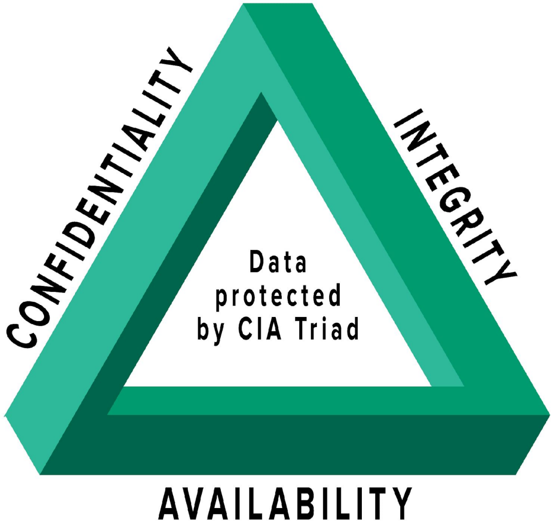
Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Types of Security

- **Network Security:**
  - Protects networks from unauthorized access, cyberattacks, and threats
- **Application Security:**
  - Protects software and applications from vulnerabilities and attacks
- **Endpoint Security:**
  - Protects devices (laptops, mobile phones, servers) from malware and threat
- **Cloud Security:**
  - Protects cloud-based applications, data, and services
- **Cyber Security:**
  - Protects against cyber threats like hacking, malware, phishing, and cyber espionage.
- **Database Security:**
  - Protects databases from breaches, SQL injections, and unauthorized access.

CIA Triad

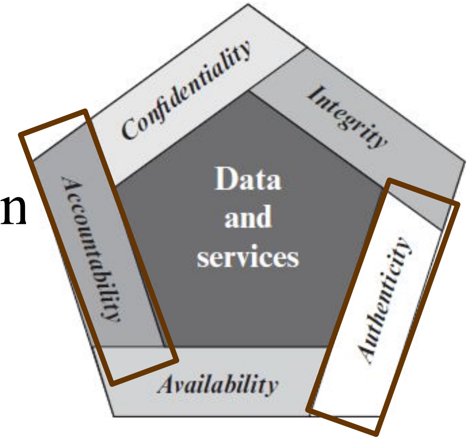
- **Confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - A loss of confidentiality is the unauthorized disclosure of information.



- **Integrity**: Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner
  - A loss of integrity is the unauthorized modification or destruction of information
- **Availability**: Assures that systems work promptly and service is not denied to authorized users.
  - A loss of availability is the disruption of access to or use of information or an information system
- These **three concepts** form what is often referred to as the **CIA triad**.

Authenticity and Accountability

- Additional Concepts for completion:
  - **Authenticity**
  - **Accountability**
- **Authenticity**: It ensures that data, users, devices, an communications are genuine, verified, and trusted.
  - It involves mechanisms like digital signatures, cryptographic authentication, certificates, and biometrics to confirm the identity of users and the integrity of data



- **Accountability**: It refers to the ability to trace actions and events in a system back to a specific user, process, or entity to ensure responsibility and compliance.
  - It is achieved through mechanisms like user authentication, logging, auditing, and access control, ensuring that actions are recorded, monitored, and verifiable

Different Types of Attacks

- **Threat**: It is a possible danger that might exploit a vulnerability.
- **Attack**: An assault on system security that derives from an intelligent threat.
- **Passive attacks**: Eavesdropping on, or monitoring of, transmissions.
  - The goal of the opponent is to obtain information that is being transmitted.
- **Active attacks**: Involves some modification of the data stream or the creation of a false stream
  - **Masquerade** takes place when one entity pretends to be a different entity
  - **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
  - **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
  - **Denial of Service (DoS)** prevents or inhibits the normal use or management of communications facilities

Security Services

- **Authentication**: It is concerned with assuring that a communication is authentic
  - It is to assure the recipient that the message is from the source that it claims to be from
- **Access Control**: It is the ability to limit and control the access to host systems and applications via communications links.
  - To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.
- **Data Confidentiality**: It is the protection of transmitted data from passive attacks. Protection of traffic flow from analysis.
- **Data Integrity**: It assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.
  - The destruction of data is also covered under this service. DoS is also covered here.
- **Nonrepudiation:** It prevents either sender or receiver from denying a transmitted message.

Introduction to Cryptography

Cryptography: An Introduction

- The word “cryptography” derives from the Greek word for “secret writing”.
- The Concise Oxford English Dictionary defines cryptography as “the art of writing or solving codes.”
- But cryptography nowadays encompasses much more than this, it deals with mechanisms for
  - Ensuring integrity, techniques for exchanging secret keys
  - Protocols for authenticating users
  - Electronic auctions and elections
  - Digital cash, and more.

Cryptography

Cryptanalysis:

- The art or process of deciphering coded messages without being told the key.
- Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

Cryptology:

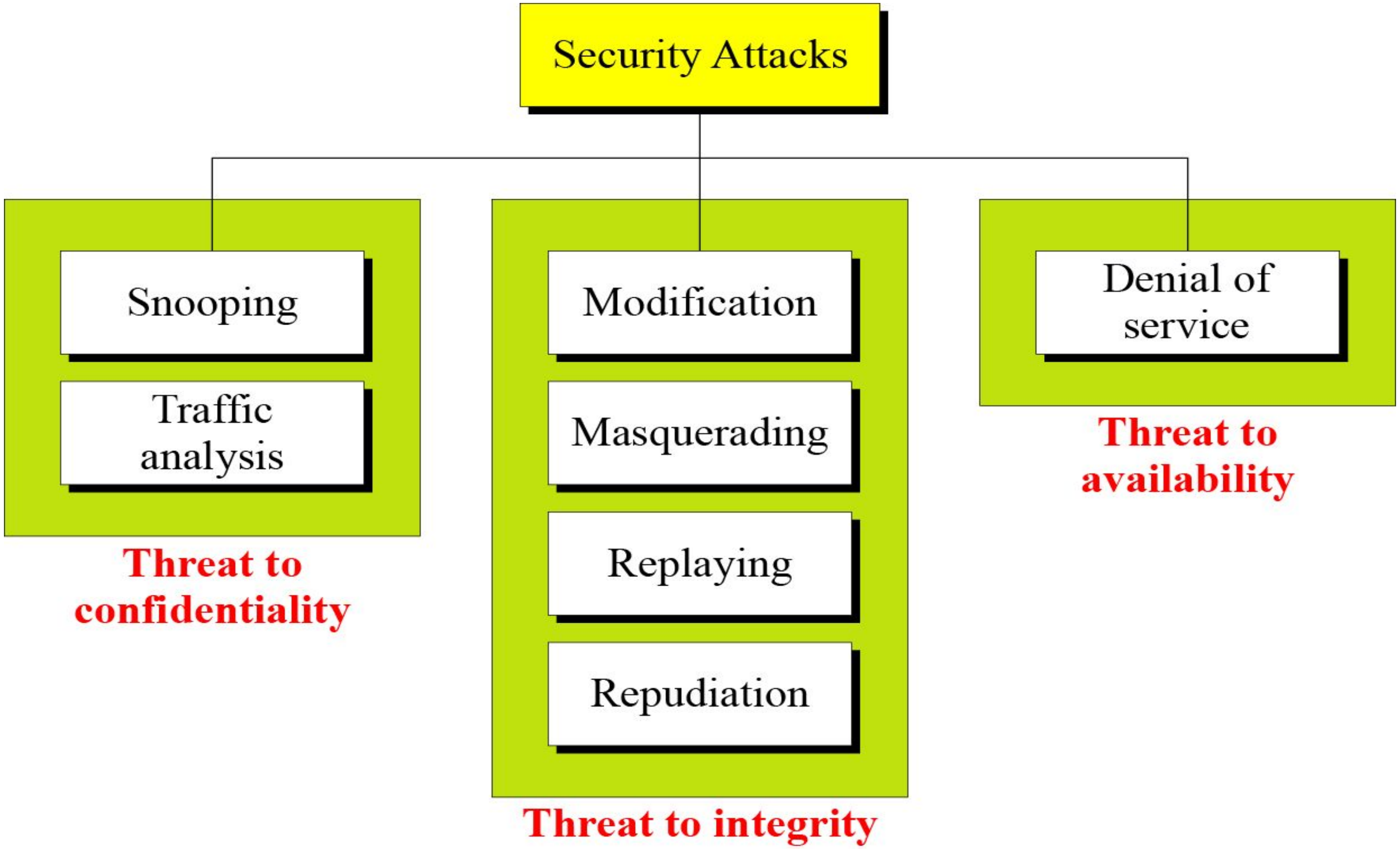
- The scientific study of cryptography and cryptanalysis.

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Attacks

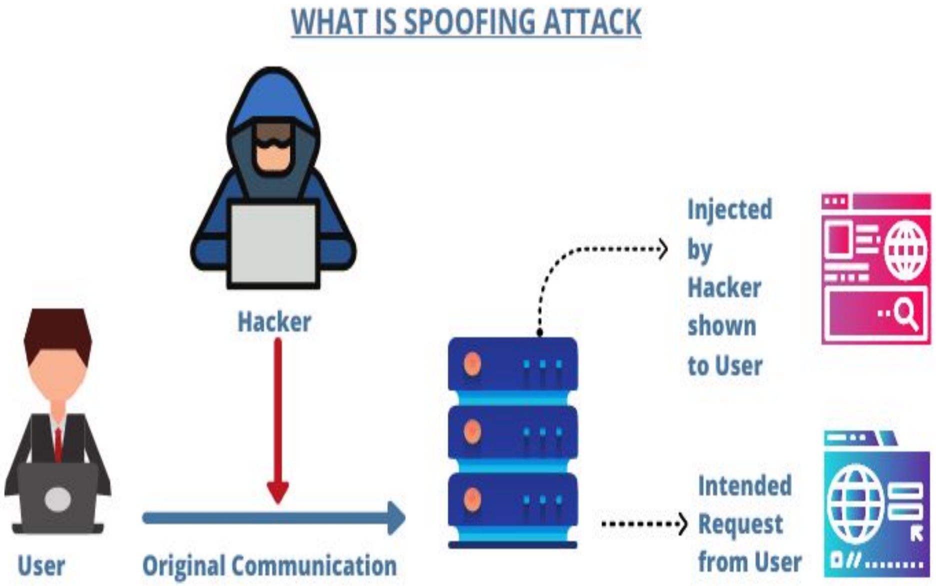
Security Attacks

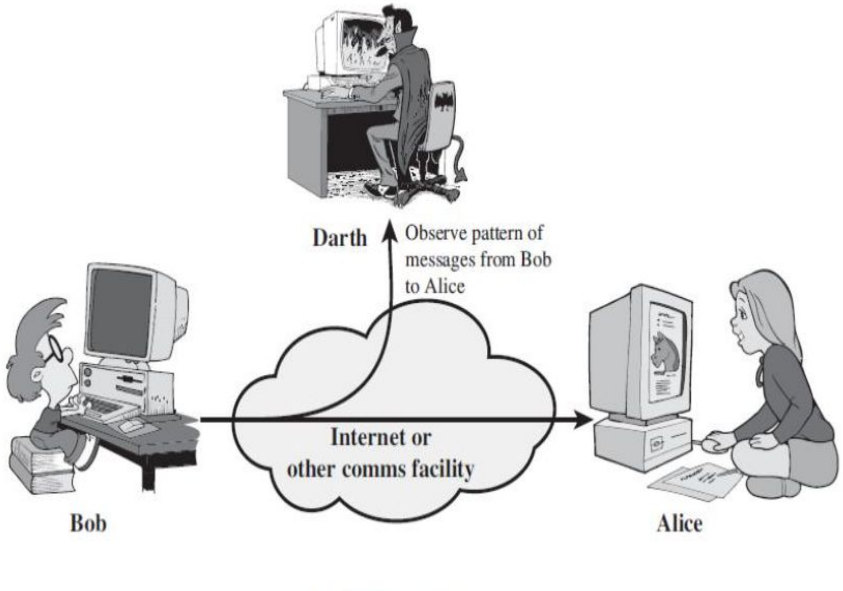
Taxonomy of Attacks with relation to security goals



Attacks Threatening Confidentiality

- 2 types of attacks threaten the confidentiality of information
  - **Snooping** refers to **unauthorized access** to or **interception** of data.
  - **Traffic analysis** refers to obtaining some other type of information by **monitoring online traffic**.




Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

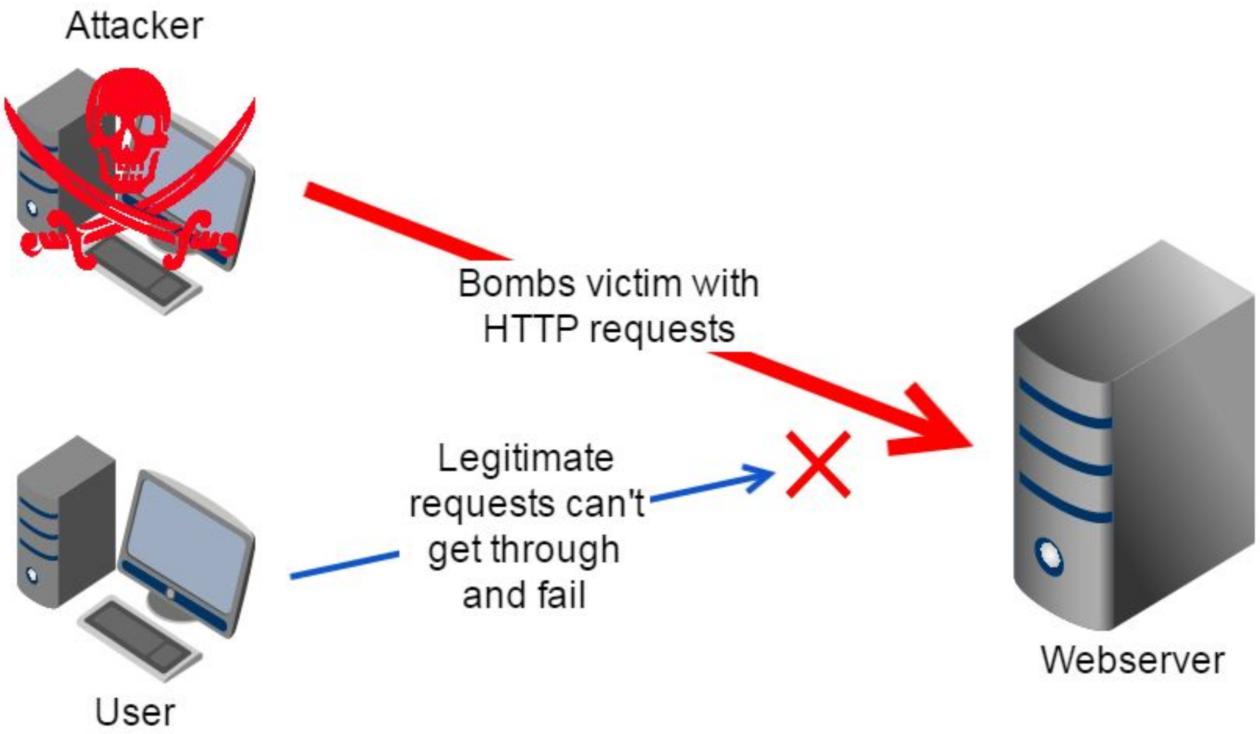
(b) Traffic analysis

Attacks Threatening Integrity

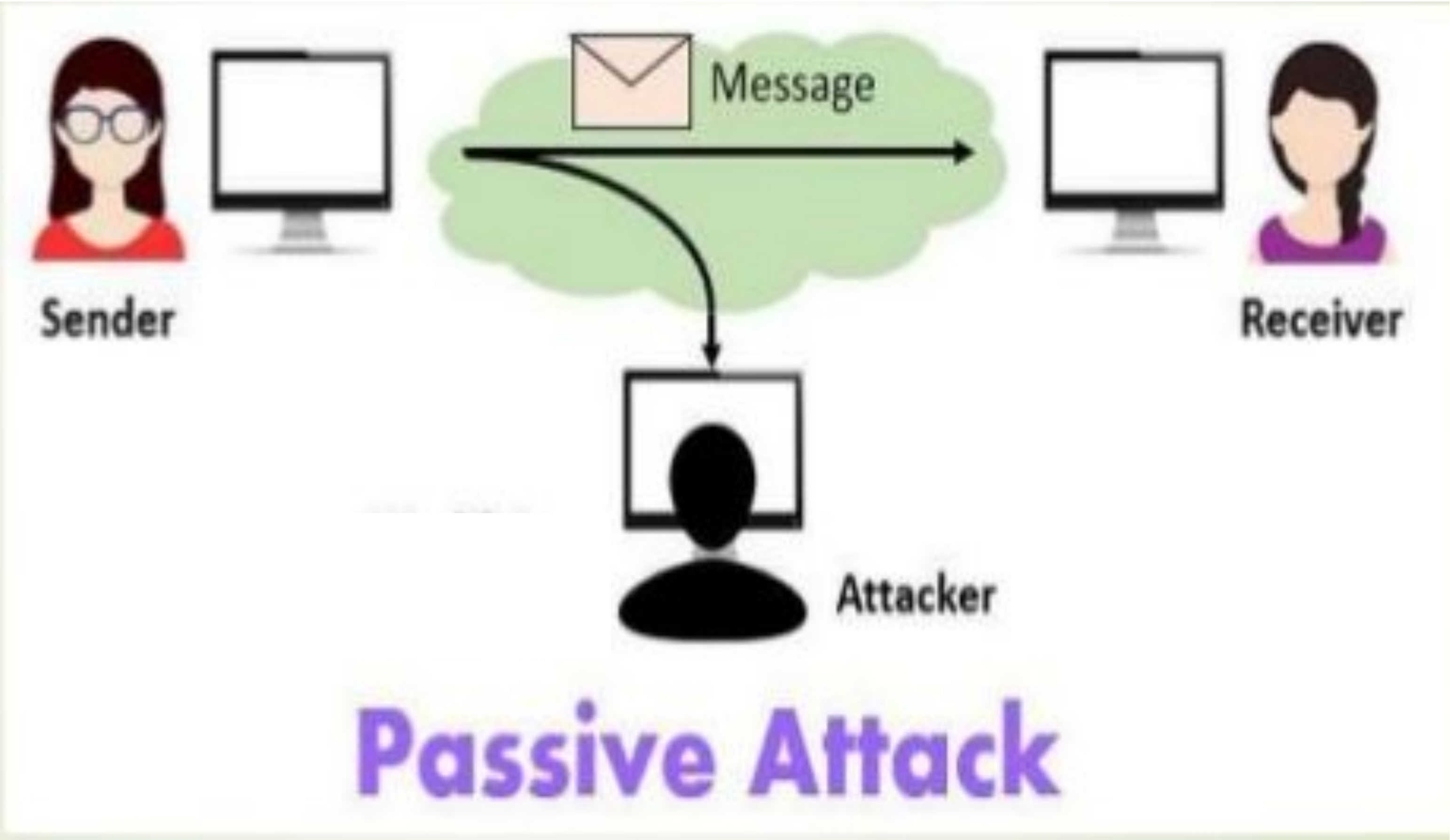
- **Modification** means that the attacker **intercepts the message** and changes it.
- **Masquerading** or spoofing happens when the attacker **impersonates** somebody else.
- **Replaying** means the attacker **obtains a copy** of a message sent by a user and later tries to replay it.
- **Repudiation** means that sender of the message might later **deny** that she has sent the message; the receiver of the message might later deny that he has received the message.

Attacks Threatening Availability

- **Denial of service (DoS)** is a very **common attack**.
- It may **slow down** or totally interrupt the service of a system.


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

Passive Attacks



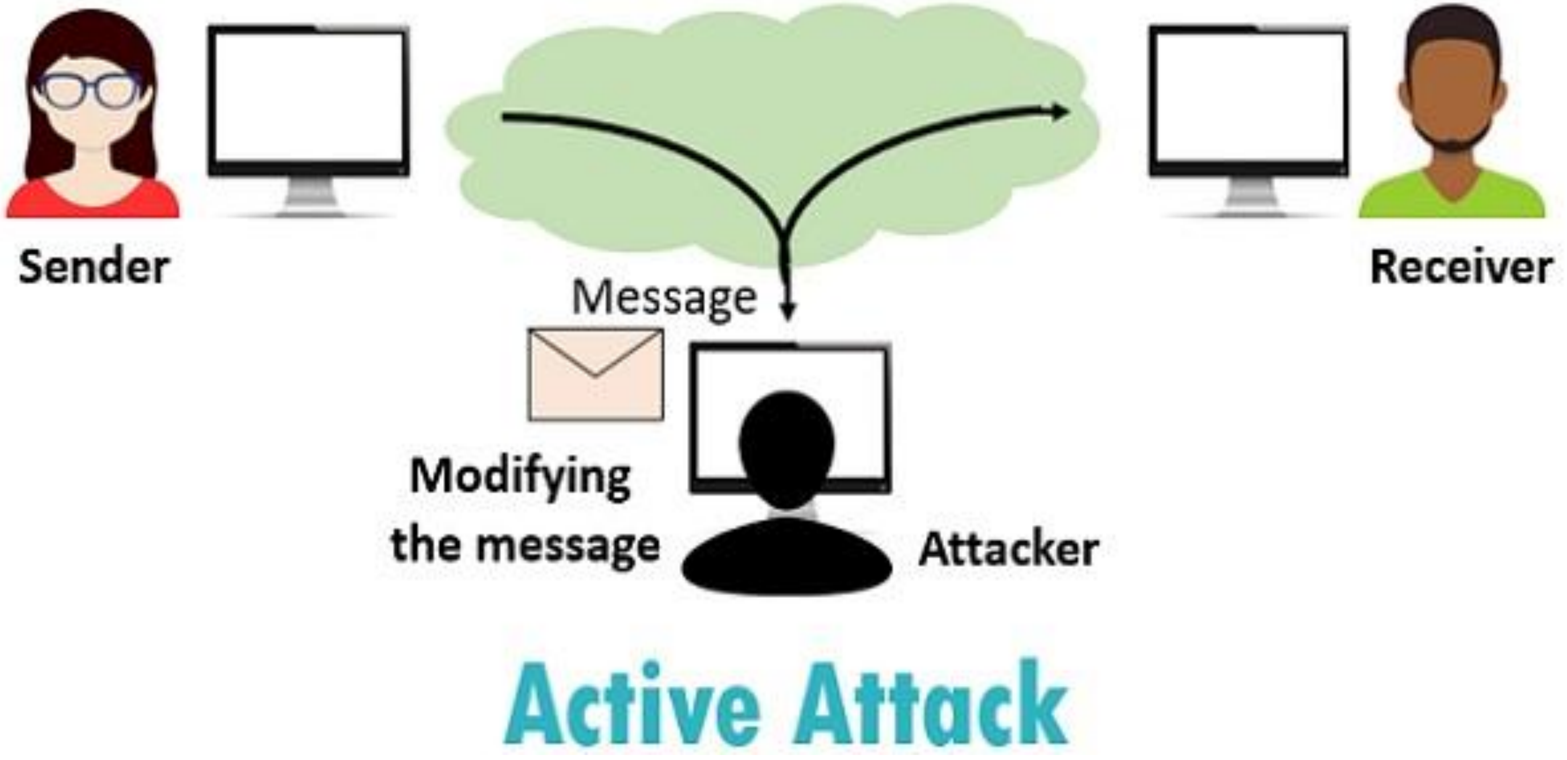
Types of Attacks

Passive Attacks

- **Passive Attacks**
    - Goal is to just **obtain information**.
    - Attack **does not modify data** or harm the system.
    - Attacks that **threaten Confidentiality** are **Passive attacks**.
    - Difficult to detect this type of attack.
    - Passive attacks can be prevented by **encipherment** of the data.

Encipherment refers to the process of converting information, such as a message or document, from its original form into a coded or ciphered form

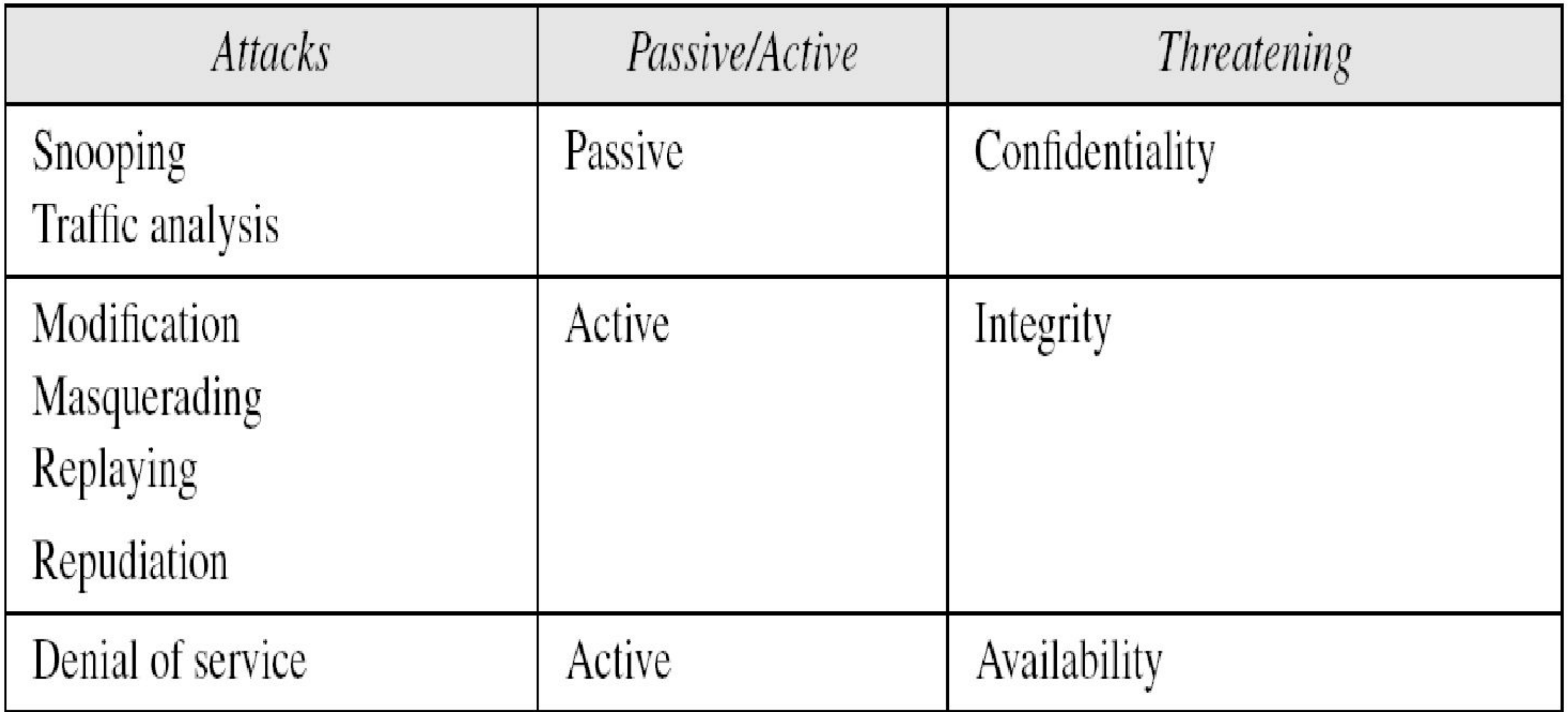
Active Attacks



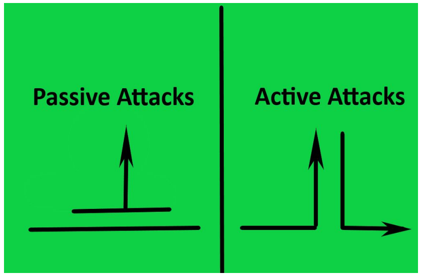
Active Attacks

- **Active Attacks**
  - Attack **may change the data** or harm the system.
  - Attacks that threaten the Integrity and Availability are Active attacks.
  - Easier to detect this type of attack than to prevent.

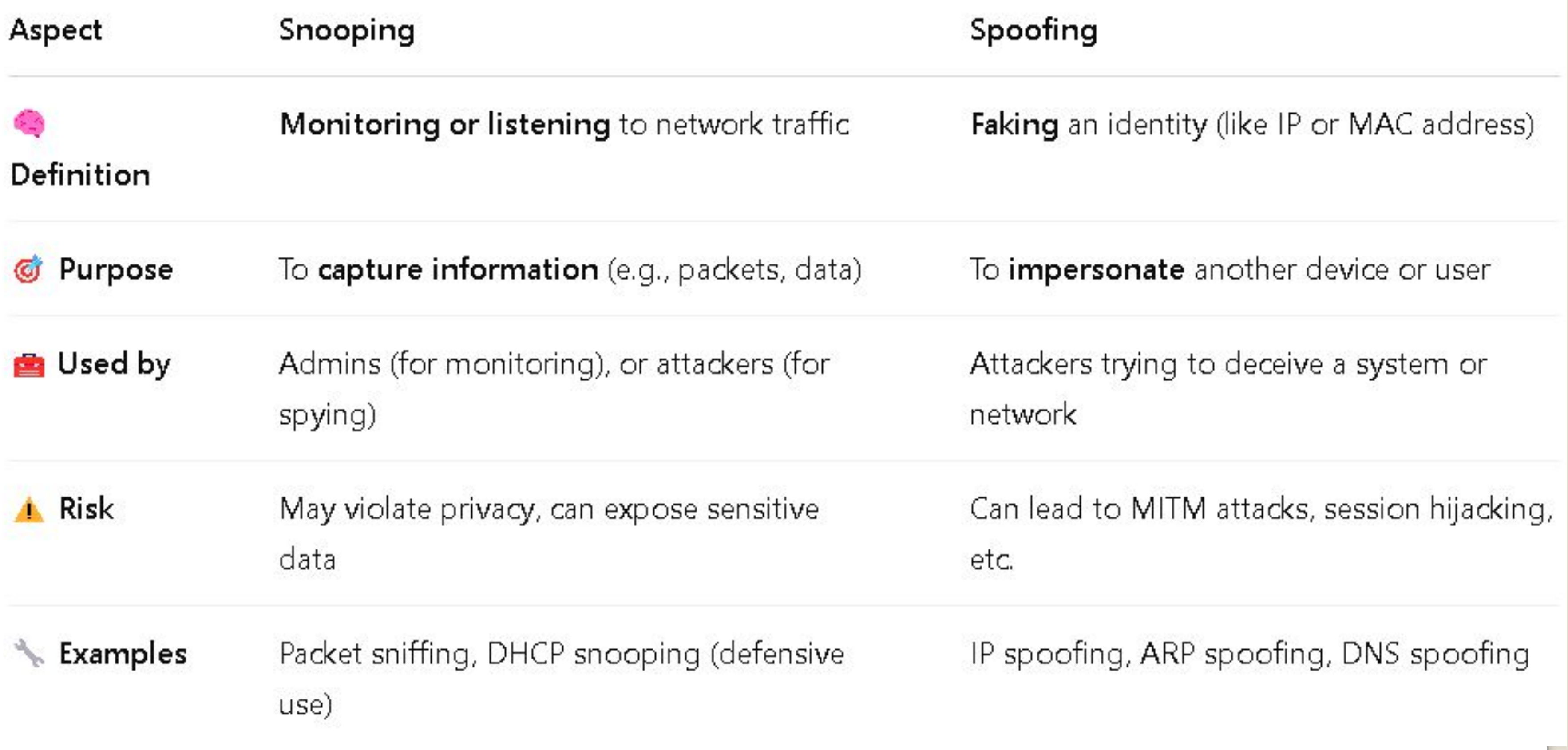
Passive Vs Active Attacks



Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability



Snooping Vs Spoofing



Aspect	Snooping	Spoofing
🧠 Definition	**Monitoring or listening** to network traffic	**Faking** an identity (like IP or MAC address)
🎯 Purpose	To **capture information** (e.g., packets, data)	To **impersonate** another device or user
🧰 Used by	Admins (for monitoring), or attackers (for spying)	Attackers trying to deceive a system or network
⚠️ Risk	May violate privacy, can expose sensitive data	Can lead to MITM attacks, session hijacking, etc.
🔧 Examples	Packet sniffing, DHCP snooping (defensive use)	IP spoofing, ARP spoofing, DNS spoofing

MITM: Man-in-the-Middle attach

Key Terms in Cryptography

- **One-way hash function-** Sometimes also called as one-way compression function to compute a **reduced hash value** for a message (**e.g., SHA-256**)
- **Symmetric key cryptography-** Compute a cipher text decodable with the same key used to encode (**e.g., AES**)
- **Public-key cryptography-** Compute a cipher text decodable with a different key used to encode (**e.g., RSA**)
- **Digital signatures-** Confirm the author of a message
- **Mix network-** Pool communications from many users to anonymize what came from whom.
  - A mix network is a cryptographic system that facilitates anonymous communication by obscuring the relationship between senders and recipients of messages.

Symmetric & Asymmetric key Cryptography

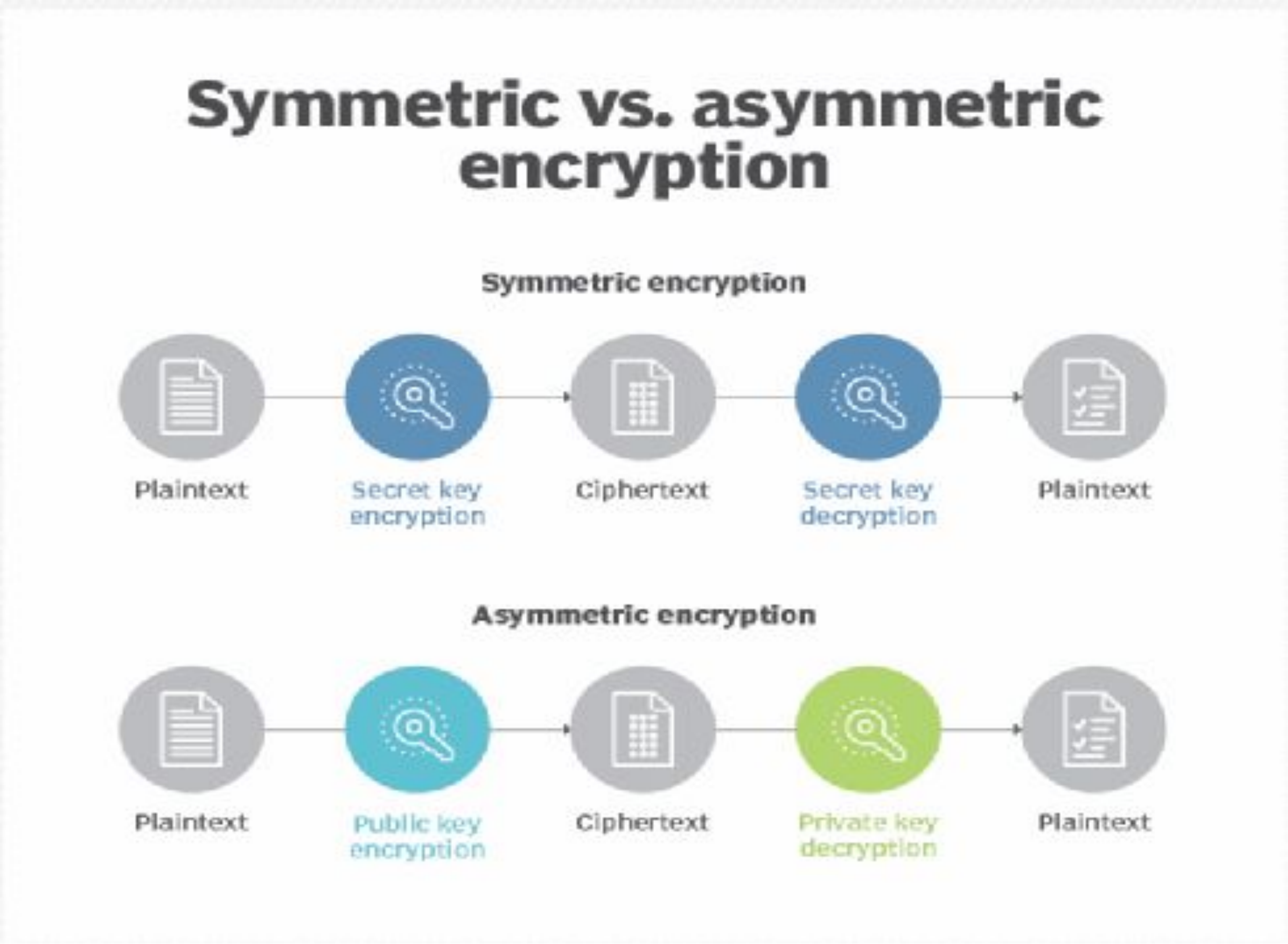
Cryptographic Techniques

- Cryptography involves 3 distinct mechanisms
  - **Symmetric key Encipherment**
  - **Asymmetric key Encipherment**
  - **Hashing**

Symmetric & Asymmetric key Cryptography

- **Symmetric key Encipherment**
  - Also called as secret key encipherment or secret key cryptography.
  - This method uses a single secret key for both encryption and decryption.
- **Asymmetric key Encipherment**
  - Also called as public key encipherment or public key cryptography.
  - This method uses 2 keys, one public key and one private key.
  - Encryption using public key, decryption using private key.

Symmetric & Asymmetric key Cryptography



Symmetric vs. asymmetric encryption

Symmetric encryption

Plaintext → Secret key encryption → Ciphertext → Secret key decryption → Plaintext

Asymmetric encryption

Plaintext → Public key encryption → Ciphertext → Private key decryption → Plaintext

Cryptography: Quiz 1 to 4

Quiz 1: Cryptography

- Which of the following is an example of a passive attack?

A. ARP spoofing

B. Packet sniffing

C. Denial of Service (DoS)

D. Session hijacking

ANS: B

Quiz 2: Cryptography

- Which of the following statements about symmetric cryptography is true?

A. It uses a pair of public and private keys

B. It is slower than asymmetric encryption

C. It uses the same key for both encryption and decryption

D. It is only used in digital signature

ANS: C

Quiz 3: Cryptography

- What is an important property of a cryptographic hash function?

A. It can be easily reversed to get the original input

B. It generates variable-length outputs

C. It produces a fixed-size output from any input

D. It always generates the same hash for different inputs

ANS: C

Quiz 4: Cryptography

- What is the main purpose of a digital signature?

A. Compress the message before sending

B. Encrypt the entire message

C. Ensure integrity and non-repudiation

D. None of the above

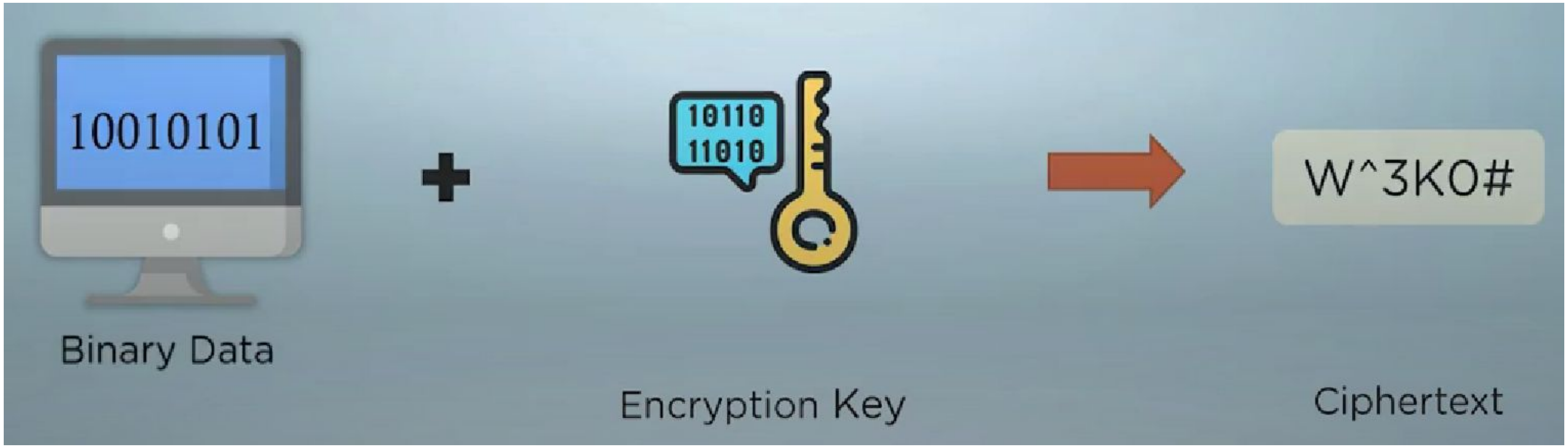
ANS: C

Types of Encryption

Types of Encryption

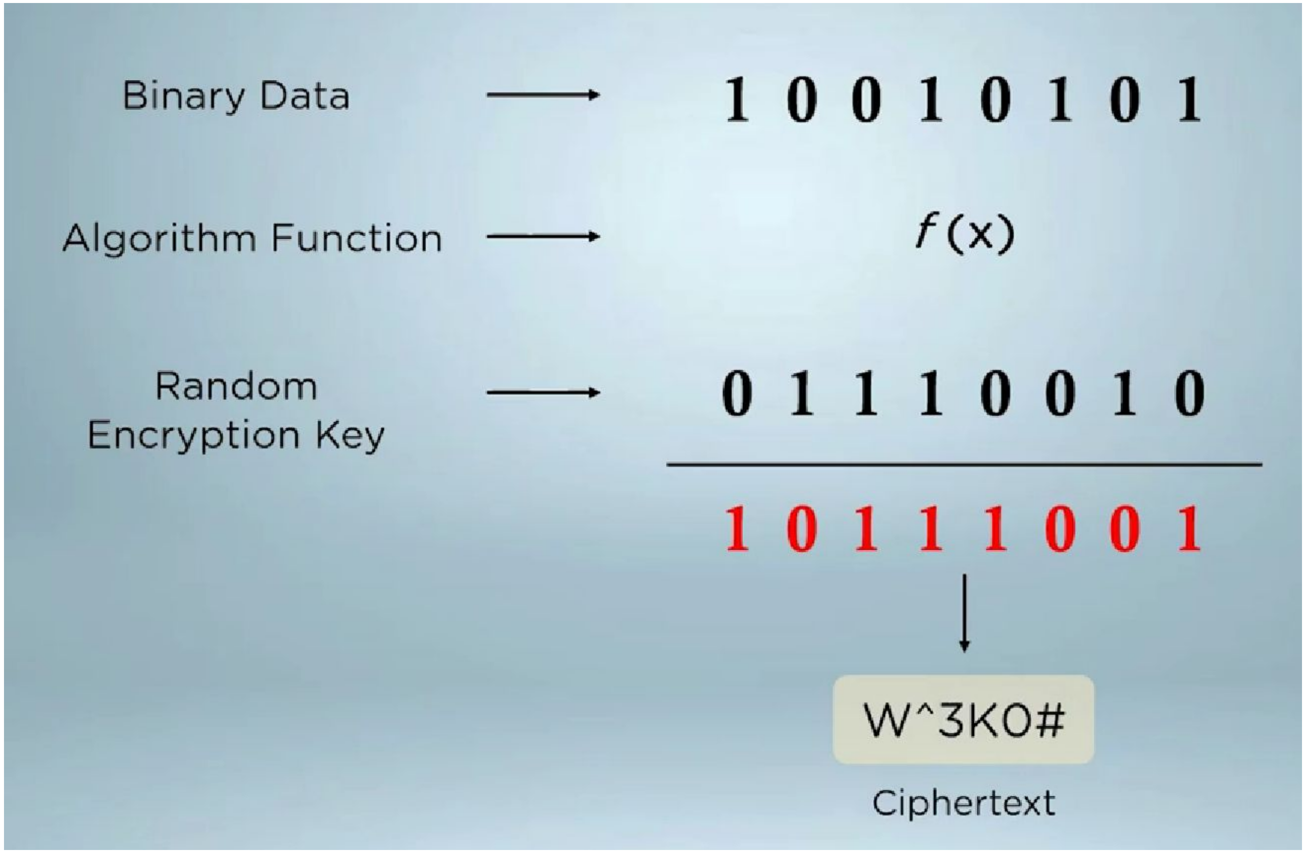
- Encryption can be done as either involves 3 distinct mechanisms
  - **Stream Ciphers**
  - **Block Ciphers**

Stream Ciphers

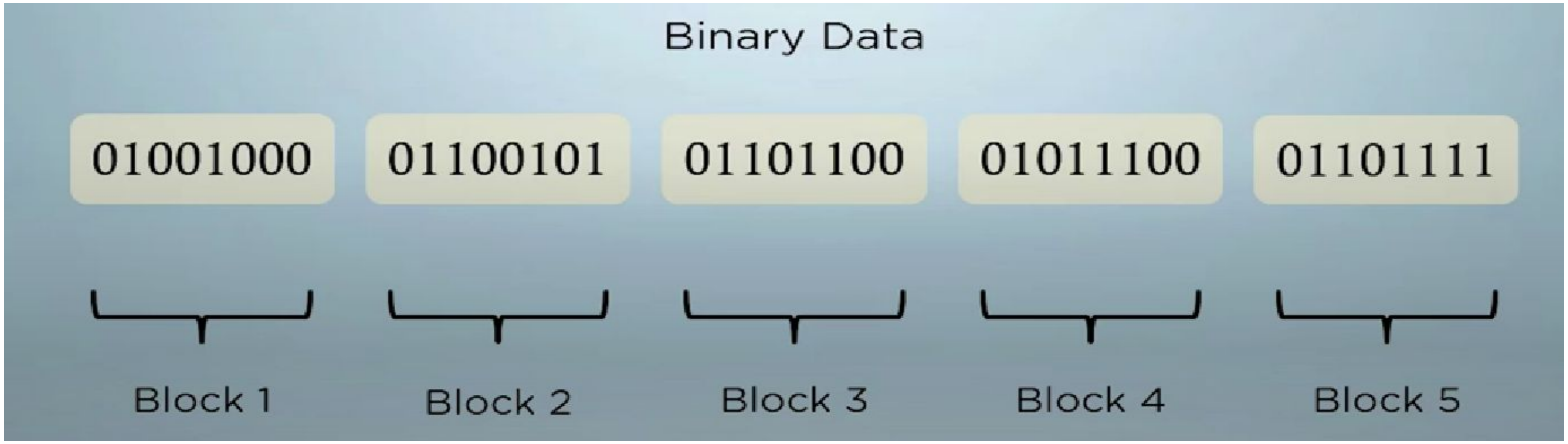


- Encrypt information one bit/byte at a time
- Quicker Format of Encryption
- Data is converted to binary digits and encrypted sequentially
- Popular algorithms- RC4, Salsa20

Stream Ciphers

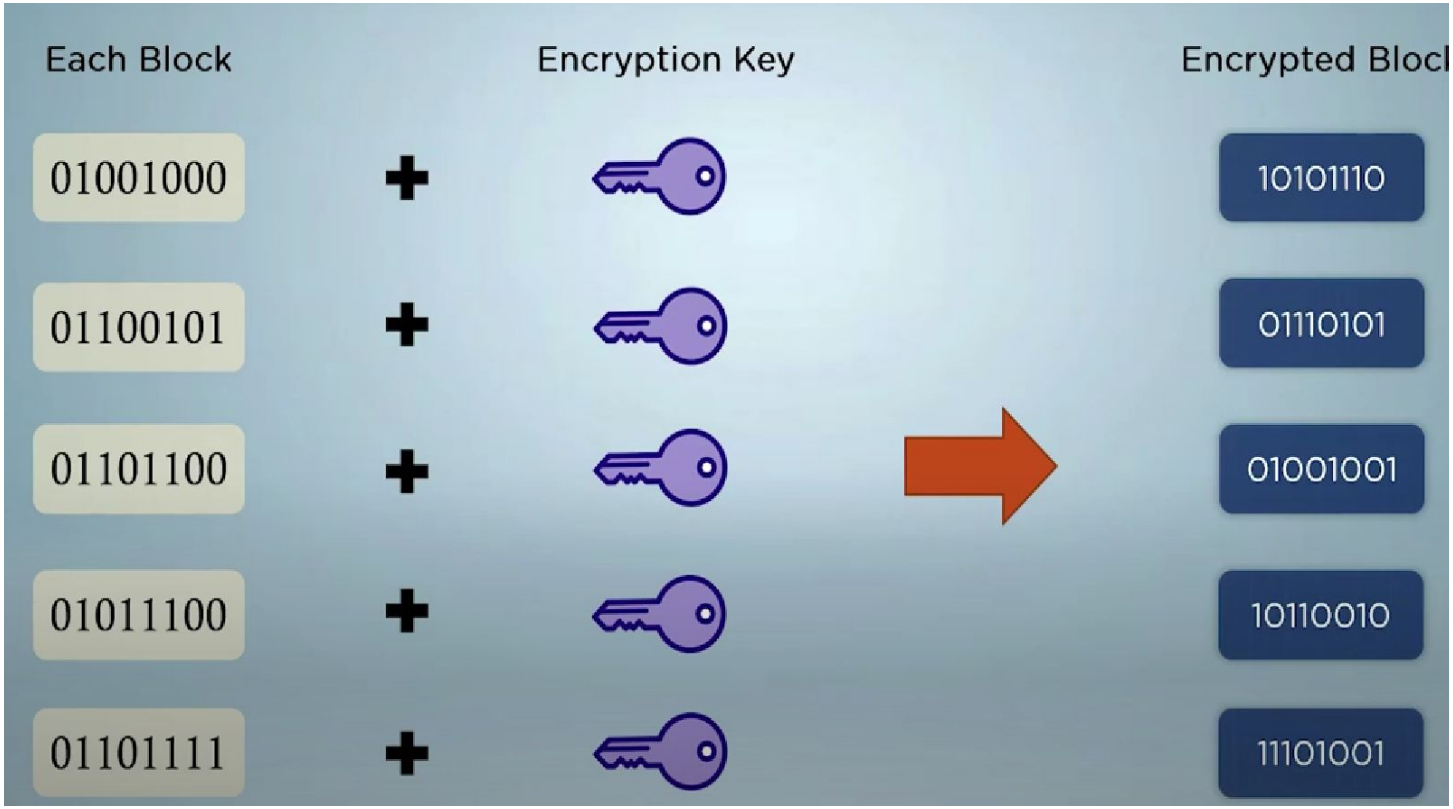


Block Ciphers

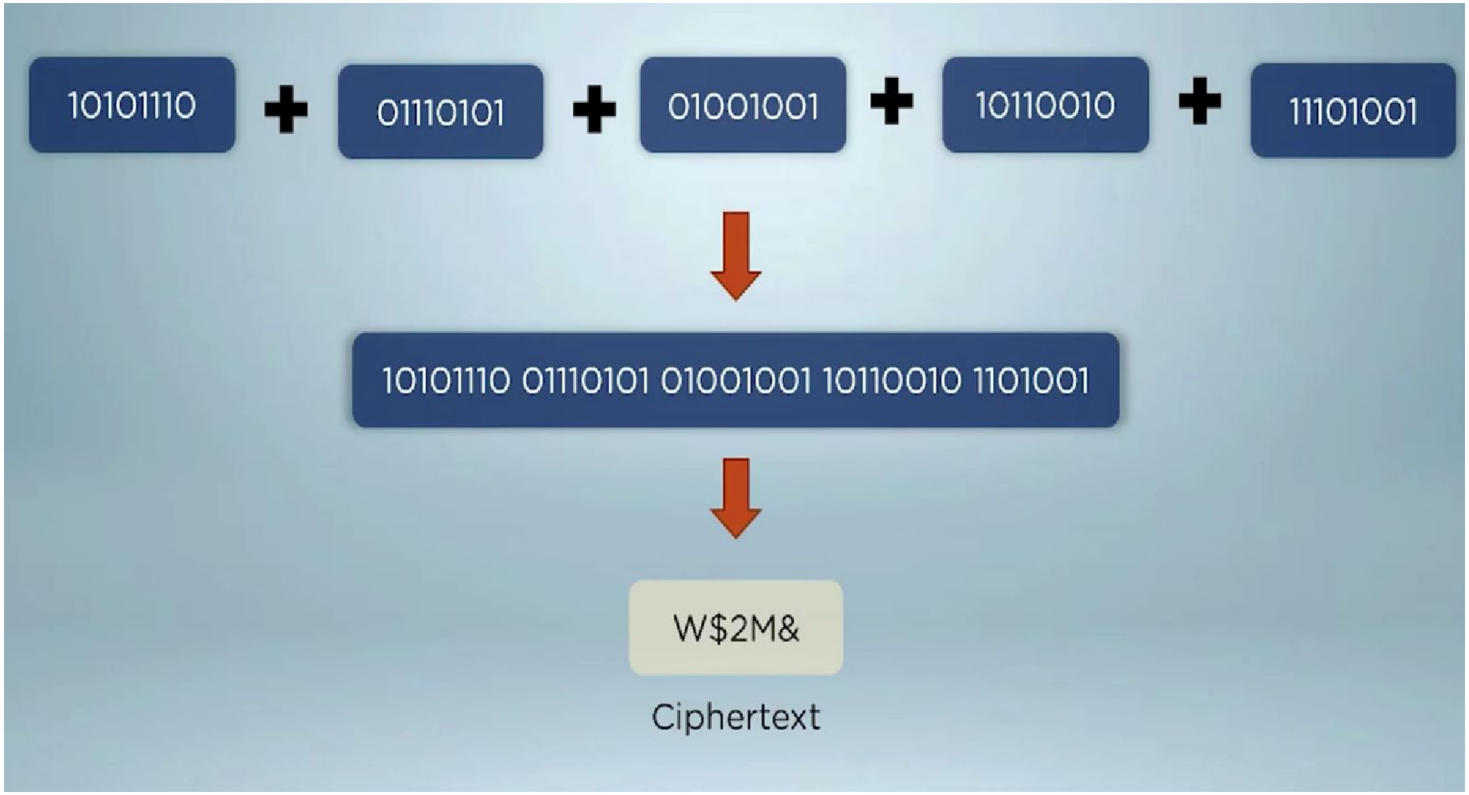


- Information broken down to chunks/blocks of fixed size
- Size of block depends on key size
- The chunks are encrypted and later chained together
- Popular algorithms- AES, DES, 3DES

Block Ciphers



Block Ciphers



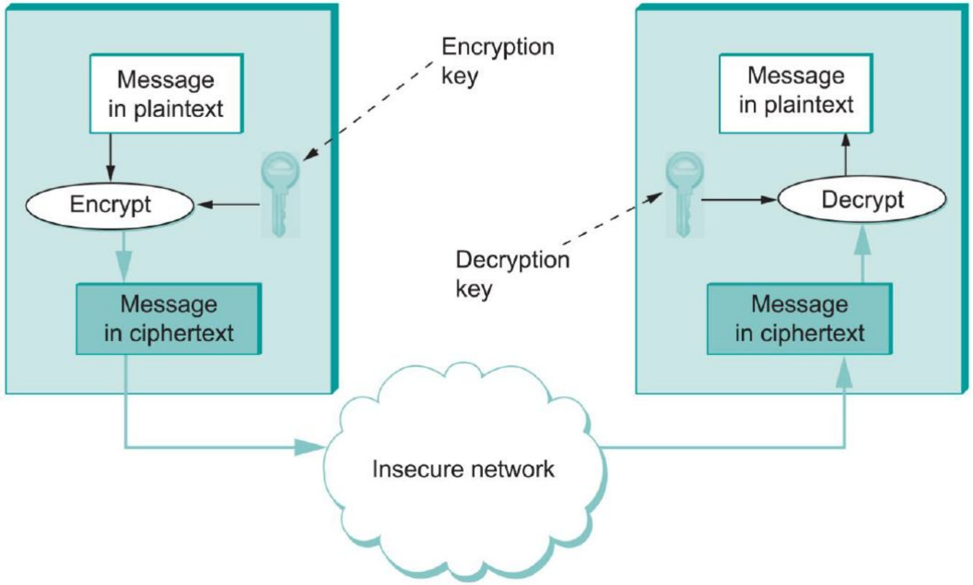
Cryptographic Techniques

Cryptographic Techniques

- Cryptography involves 3 distinct mechanisms
  - **Symmetric key Encipherment**
  - **Asymmetric key Encipherment**
  - **Hashing**

Symmetric Key Ciphers (secret-key)

Secret-key Encryption and Decryption



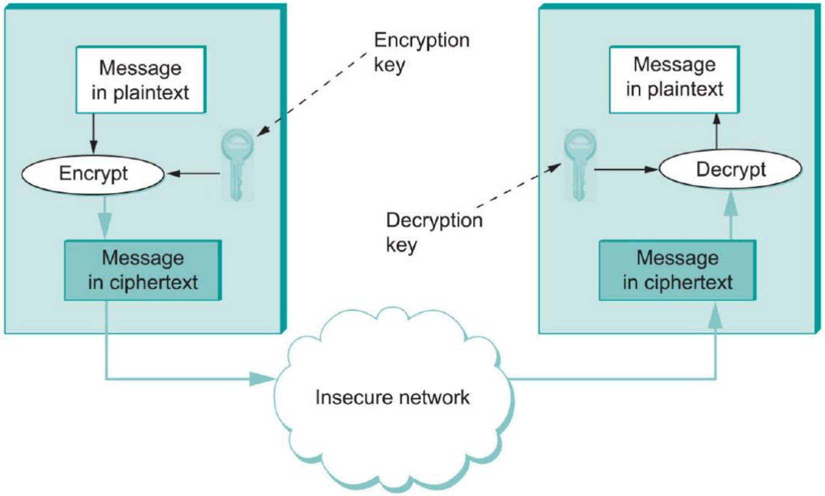
Plain text is the original, unencrypted information or data.

Cipher text is the result of applying an encryption algorithm to the plain text; it appears scrambled or unreadable without the appropriate decryption key.

- The **transformation** represented by an **encryption** function and its corresponding **decryption** function is called a **cipher**.
- Encryption and decryption functions have to be parameterized by a key and the functions are considered to be public knowledge—only the key needs to be secret.
- The **ciphertext** produced for a given **plaintext** message depends on both the **encryption function** and the **key**.

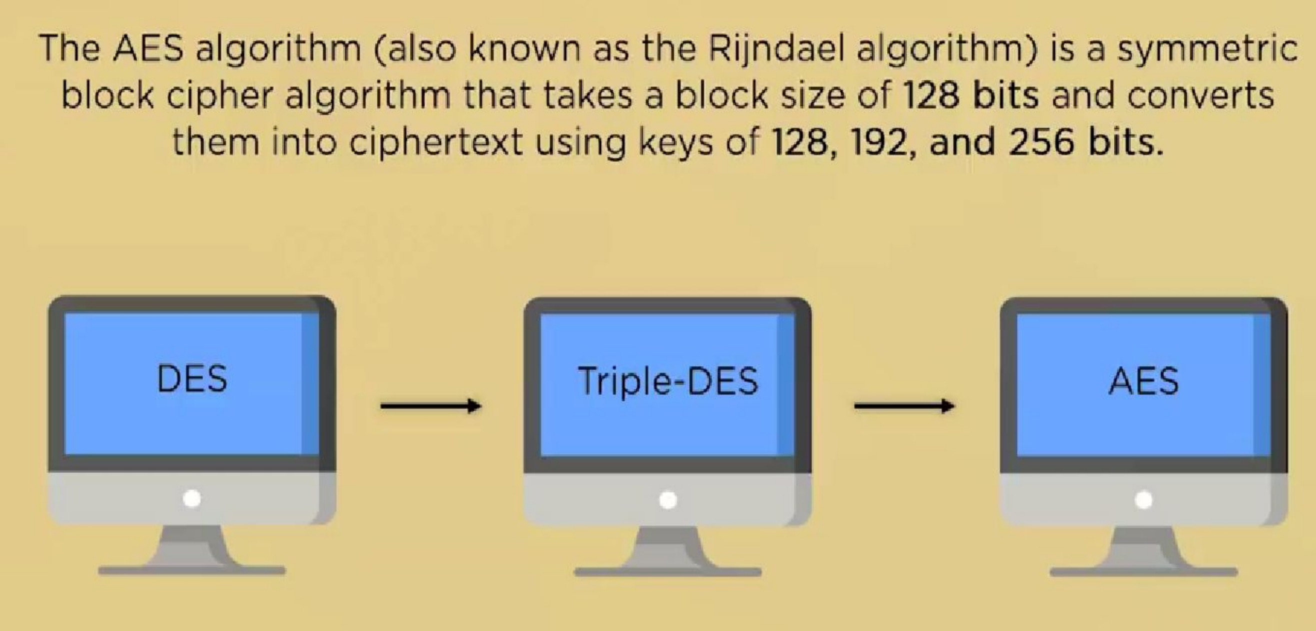
Secret-key Encryption and Decryption

- Here, **both participants** in a communication **share** the **same key**.
- **Secret-key** ciphers are also known as **symmetric-key** ciphers.
- Advanced Encryption Standard (**AES**) standard issued by NIST.



- AES supports key lengths of 128, 192, or 256 bits, and the block length is 128 bits. AES permits fast implementations in both software and hardware.
- It does not require much memory, which makes it suitable for small mobile devices.
- It is used to securely encrypt data in fixed-size blocks (often 128 bits).
- AES has some mathematically proven security properties and, has not suffered from any significant successful attacks.

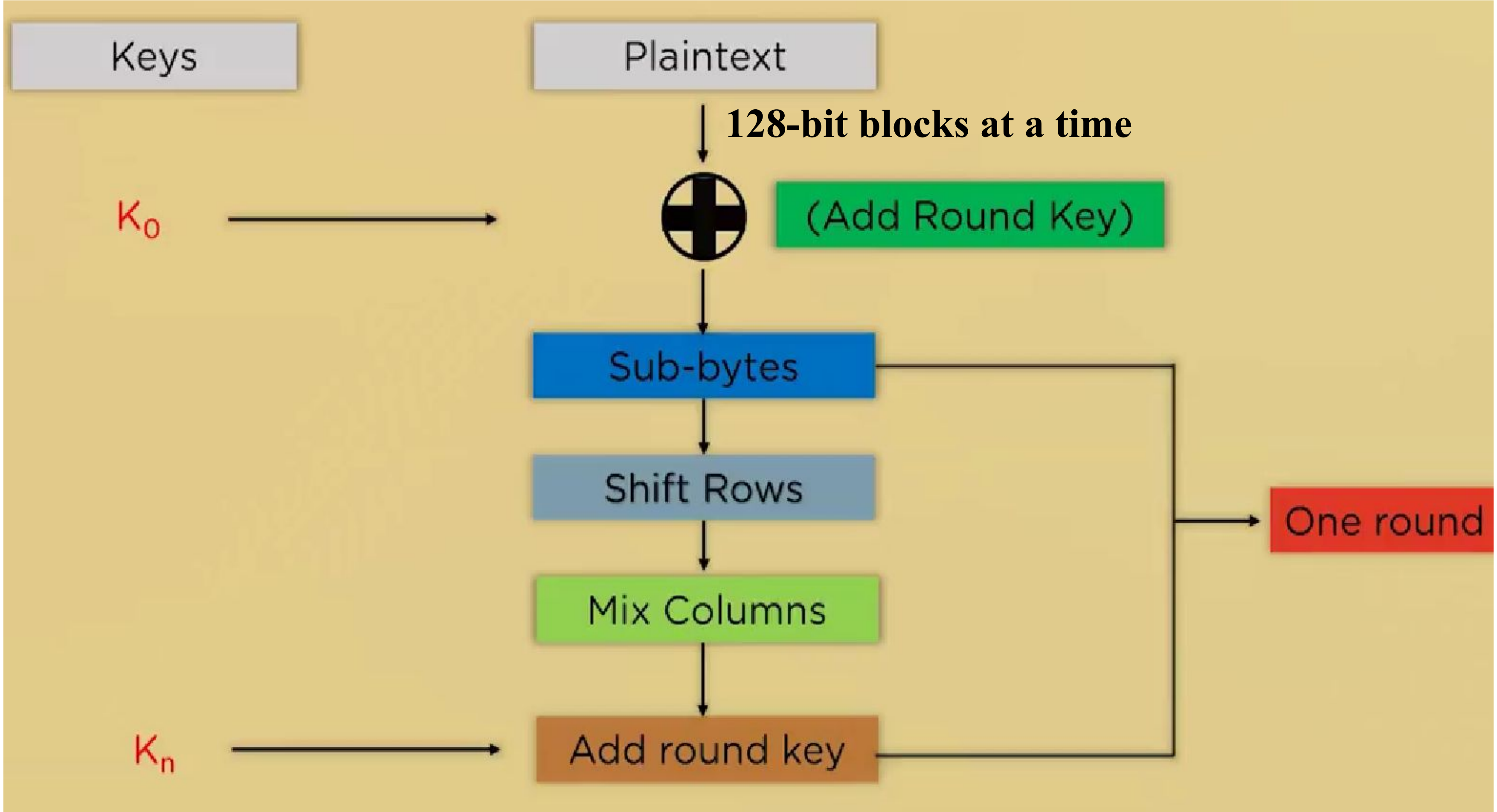
AES (Advanced Encryption Standard)



The AES algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm that takes a block size of 128 bits and converts them into ciphertext using keys of 128, 192, and 256 bits.

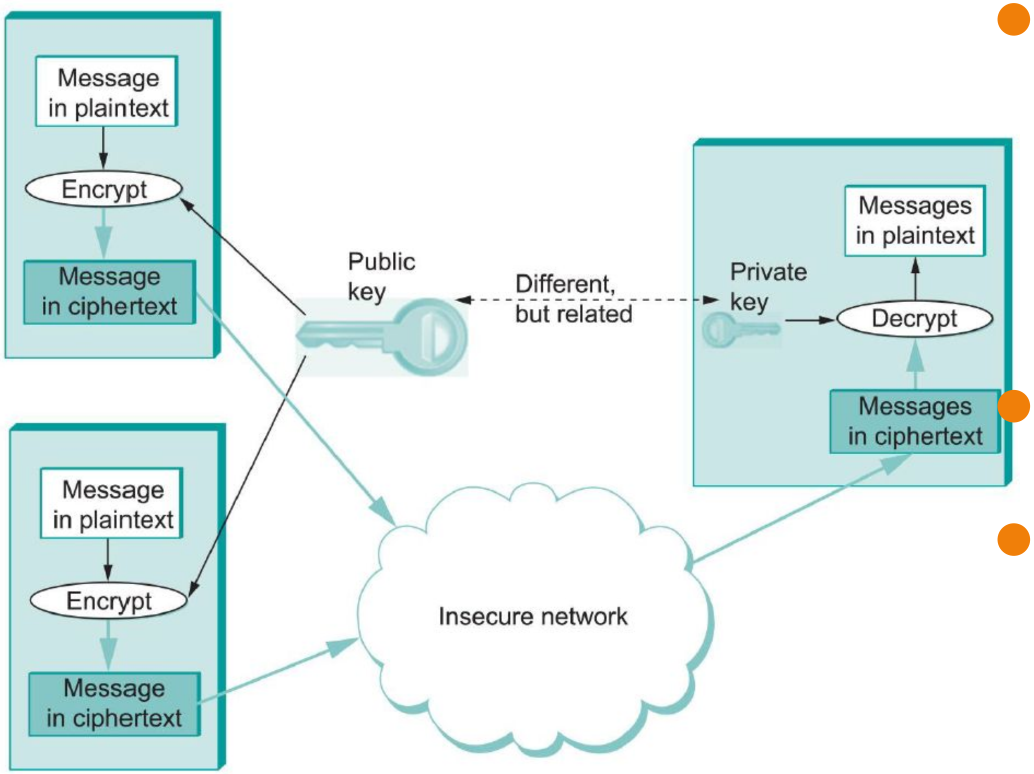
AES encrypts data by processing it in **128-bit blocks** using a **secret key**, employing **multiple rounds of operations** like byte **substitution**, **row shifting**, **column mixing**, and **adding the round key.**

AES


Keys
Plaintext
128-bit blocks at a time
K_0
(Add Round Key)
Sub-bytes
Shift Rows
Mix Columns
One round
K_n
Add round key

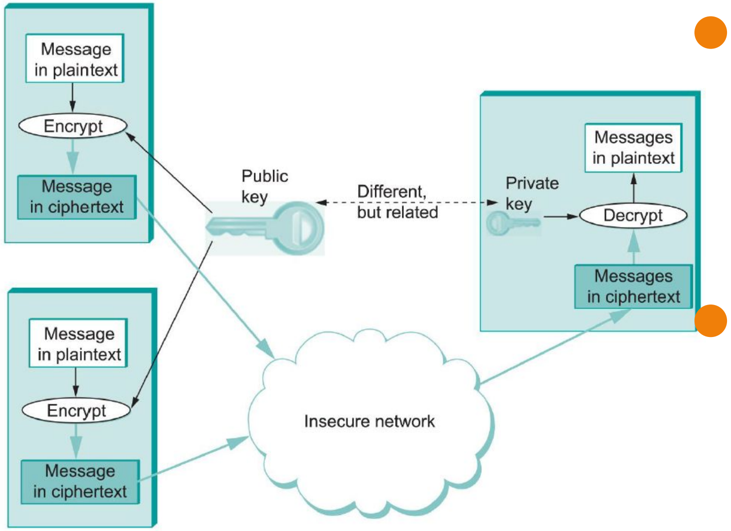
Asymmetric Key Ciphers (private and public keys)

Public-key Encryption and Private-key Decryption



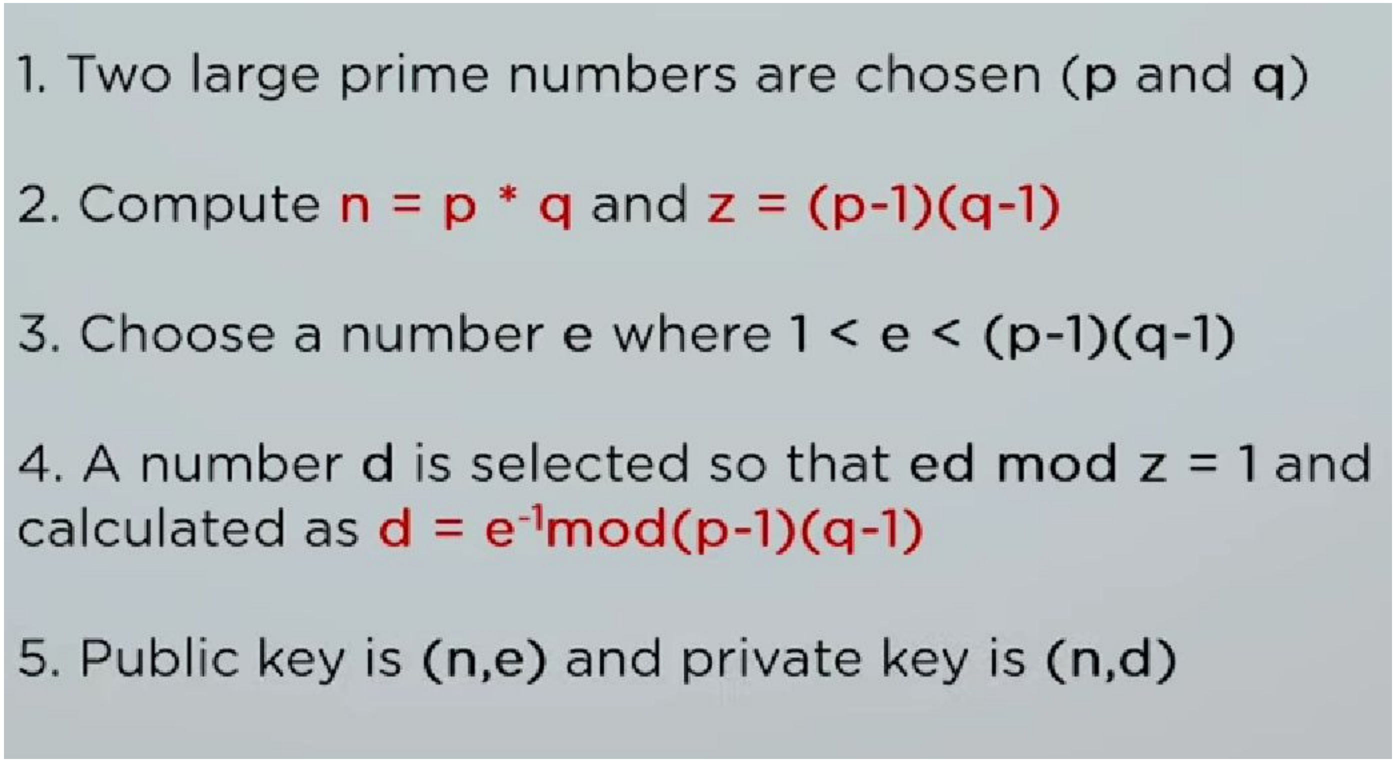
- Instead of a single key shared by two participants, a **public-key cipher** uses a **pair of related keys**, one for encryption and a different one for decryption.
- The pair of keys is "owned" by just one participant.
- The **owner** keeps the **decryption key secret** so that only the owner can decrypt messages; that key is called the **private key**.
- The **owner** makes the **encryption key public** so that anyone can **encrypt messages** for the owner; that key is called the **public key**.
- Obviously, for such a scheme to work, it must not be possible to deduce the private key from the public key.

Public key Encryption and Private key Decryption



- Any participant can get the public key and send an encrypted message to the owner of the key, and only the owner has the private key necessary to decrypt it.
- If we think of keys as defining a communication channel between participants, secret-key cipher provides a channel that is two-way between two participants.
- In secret-key, each participant holds the same (symmetric) key that either one can use to encrypt or decrypt messages in either direction.
- A public/private key pair, in contrast, provides a channel that is one-way and many-to-one: from everyone who has the public key to the unique owner of the private key.
- In public-key, for two-way confidentiality between two participants, each participant needs its own pair of keys, and each encrypts messages using the other's public key.

RSA- Key Generation - Info



1. Two large prime numbers are chosen (p and q)

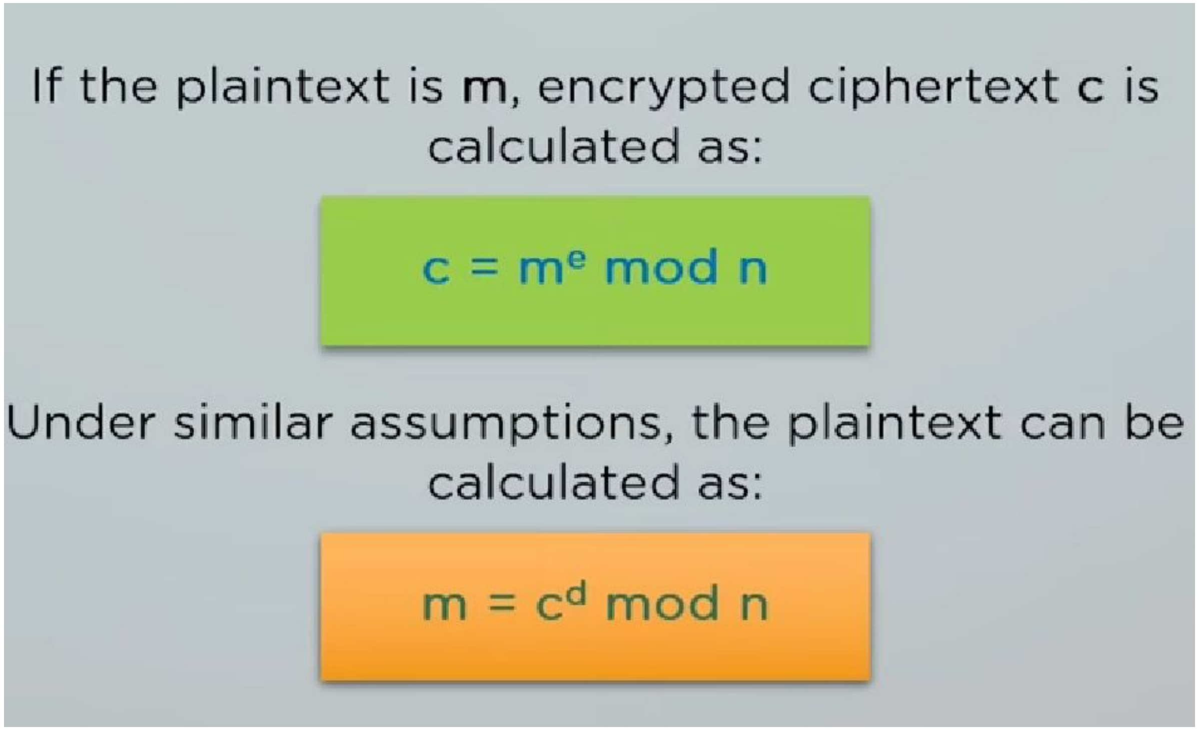
2. Compute $n = p * q$ and $z = (p-1)(q-1)$

3. Choose a number e where $1 < e < (p-1)(q-1)$

4. A number d is selected so that $ed \bmod z = 1$ and calculated as $d = e^{-1} \text{mod} (p-1)(q-1)$

5. Public key is (n,e) and private key is (n,d)

RSA- Encryption & Decryption - Info



If the plaintext is m, encrypted ciphertext c is calculated as:

$$c = m^e \bmod n$$

Under similar assumptions, the plaintext can be calculated as:

$$m = c^d \bmod n$$

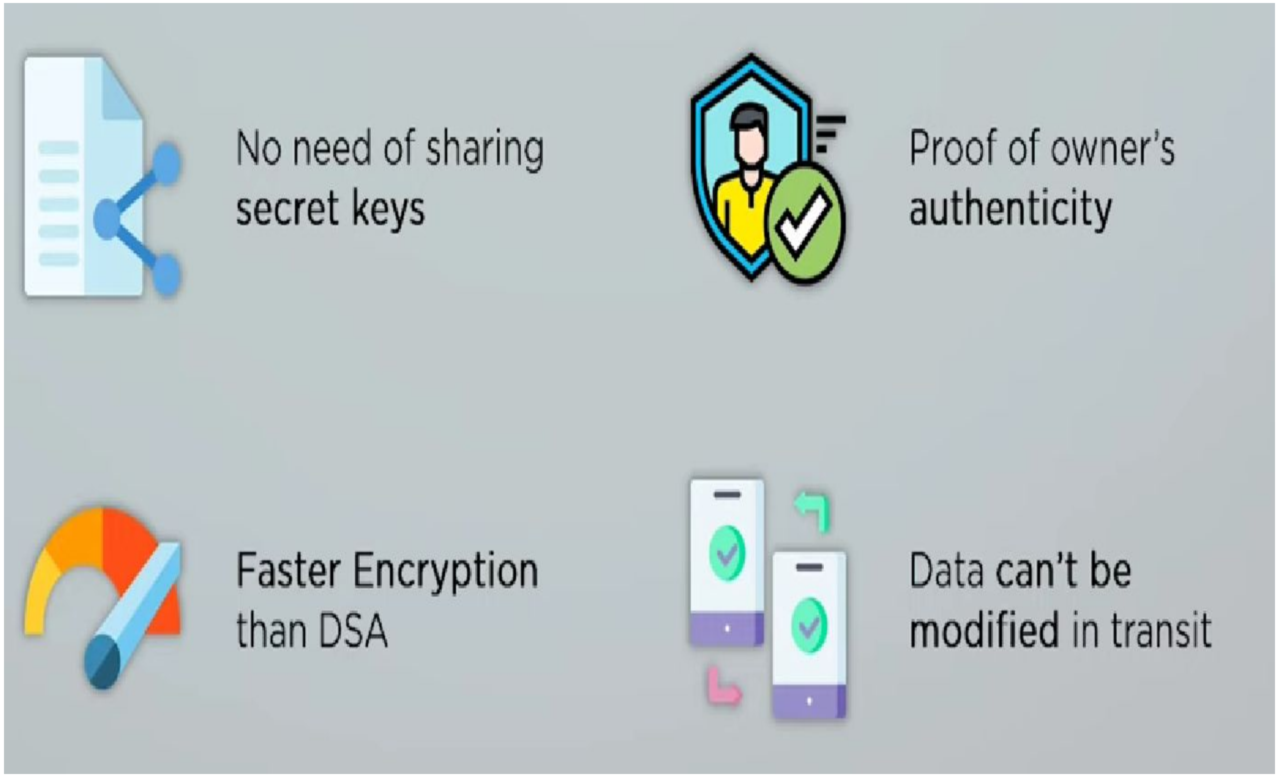
Note:
Calculate **Euler's totient** function:
$\boldsymbol{\varphi(n) = (p-1)\times(q-1)}$

1. Pick two **large prime numbers**, say **p** and $\boldsymbol{q}$.
2. Compute their product: $\boldsymbol{n = p \times q}$

Note: This **n** is part of both the **public** and private **keys**.

3. $\boldsymbol{e}$ is **co-prime**
4. **d** as the **modular multiplicative inverse** of e mod $\varphi(n)$

RSA- Advantages



No need of sharing secret keys

Proof of owner's authenticity

Faster Encryption than DSA

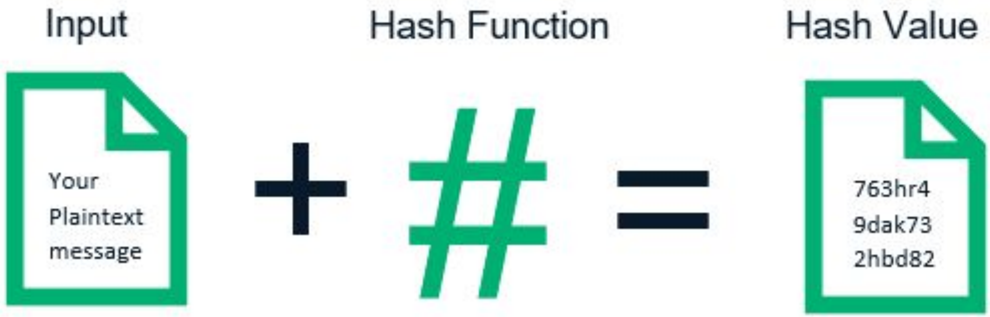
Data can't be modified in transit

DSA: Digital Signature Algorithm

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

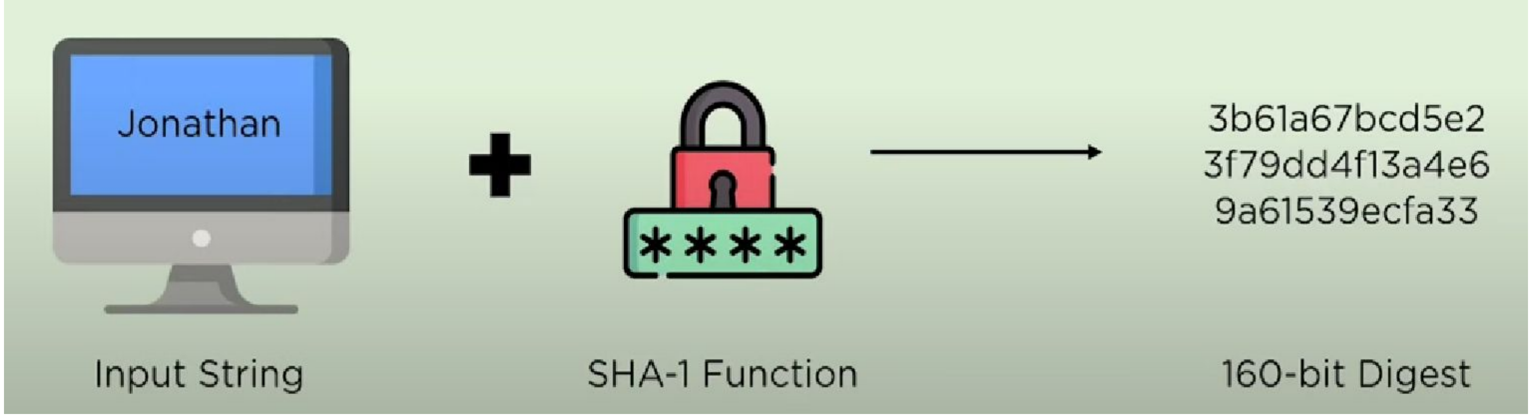
Hashing

Hashing



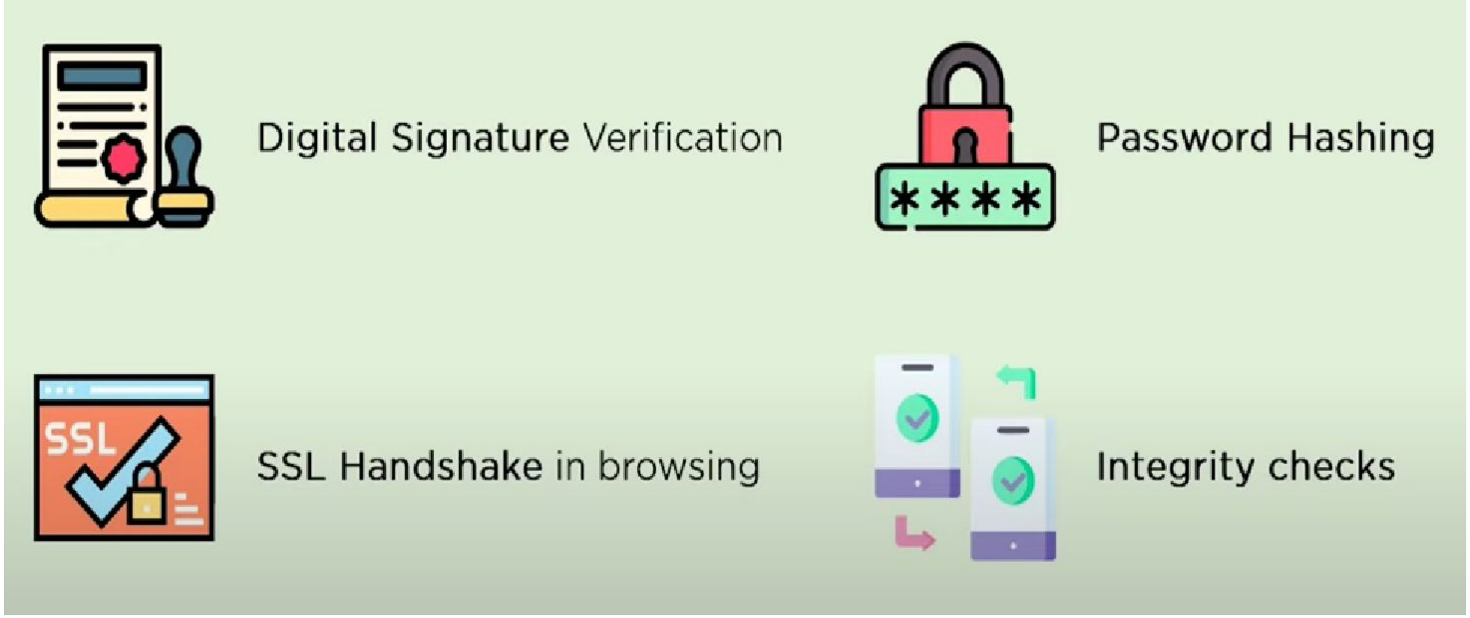
- In hashing, a **fixed length message digest** is created out of a variable length message.
- The digit is normally **much smaller** than the message.
- Hashing is used to provide **check values.**

Hashing-SHA



- Secure Hash Algorithm
- Has Multiple families such as SHA-0, SHA-1, SHA-2, SHA-3

Applications of SHA



Digital Signature Verification

Password Hashing

SSL Handshake in browsing

Integrity checks

Introduction to Post Quantum Cryptography