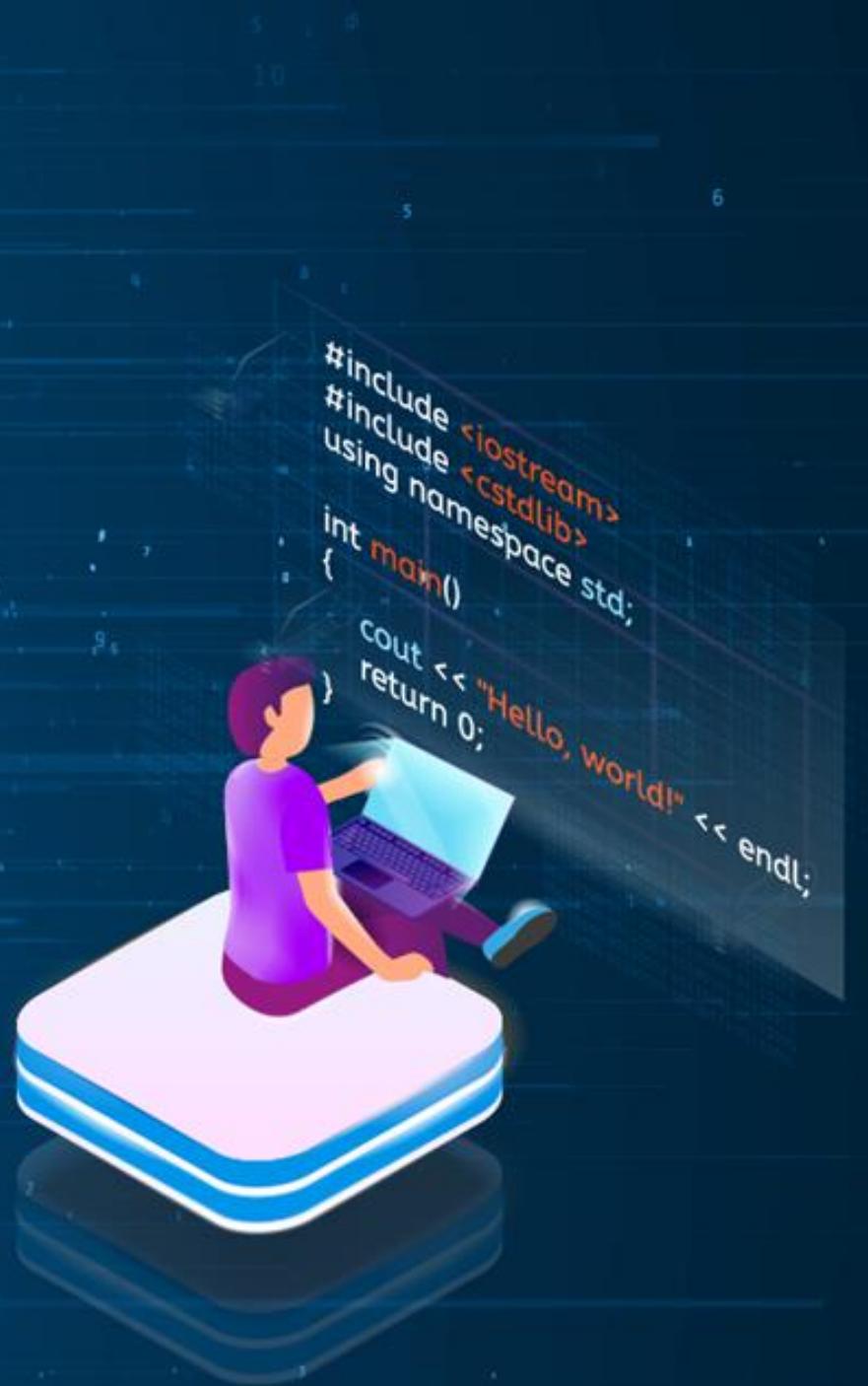




CompTIA Security + 701

Domain 1: General Security Concepts



```
#include <iostream>
#include <cstdlib>
using namespace std;

int main()
{
    cout << "Hello, world!" << endl;
    return 0;
}
```

Learning Objectives

By the end of this lesson, you will be able to:

- Identify security concepts to protect data, ensure availability, and mitigate cyber threats effectively
- Compare and contrast various types of security controls to optimize protection against cyber threats
- Interpret personnel security to safeguard networks against threats
- Discover the importance of change management processes and their impact on security to maintain operational stability
- Identify the importance of using appropriate cryptographic solutions to secure data and communications effectively



TECHNOLOGY

Introduction to Security Concepts

What Is Information Security?

Information security, often called InfoSec, is the practice of protecting information by mitigating information risks.



It is about safeguarding data from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information can be anything valuable, including customer data, financial records, intellectual property, personal details, and even classified government information.

Why Information Security?

- With digital transformation and integration comes a heightened risk of cyber threats.
- Cybersecurity is not just an IT issue; it is also a business and personal concern.
- From identity theft to financial fraud, the repercussions of a security breach can be far-reaching and devastating.
- The advent of artificial intelligence and deepfakes has added fuel to the fire and worsened the situation.



Factors Impacting Information Security



Nature of business



Security culture



Legal and regulatory compliance



Management support

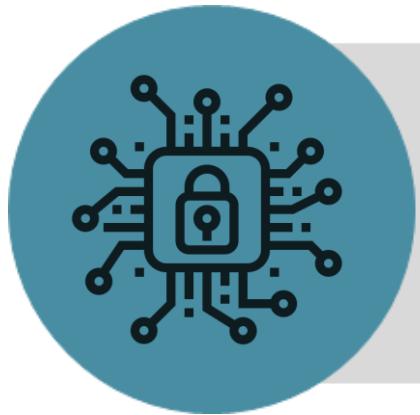


Risk appetite



Industry threats

Cybersecurity



Cybersecurity is the process of securing sensitive data and critical systems from cyber threats.

- It refers to anything intended to protect enterprises from intentional attacks, breaches, incidents, and consequences.
- It can also be defined as protecting information assets by addressing threats to information processed, stored, and transported by internetworked information systems.



Goal of Cybersecurity



The primary objective of cybersecurity is to preserve the confidentiality, integrity, and availability of an organization's critical assets from attack, damage, or unauthorized access.

Why Is Cybersecurity Important?



- Due to technological advancement, the rate of cybercrime is increasing.
- As most of the business happens online, there is an increasing demand to protect this data.
- The presence of crime syndicates, cyber armies, and financial frauds has also highlighted the importance of cybersecurity.

Difference Between Information Security and Cybersecurity

Information Security

- Information security deals with information regardless of its format.
- It encompasses paper documents, digital data, and intellectual property.

Cybersecurity

- Cybersecurity is a component of information security.
- It can be defined as the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.

Risks of Security on Business



Reputational and financial loss



Business interruption loss



Loss of customer confidence



Legal action against company



Intellectual property loss



Data breach

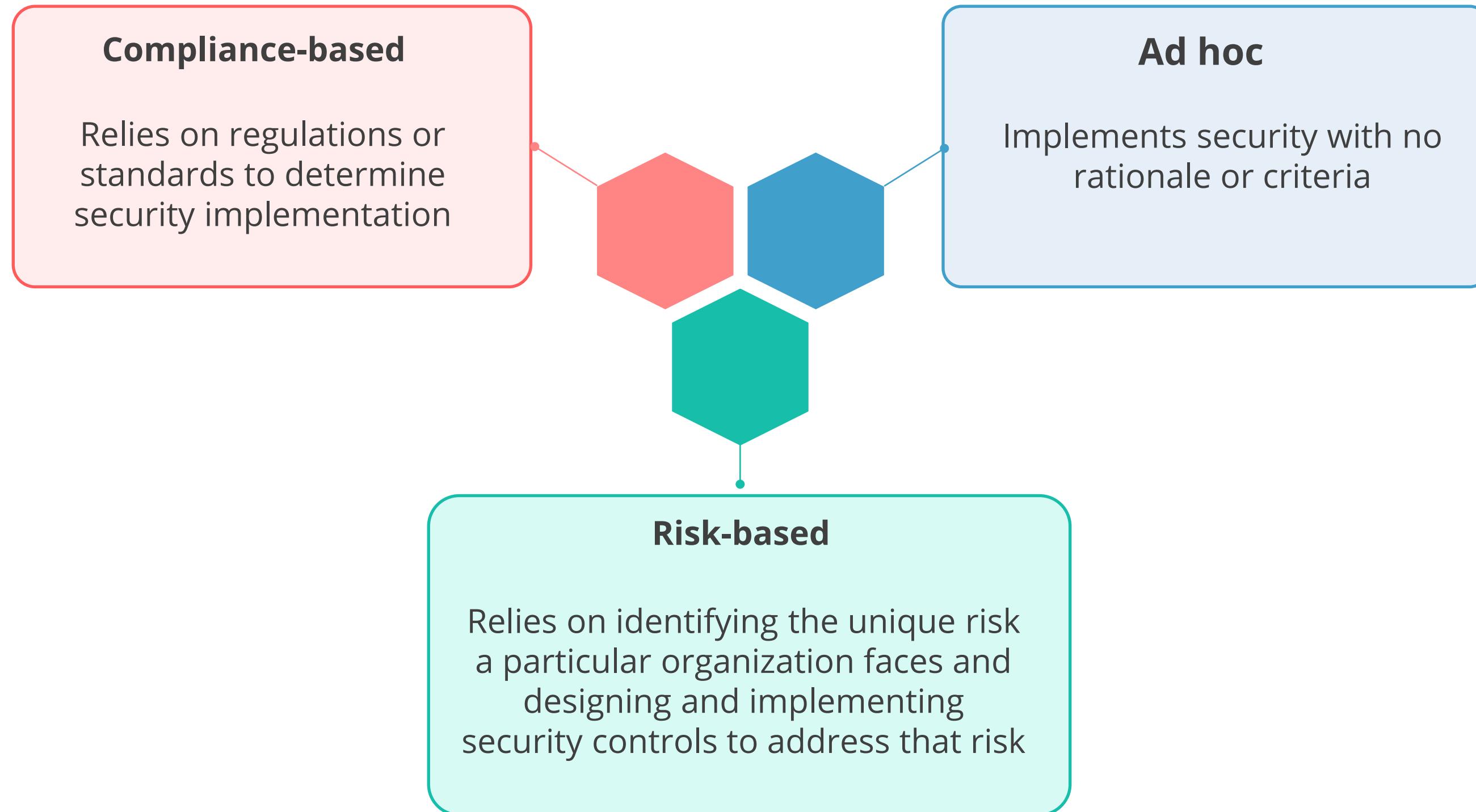
Terrifying Cybercrime Statistics

Recent trends that make Cybersecurity more important:

- During 2023, 5 billion data breaches were reported, compromising around 867 million records.
- Google blocked over 2.8 million bad apps from entering the Play Store in 2023.
- Ransomware attacks on the healthcare industry will quadruple.
- Cybercrime is expected to cost 23.84 trillion by 2025.
- There will be 350 billion passwords worldwide by 2025.
- More than 60% of fraud originates from mobile devices.
- Personal data sells for as little as \$0.20.
- 90% of hackers use encryption.



Approaches to Cybersecurity

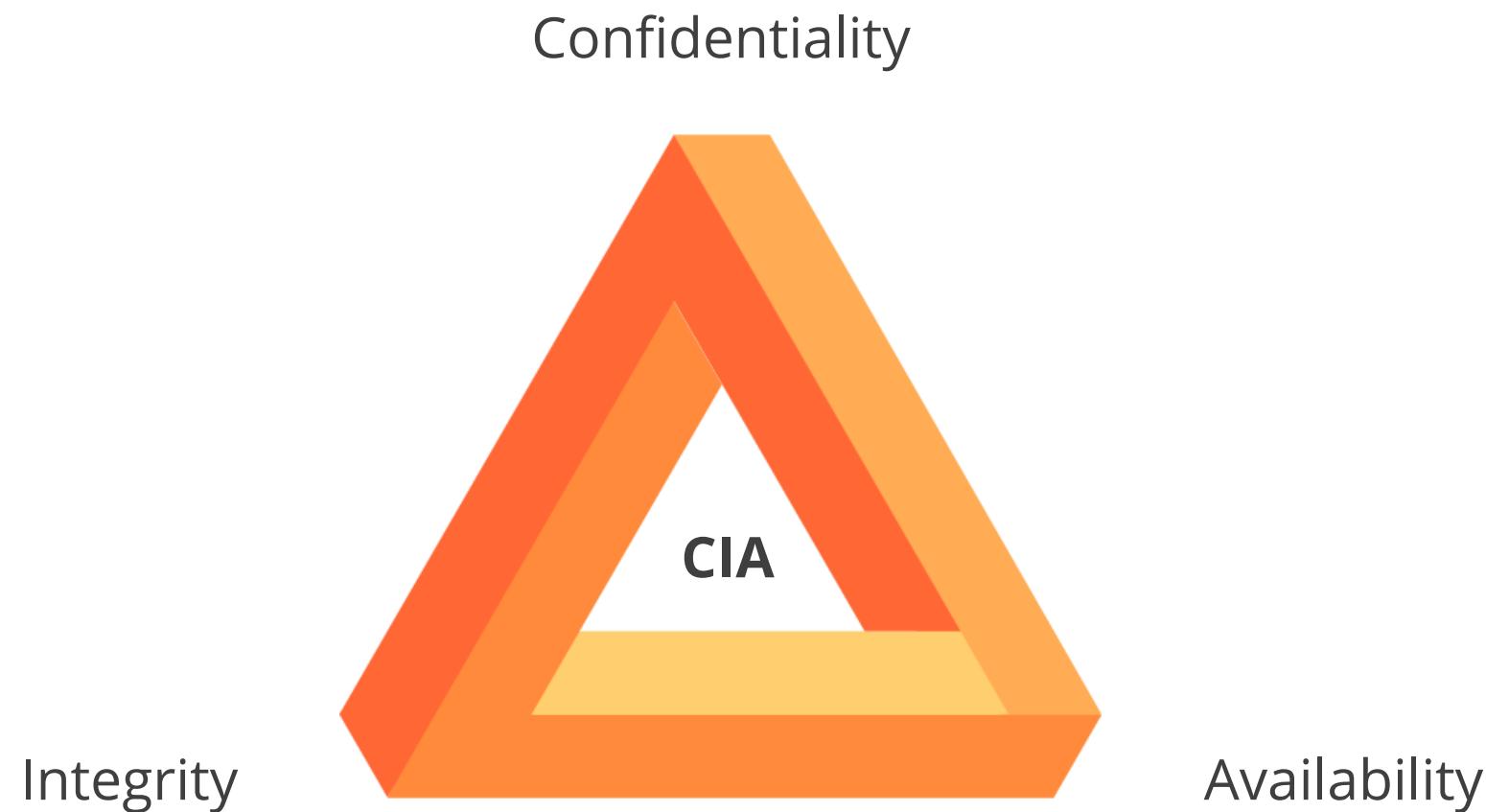


TECHNOLOGY

CIA

CIA Triad

This stands for confidentiality, integrity, and availability, which are the primary goals of cybersecurity.



CIA Triad: Confidentiality

Confidentiality means private or confidential information should not be disclosed to unauthorized individuals.



CIA Triad: Confidentiality



CIA Triad: Confidentiality

The following are some countermeasures to ensure confidentiality:

Encryption

Converts information to an unreadable format

Access control

Prevents users from accessing confidential information without permission

Administrative policies

Confidentiality policy and non-disclosure agreement (NDA) act as deterrent control

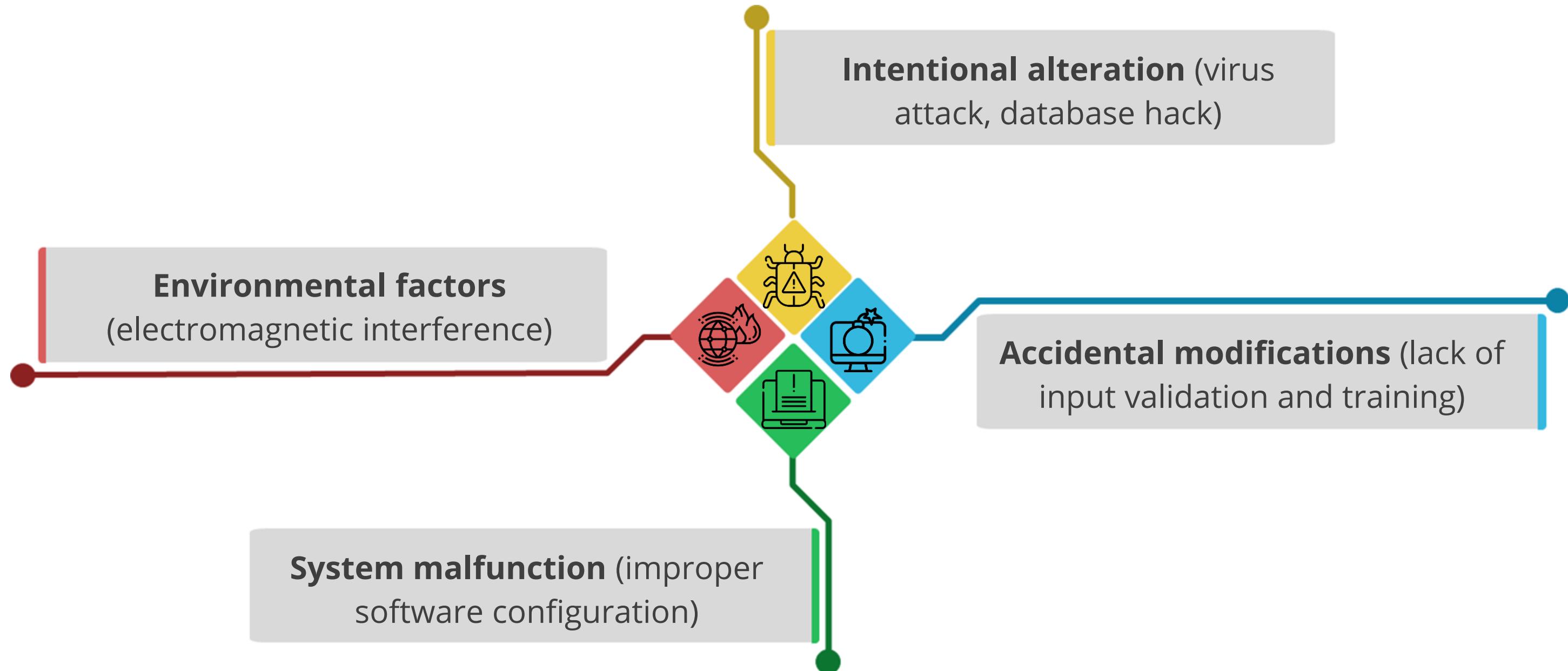
CIA Triad: Integrity

Integrity means that information or systems should be protected from intentional, unauthorized, or accidental changes.



CIA Triad: Integrity

Threats to integrity are:



CIA Triad: Integrity

The following are some countermeasures to ensure integrity:

~**Cryptographic hash**

Hash value of a file can be used to figure out if the file has been modified.

~**Checksums**

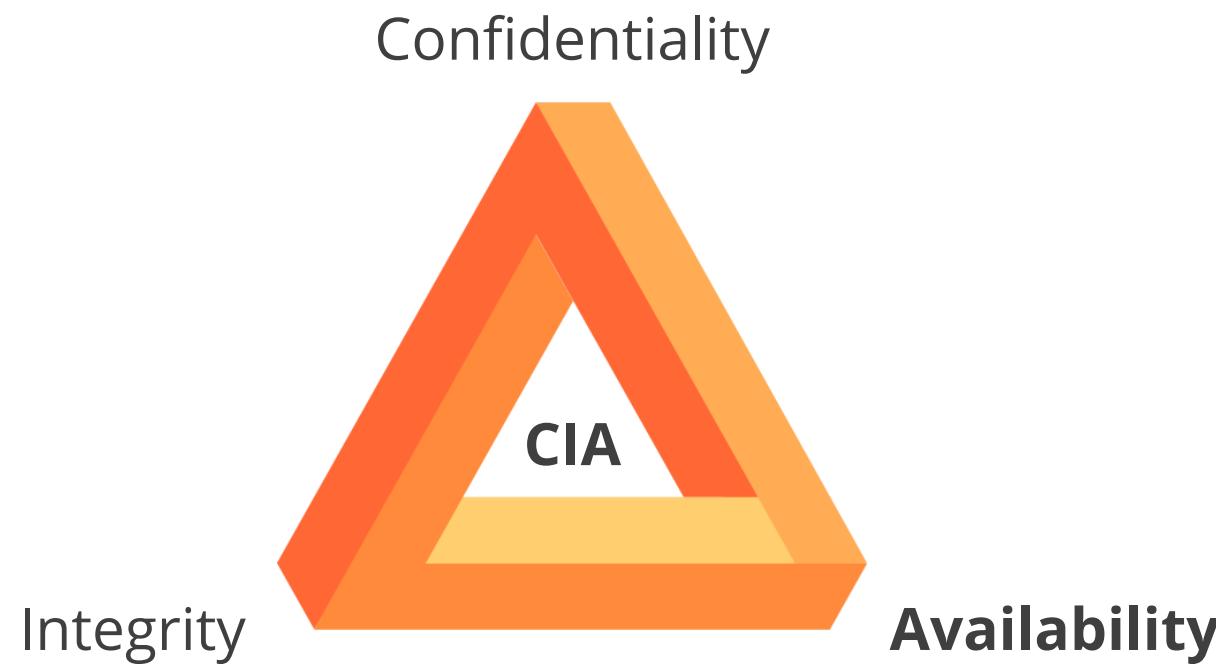
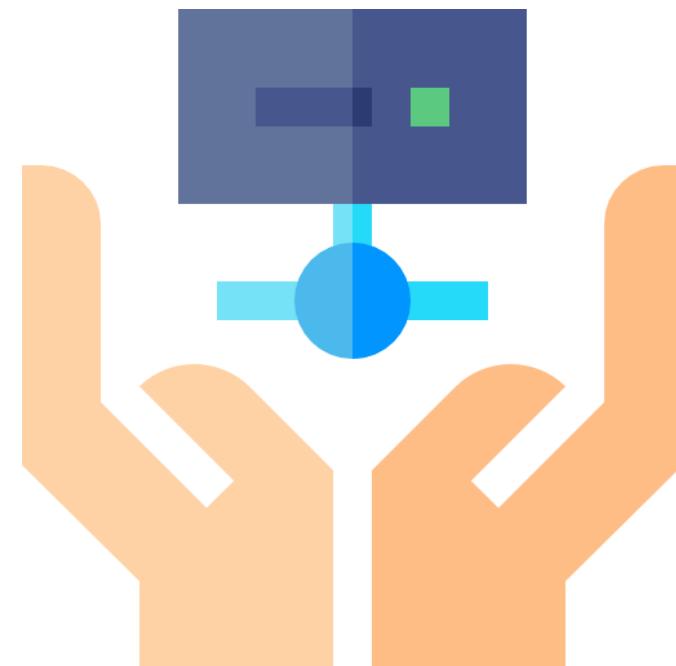
Checksums can detect errors and reconstruct missing data.

~**Database integrity**

Referential and entity integrity ensure logical consistency.

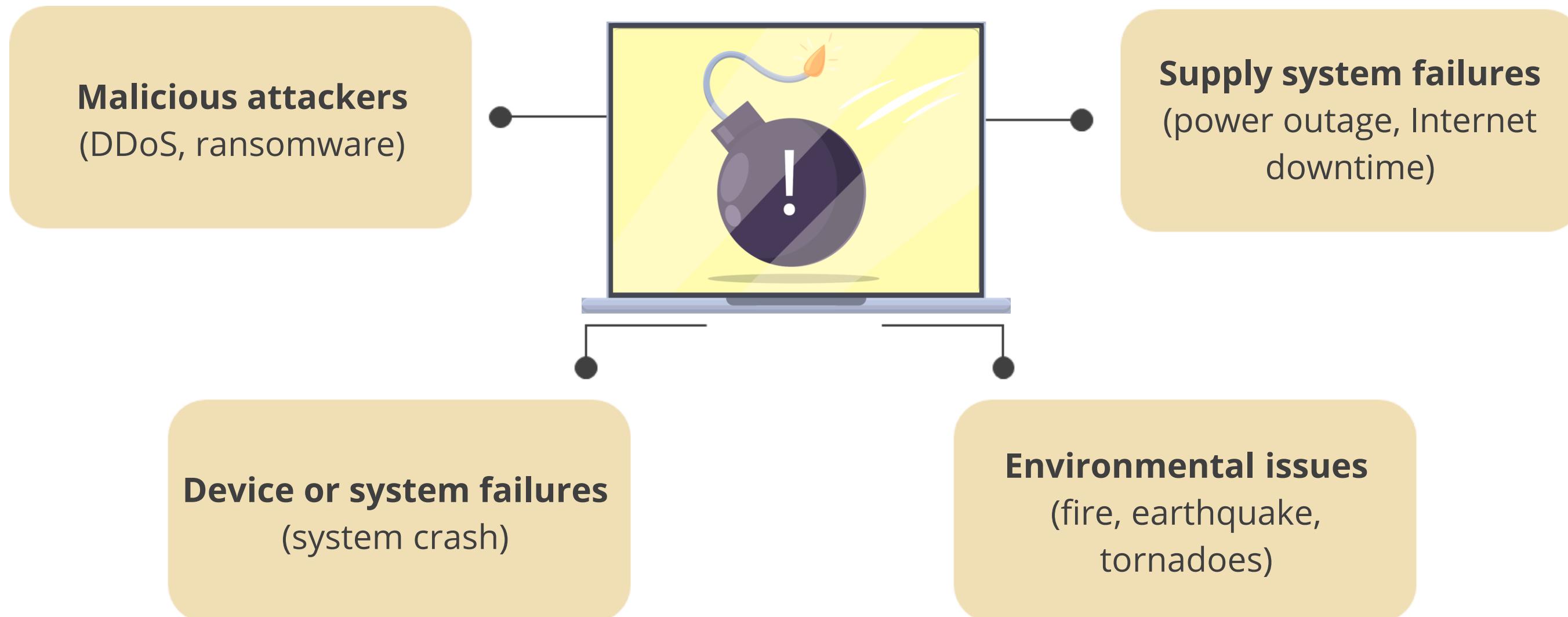
CIA Triad: Availability

Availability means systems or information must be available on demand according to agreed-upon parameters.



CIA Triad: Availability

Threats to availability are:



CIA Triad: Availability

The following are some countermeasures to ensure availability:

~ High availability

Ensure system availability at all times.

~Backup procedures

Ensure data restoration after a disaster

~ Security devices

Prevent DoS/DDoS attacks by deploying intrusion prevention system (IPS) and web application firewall (WAF)

TECHNOLOGY

Non-Repudiation

Non-Repudiation

Non-repudiation, in the context of cryptography and information security, refers to a service that provides proof that a particular action or event cannot be denied by anyone.

- This prevents denial of actions, ensuring accountability and reliability in electronic transactions and communications.
- Non-repudiation ensures proof of the origin and integrity of data exchanged between parties.

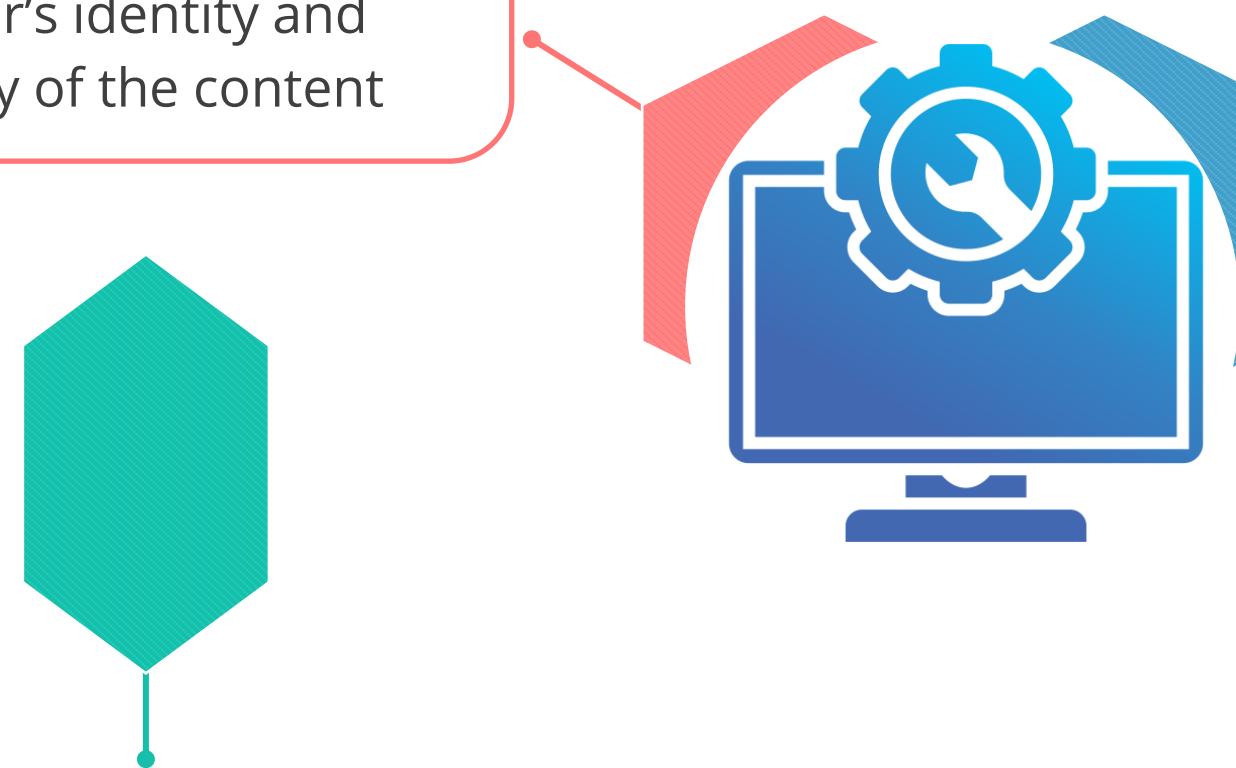


Tools for Non-Repudiation

Digital signature: Utilizes cryptographic identifiers to confirm the sender's identity and ensure the integrity of the content

Audit trail: Involves maintaining chronological records of actions, which are crucial for tracing events and assigning accountability to the parties involved

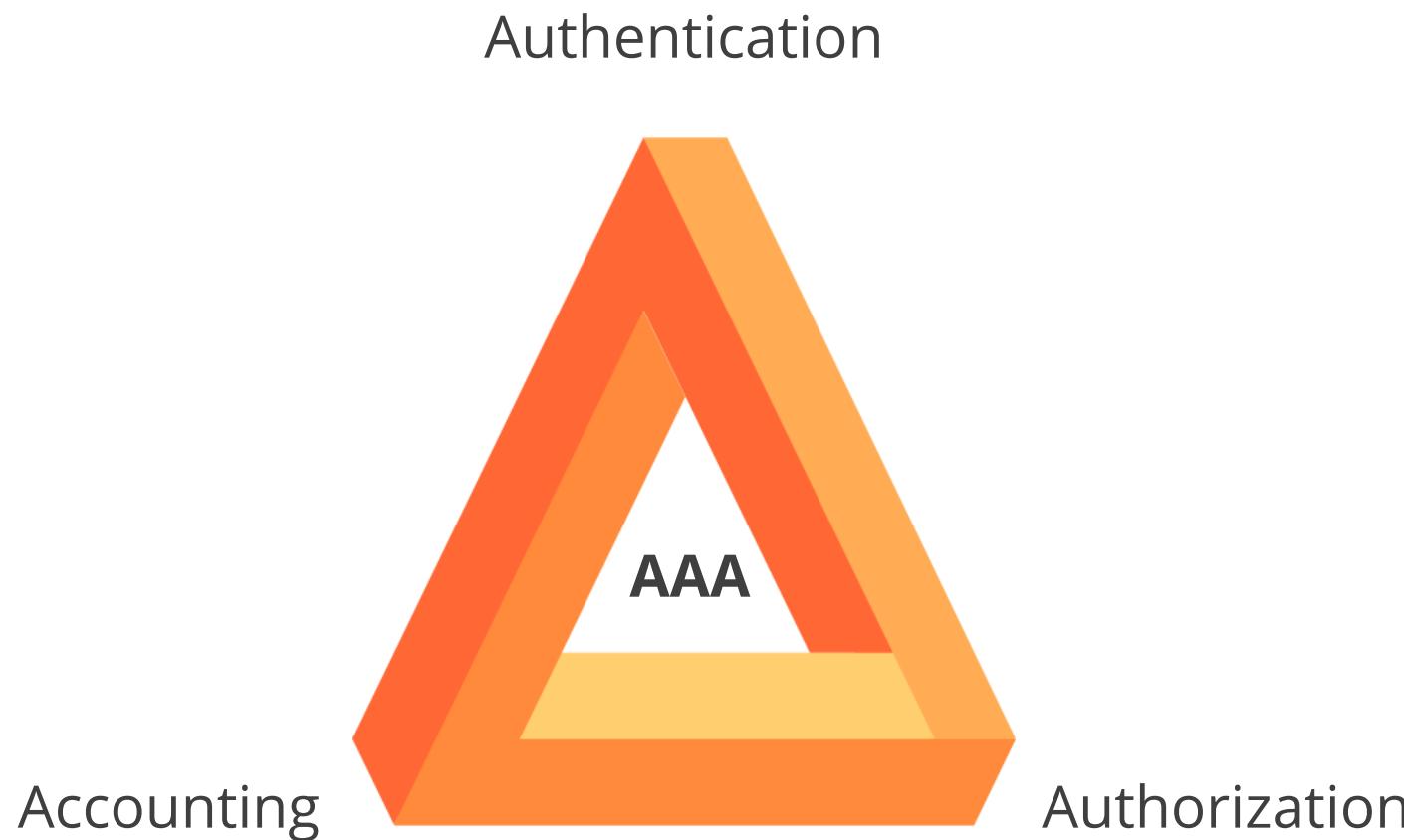
Secure timestamping: Involves a trusted third-party service that creates a verifiable record of the exact time a digital record was created



AAA (Authentication, Authorization, and Accounting)

AAA

In computer security, AAA stands for Authentication, Authorization, and Accounting.

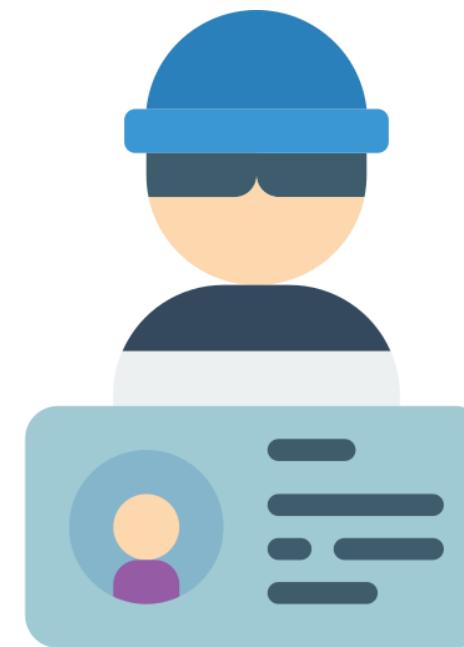


It is a framework that controls user access to networks and resources, ensuring only authorized users can access specific resources and monitor their activities.

Identification



The process of an individual claiming or professing an identity is known as identification.

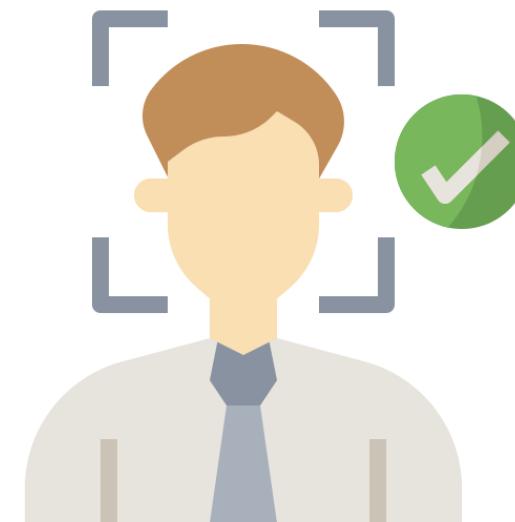


To begin the authentication, authorization, and accountability procedures, a subject must submit an identity to the system.

Authentication



Authentication is the process of comparing one or more criteria to a database of legitimate identities such as user accounts, to validate the subject's identity.



An example of identification and authentication is a username and password. Users identify themselves with usernames and authenticate with passwords.

Authorization

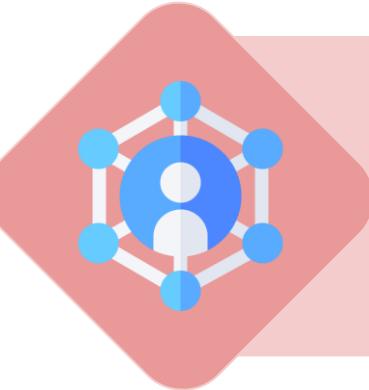


Authorization is the process of granting access to an object after the subject has been properly identified and authenticated.



Example: CRUD operations include create, read, update, and delete

Accounting

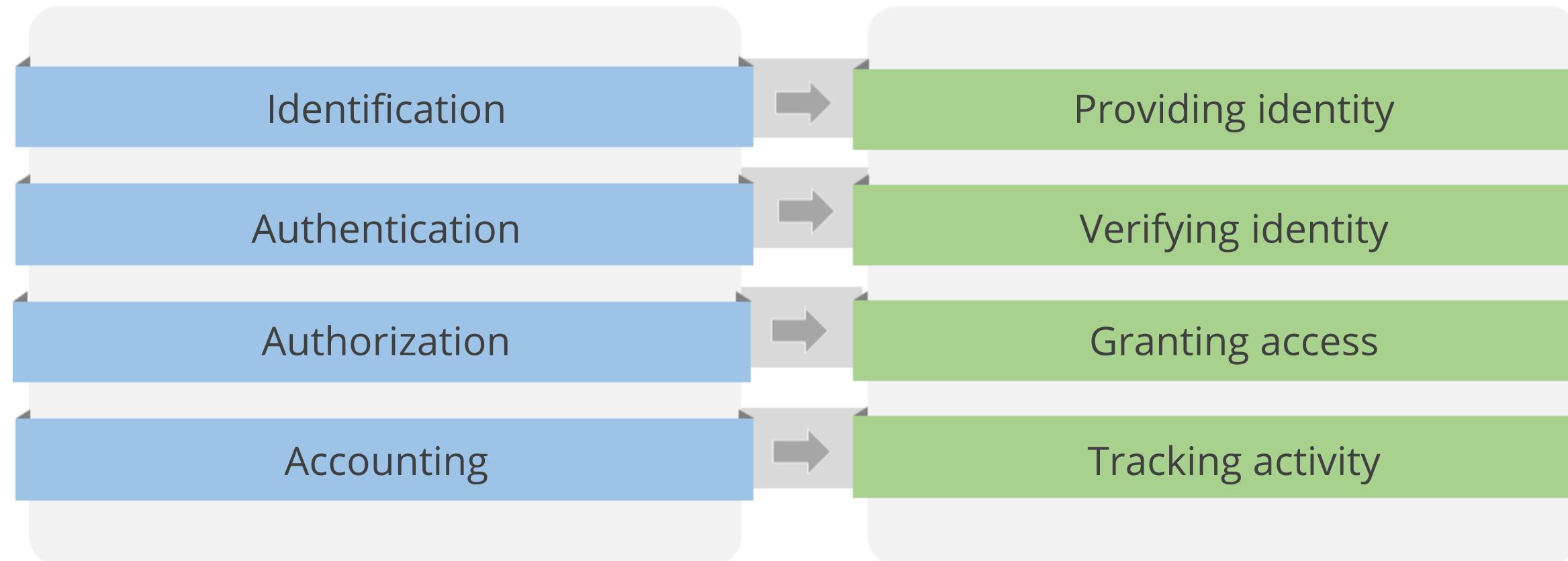


Accounting is the ability of a system to associate users and processes with their actions.



Example: Keeping a record of user activity like time of login, IP address, activities performed, and so on

AAA: Summary



Multi-Factor Authentication (MFA)

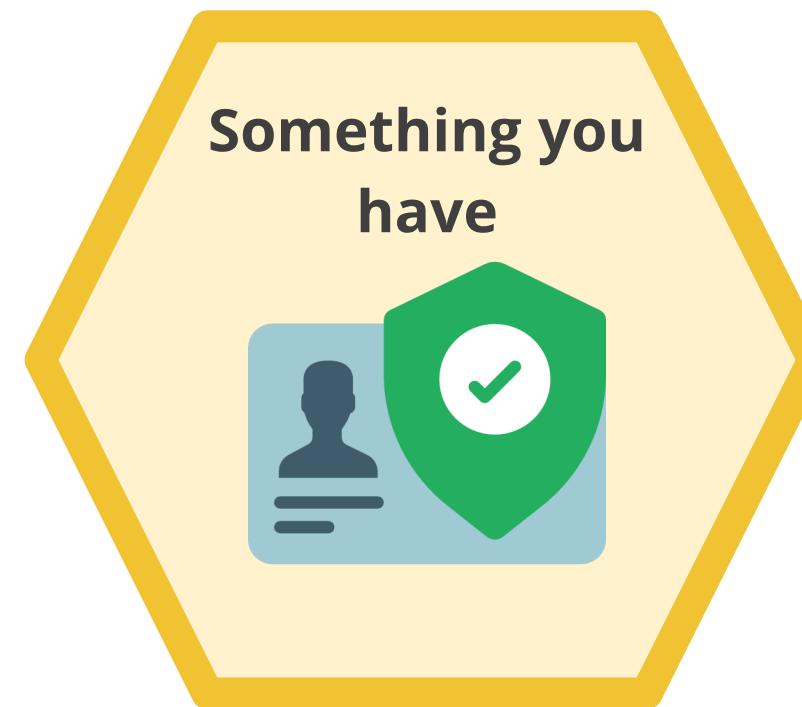
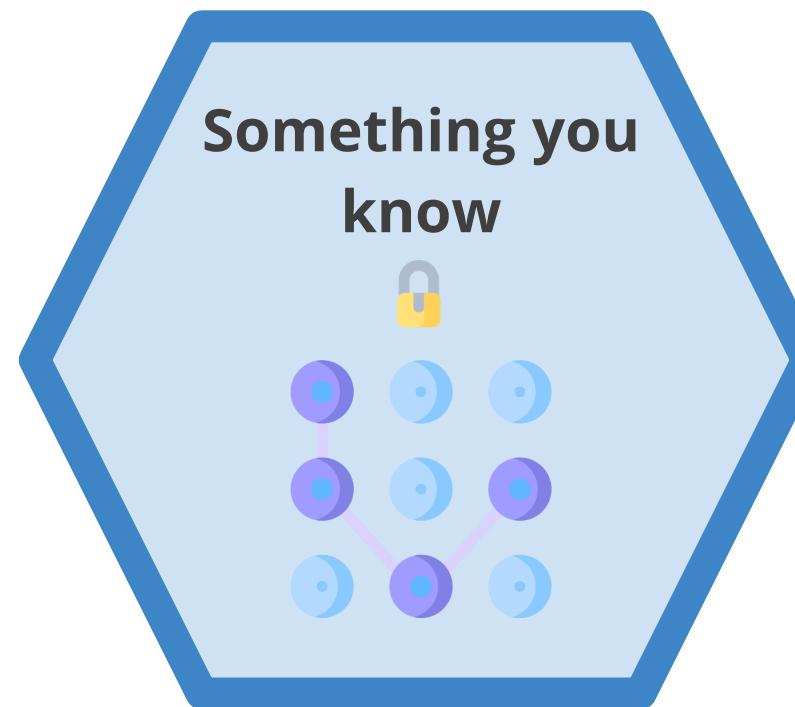


Multi-factor authentication is a type of authentication that requires the use of more than one different authentication factor to be successful.



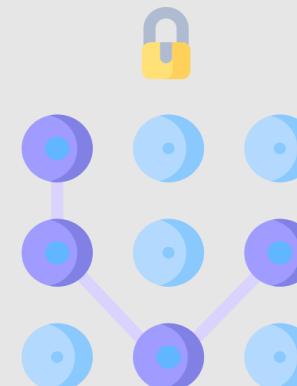
Multi-Factor Authentication (MFA)

Based on the type of authentication, MFA can be categorized into:



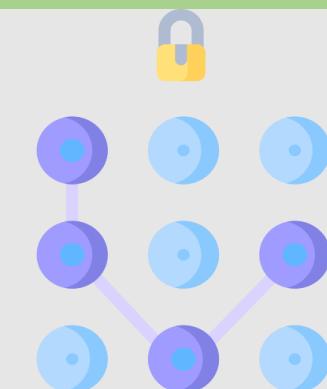
MFA: Types

Two-factor authentication



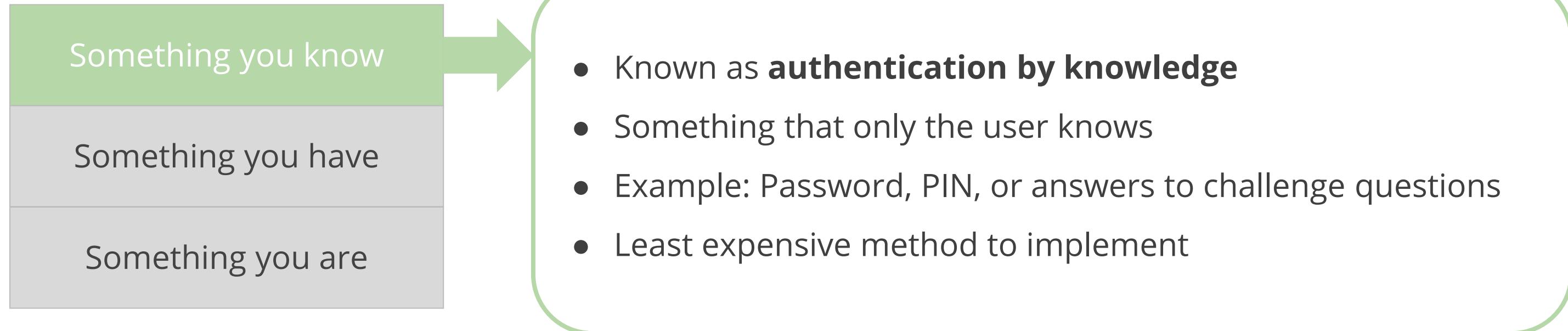
Uses a combination of any two of three authentication factors available

Three-factor authentication

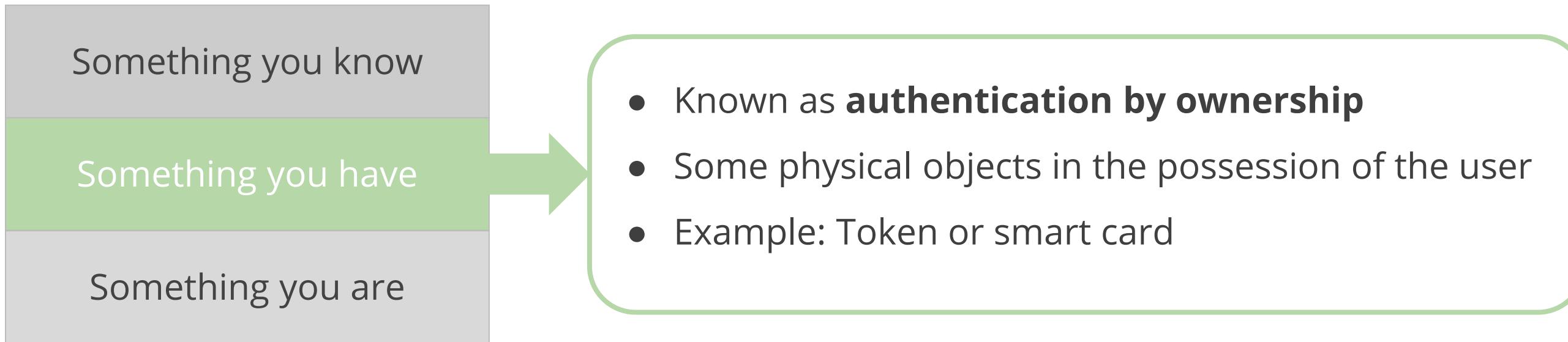


Uses all three authentication factors

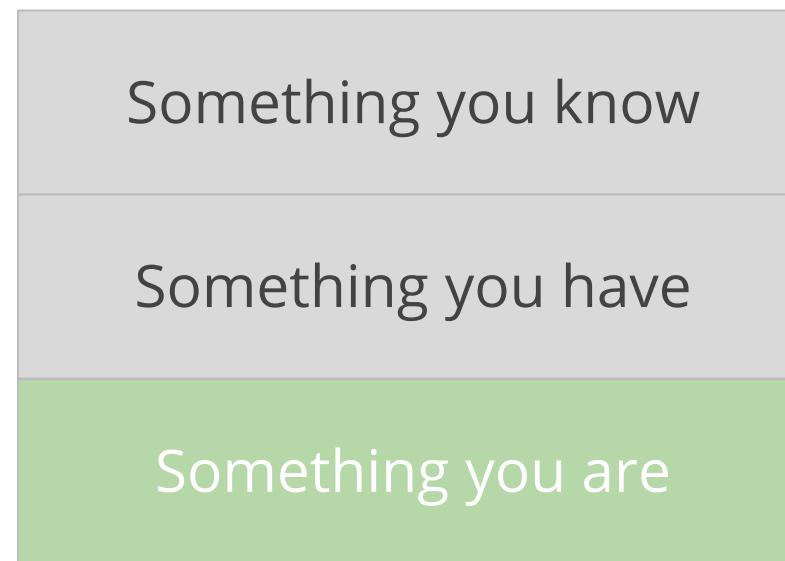
Multi-Factor Authentication (MFA)



Multi-Factor Authentication (MFA)



Multi-Factor Authentication (MFA)

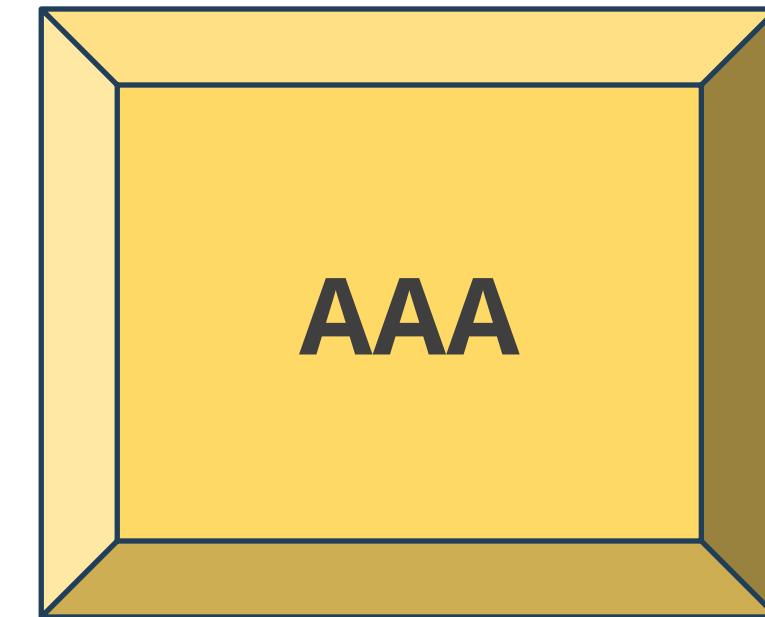


- Known as **authentication by characteristics**
- Some physical characteristics of a user, like biometrics
- Example: Biometrics or a fingerprint
- Most expensive and secure method

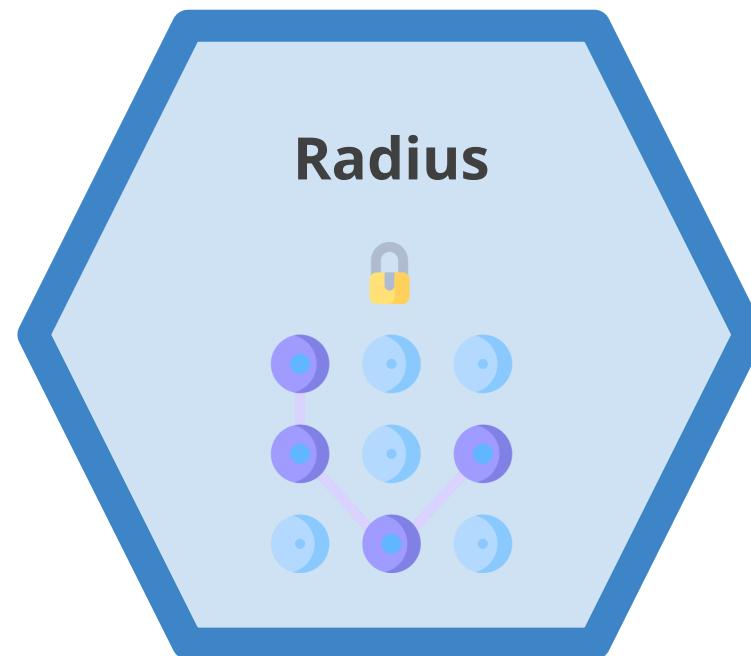
AAA Protocols

The AAA protocol, which stands for authentication, authorization, and accounting, is a framework used to manage access and security in computer networks.

- It essentially regulates who can access network resources (authentication), what they're allowed to do once they're in (authorization), and tracks their activity (accounting).
- AAA protocols are typically implemented on a centralized server, which can manage access control for multiple network devices.
- This simplifies administration and ensures consistent enforcement of security policies.



AAA Protocols

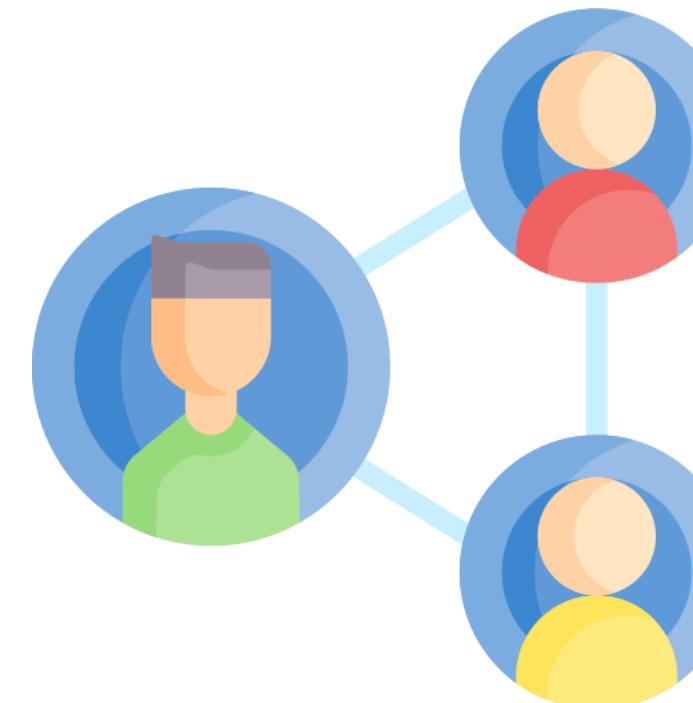


- RADIUS - Remote Authentication Dial-in User Service
- TACACS+ - Terminal Access Controller Access-Control System Plus

Remote Authentication Dial-in User Service (RADIUS)

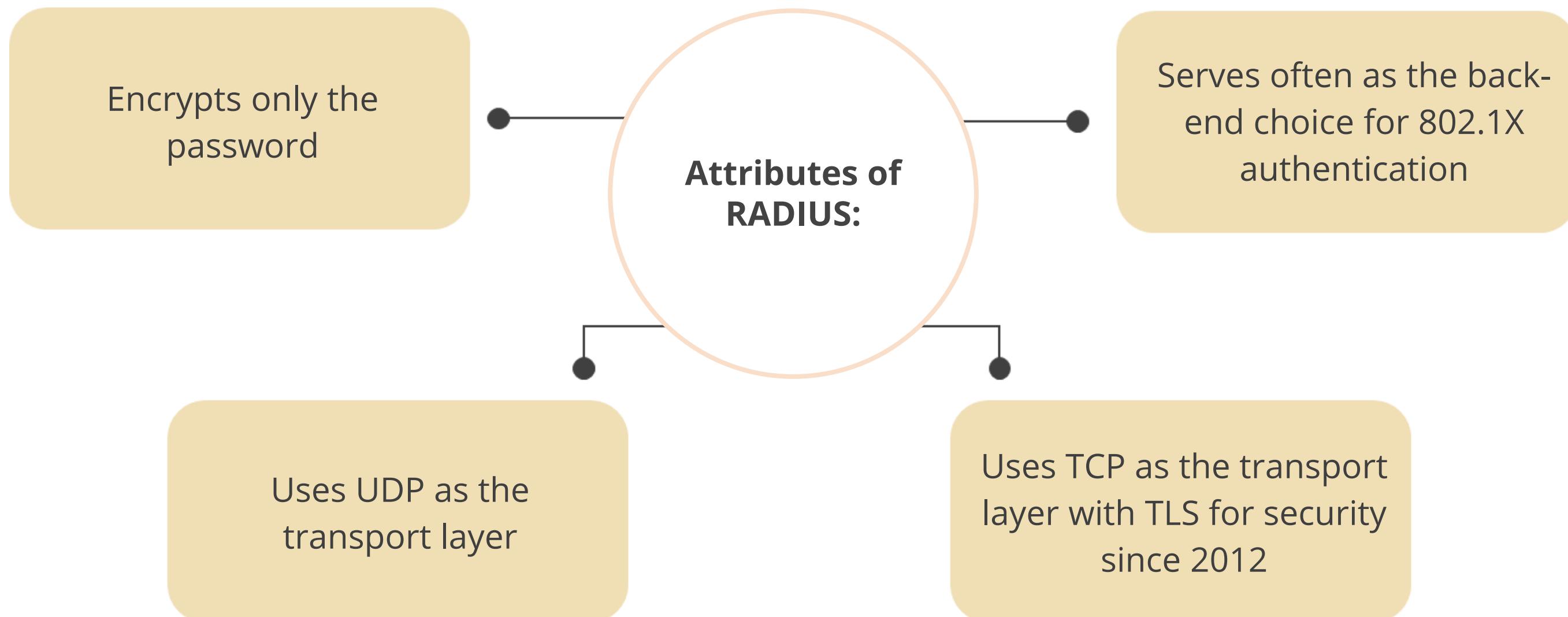


RADIUS is a networking protocol created in 1991 to offer centralized authentication, authorization, and accounting (AAA) management for users that connect to and utilize a network service.

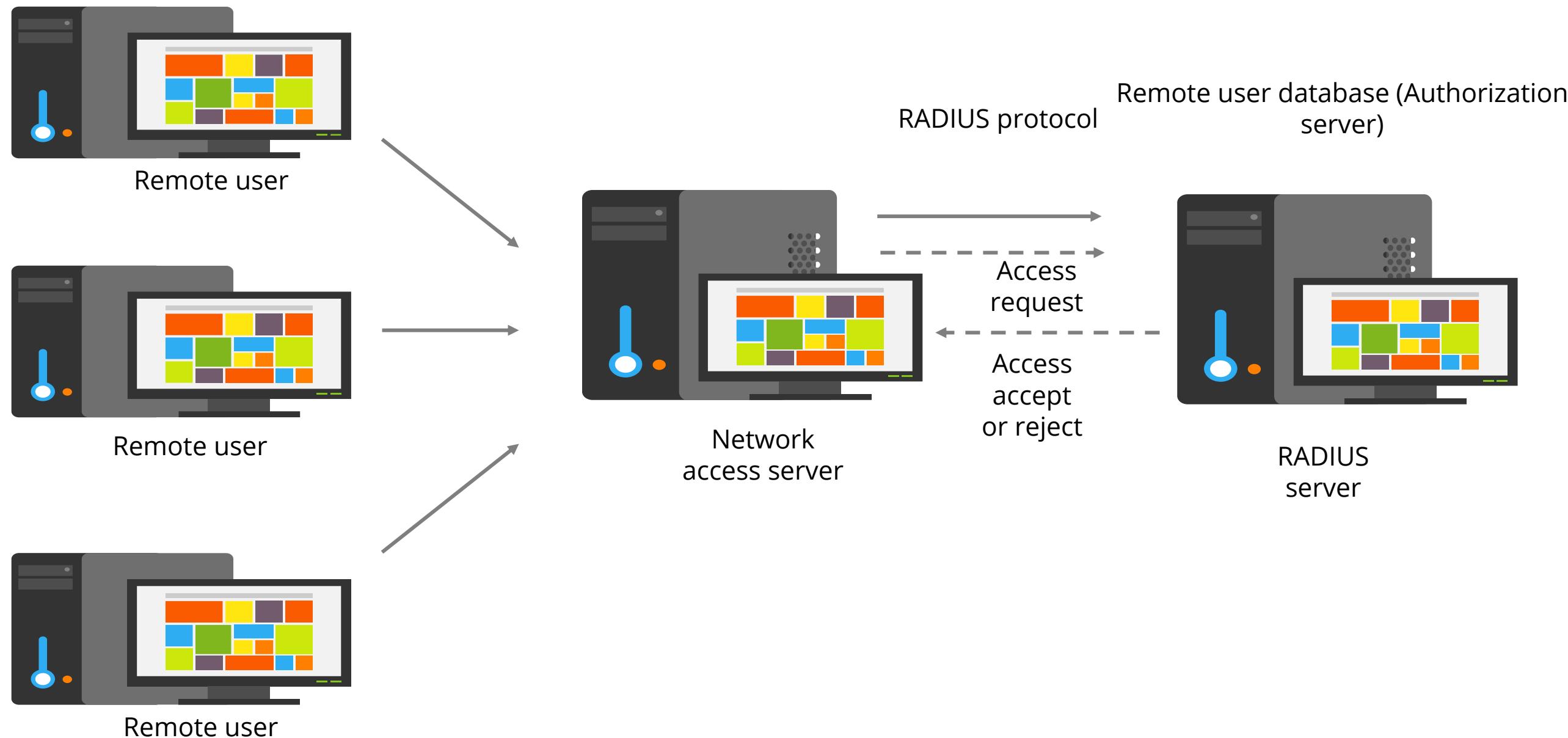


Remote Authentication Dial-in User Service (RADIUS)

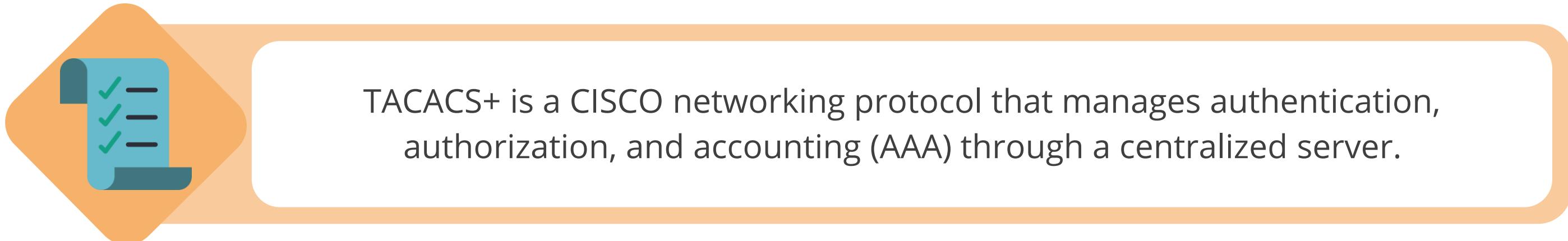
It is a client or server protocol running in the application layer.



Remote Authentication Dial-In User Service (RADIUS)



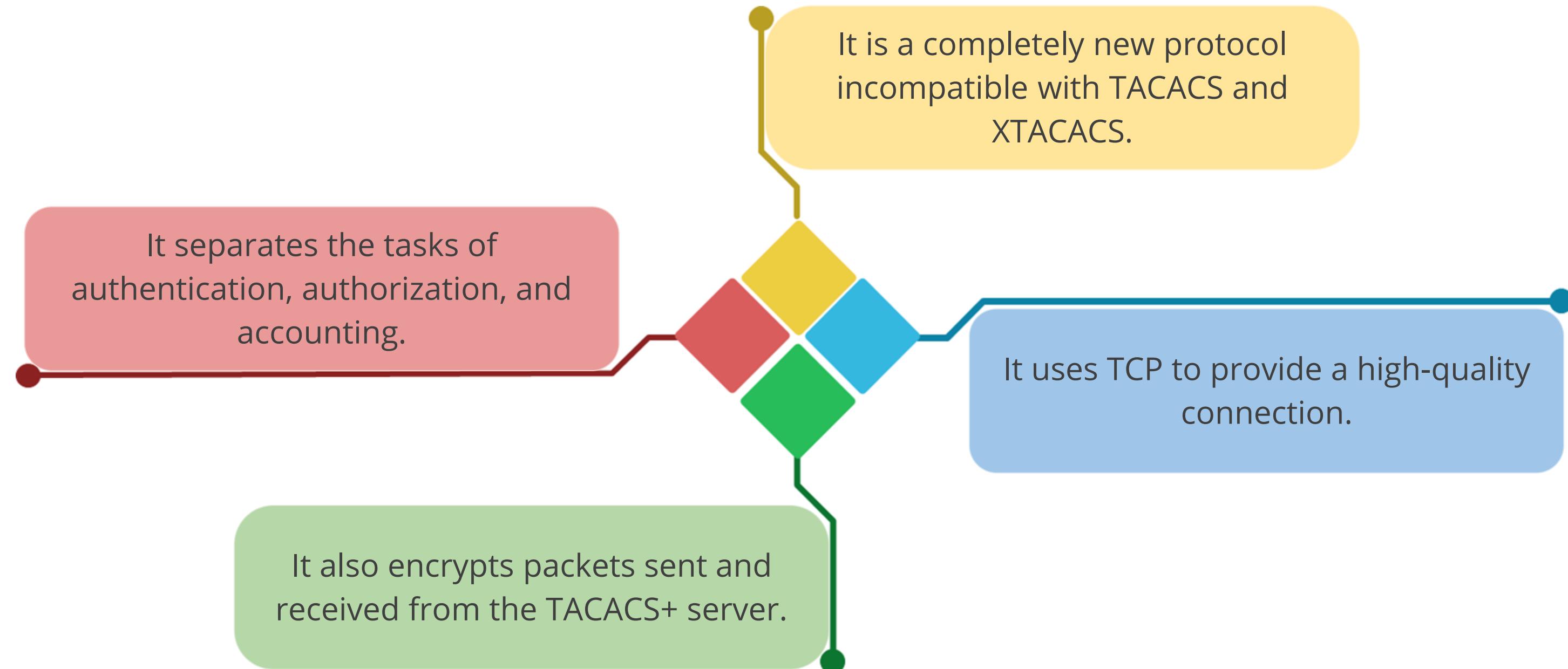
Terminal Access Controller Access-Control System Plus (TACACS+)



TACACS+ is a CISCO networking protocol that manages authentication, authorization, and accounting (AAA) through a centralized server.



Terminal Access Controller Access-Control System Plus (TACACS+)



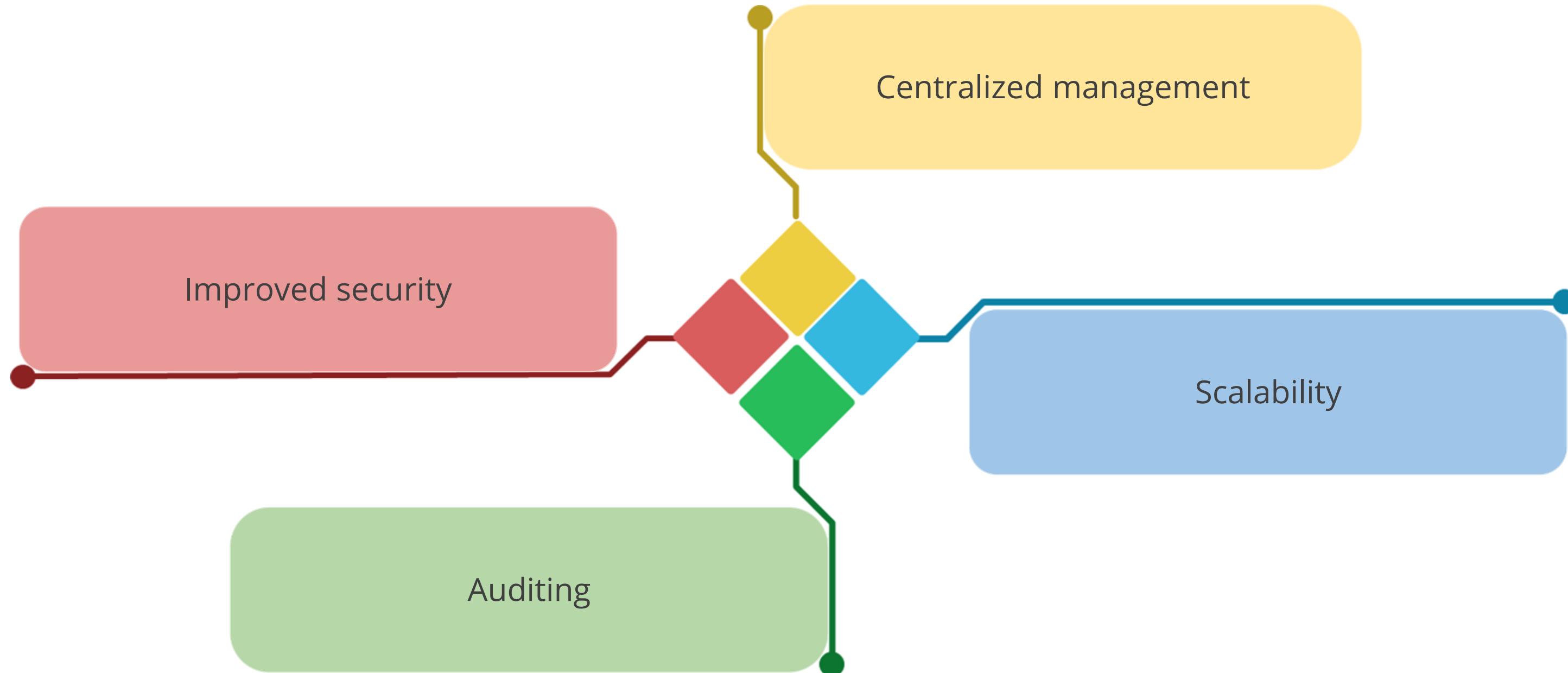
Diameter

It is a protocol that supports all forms of remote connectivity.



- It uses 32 bits for the attribute-value pair (AVP) field.
- It uses TCP port 3868.
- Diameter security uses existing encryption standards, including IPsec or TLS.
- It is a peer-based protocol.
- The server or client initiates communication.
- It has better error detection, correction, and failover functionality than RADIUS.

Benefits of AAA



Decentralized Access Control (DAC)

DAC is a concept in cybersecurity that moves away from centralized control of access permissions

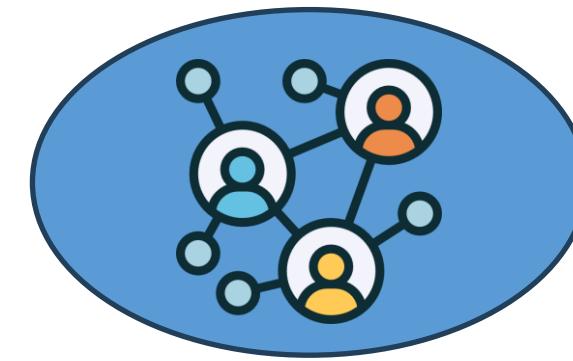


- It provides access control decisions to people closer to the resources.
- Functional manager assigns access control rights to employees.
- Changes can happen faster.
- Conflict of interest possibility can arise.
- It does not provide uniformity and fairness across the organization.
- Certain actions can overlap.

Decentralized Access Control

Site administrators are responsible for managing their sites independently. A sample scenario is as follows:

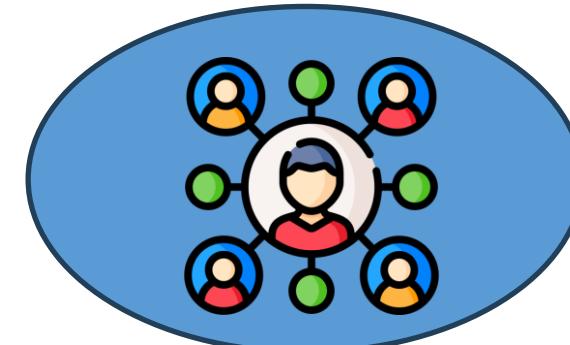
Site D



Site C



Site A



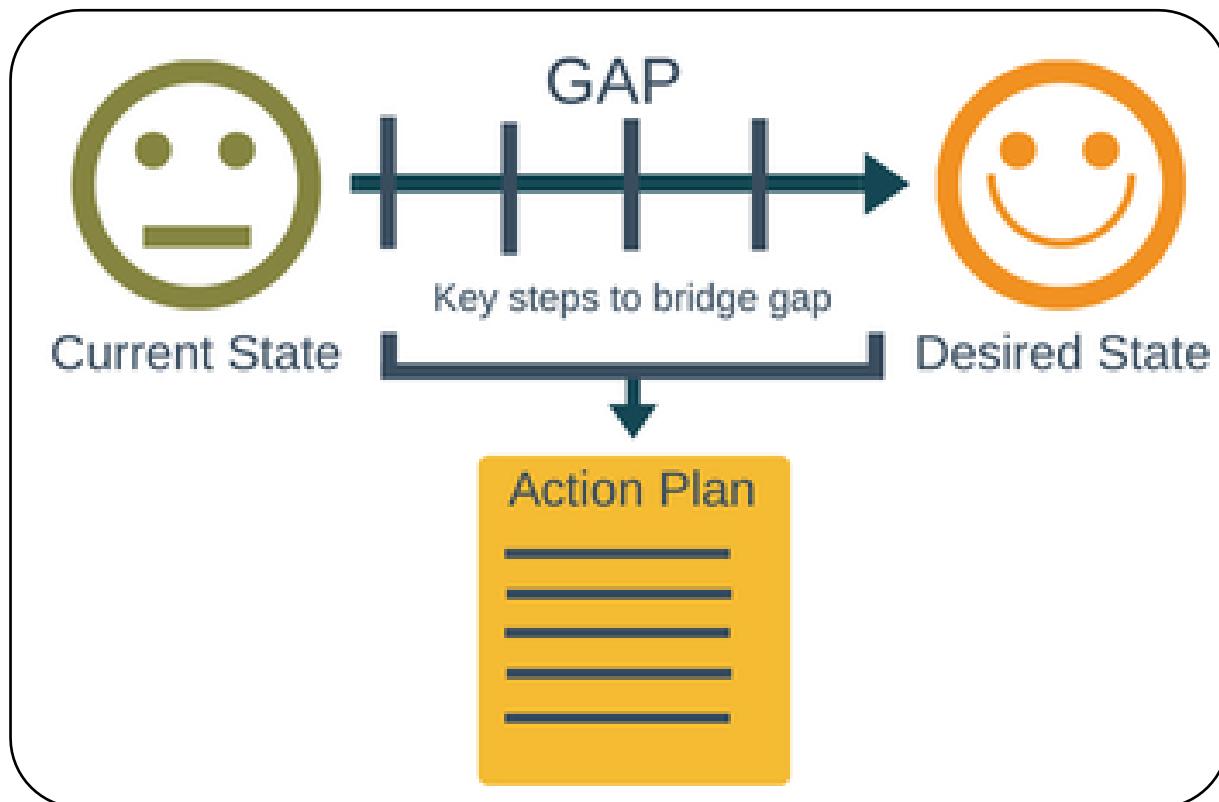
Site B



TECHNOLOGY

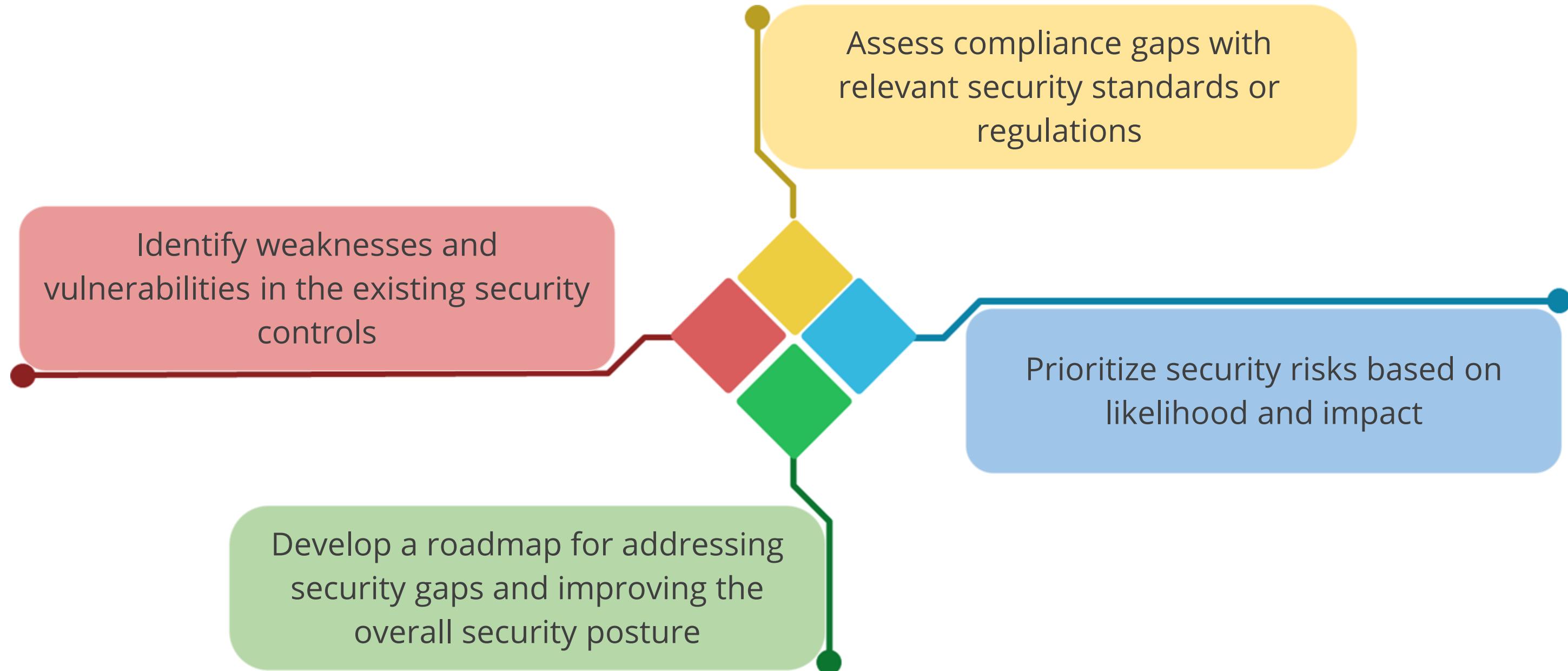
Gap Analysis

Gap Analysis

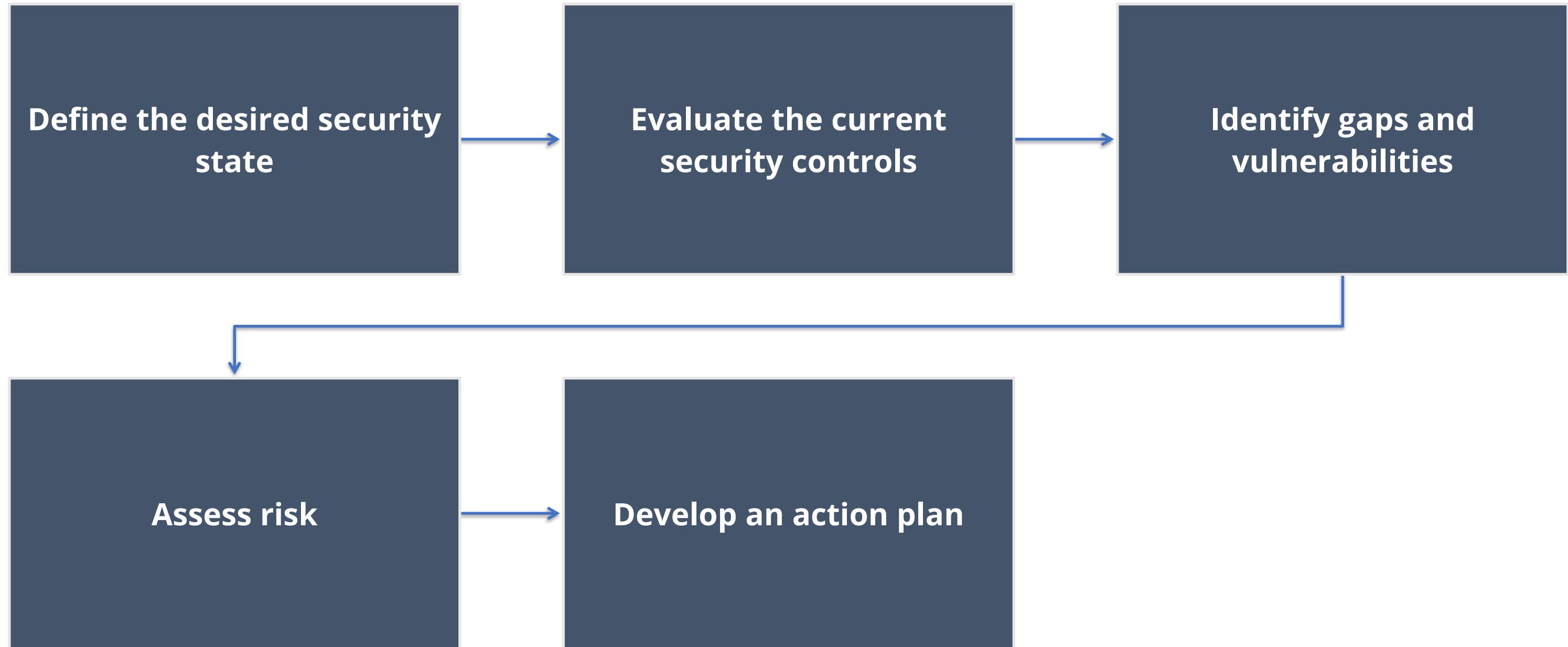


A security gap analysis systematically assesses the differences between an organization's current security posture and its desired state, evaluating practices against standards, regulations, and industry best practices.

Goals of Gap Analysis



Steps in Gap Analysis



Step 1: Define the Desired State

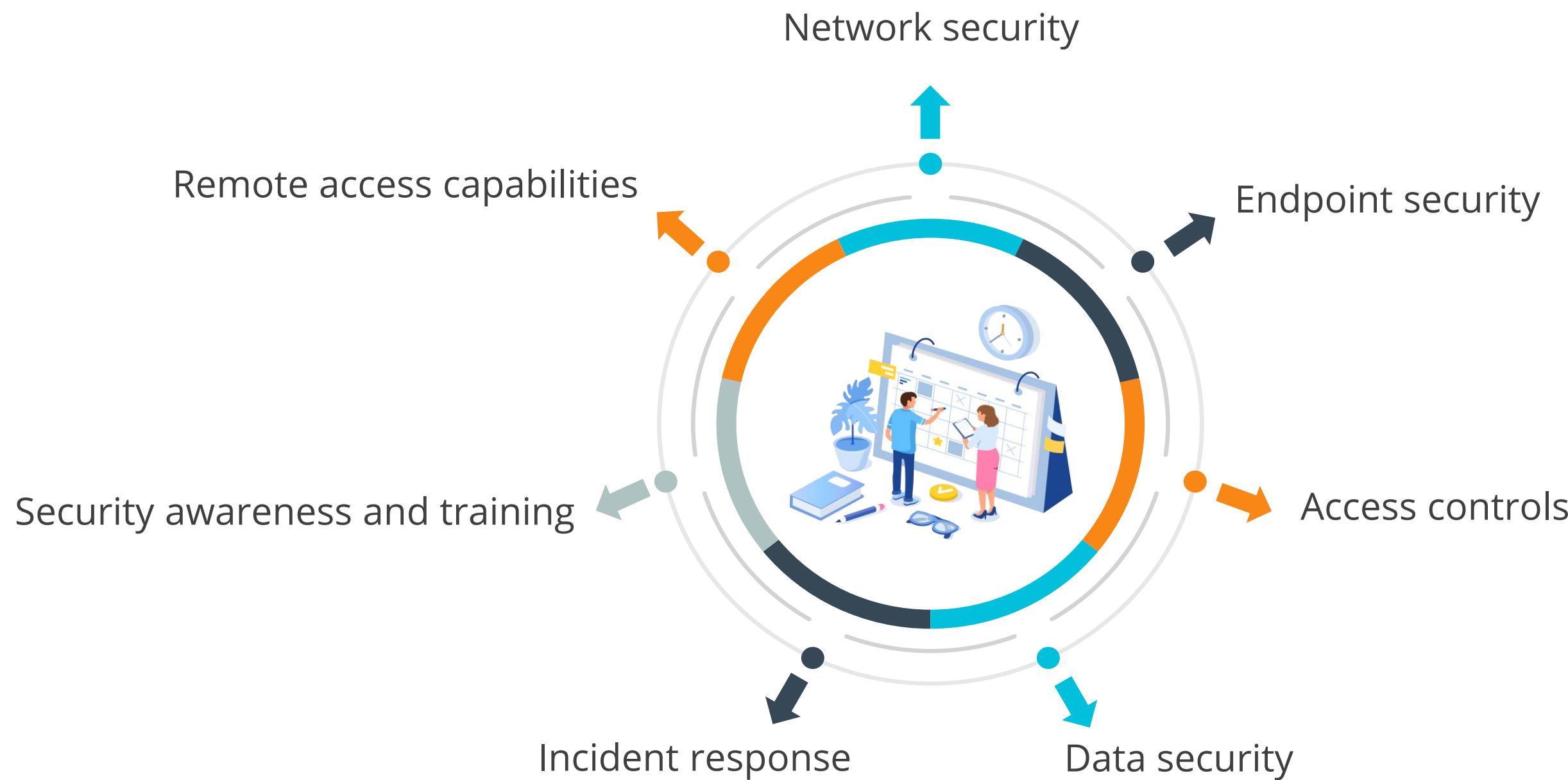
This involves outlining your organization's security goals and objectives.



Consider industry standards, regulations, and best practices that may be relevant.

Step 2: Evaluate the Security Controls

This stage involves taking inventory of the existing security measures across different areas as follows:



Step 3: Identify Gaps and Vulnerabilities

Compare the desired security state with the current controls. This will reveal areas where the defenses are lacking or not aligned with the goals.

The following are some identified gaps:

Weak password policies

Unpatched systems

Lack of multifactor authentication

Unencrypted sensitive data

Step 4: Assess Risk

Analyze the potential impact and likelihood of exploiting identified vulnerabilities. Prioritize the most critical gaps that pose the greatest risk to the organization.



Step 5: Develop an Action Plan

Create a roadmap to address the identified security gaps.



This plan should include:

- Specific actions to be taken
- Resources required
- Timeline for implementation

Benefits of Security Gap Analysis

Improved security posture:
By identifying and addressing gaps, you can significantly strengthen the overall security defenses

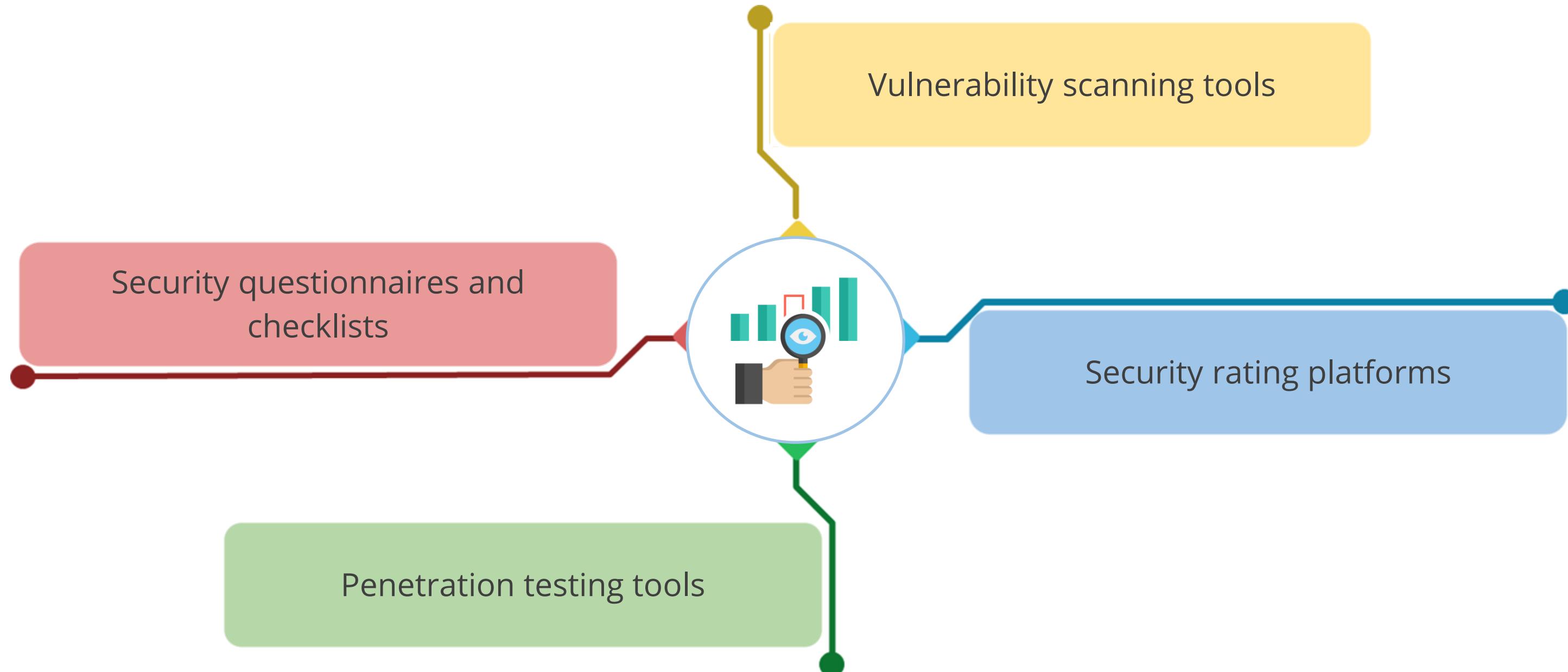
Enhanced risk management:
Prioritizing vulnerabilities allows to focus resources on the areas that matter most

Compliance readiness:
Regular gap analysis ensures you are on track to meet the security requirements of regulations or standards

Better decision-making:
Data-driven insights from the analysis help make informed security investments



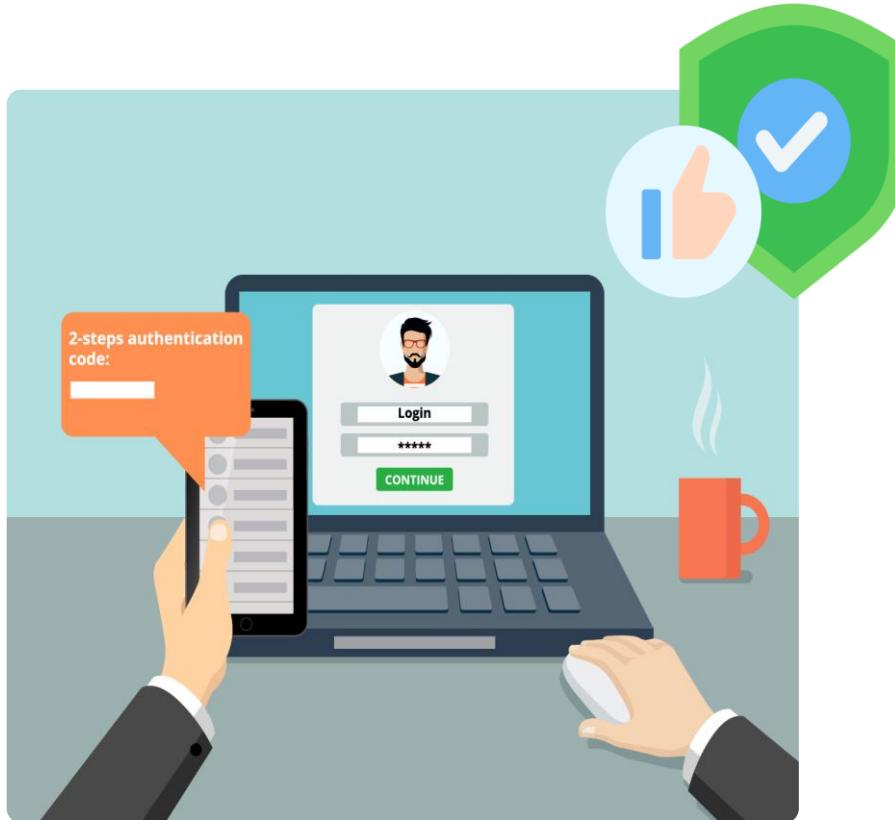
Tools and Techniques for Security Gap Analysis



Zero Trust Architecture and Defense in Depth

Zero Trust Network

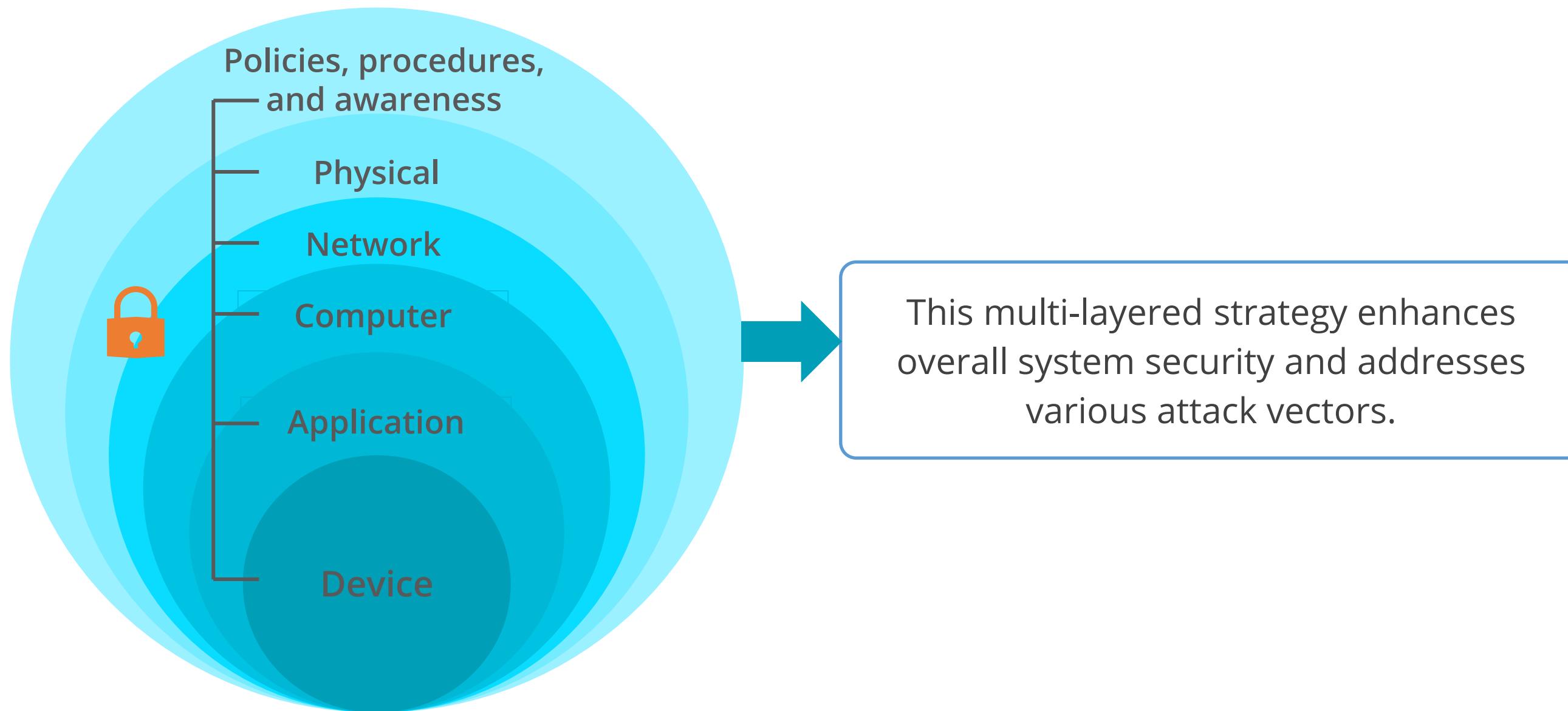
Zero trust network is a security model based on the principle of '**trust nothing and verify everything.**'



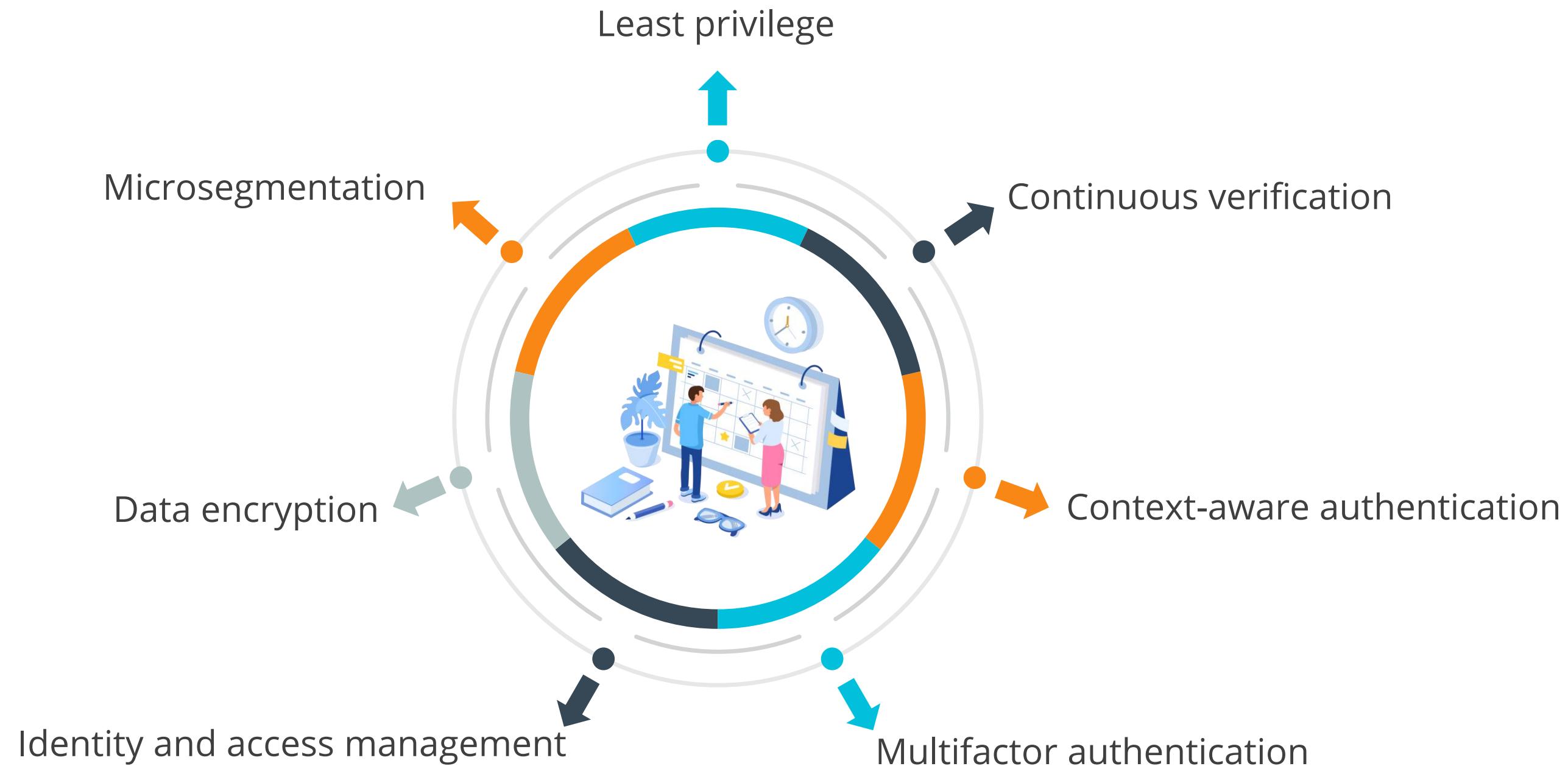
- Devices should not be trusted by default, even if connected to a managed corporate network or were previously verified.
- Every person and device accessing a private network must undergo identity verification, whether inside or outside the network perimeter.

Defense in Depth

Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information.



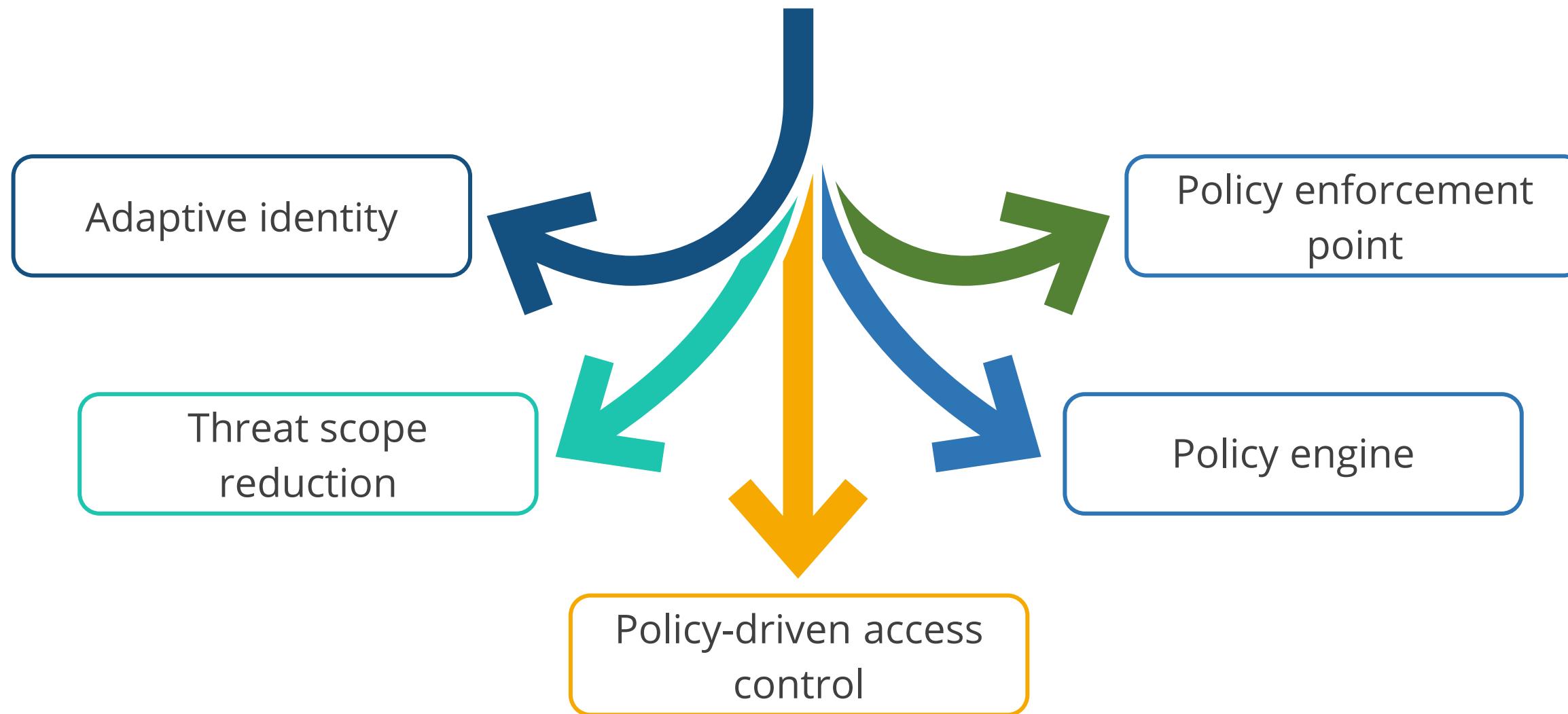
Core Tenets of Zero Trust Architecture



Zero Trust Control Planes

These are parts of the network architecture responsible for routing and traffic control and plays a crucial role in the zero trust model by enabling intelligent decisions.

The following are the components of control planes:



Adaptive Identity

Adaptive identity is a crucial concept, moving beyond static verification and acknowledging that trust is not a one-time occurrence.



- Considers contextual factors like user location, device type, time of access, and behavior patterns
- Continuously monitors user activity and device health for suspicious behavior

Threat Scope Reductions

Zero trust security aims to reduce the impact of security threats by limiting the attack surface and blast radius.



- The scope of potential threats is reduced by limiting the privileges of users, systems, and processes, minimizing points of attack.
- This is achieved through least privilege access, microsegmentation, continuous verification, and deny-all by default.

Policy Driven Access Control

Access to network resources is granted or denied based on predefined policies that consider factors like user role, data type, and device security status.



This is achieved through centralized policy management, implementing the least privilege principle, dynamic access control, integration with adaptive identity, and reducing the attack surface.

Policy Engine

The policy engine determines access to critical network resources on a per-user basis.



- It operates based on policies set by the organization's security team.
- The engine uses context from SIEM data, threat intelligence, user attributes, and device information.
- It communicates decisions to a policy administrator for execution.

Policy Enforcement Point

The Policy Enforcement Point (PEP) is crucial in access control, ensuring security by implementing decisions and rules set by the Policy Engine:



- Acts as the gatekeeper, enforcing access control decisions made by the Policy Engine.
- Functions like a security checkpoint, ensuring only authorized actions get through and preventing breaches.

Zero Trust Data Planes

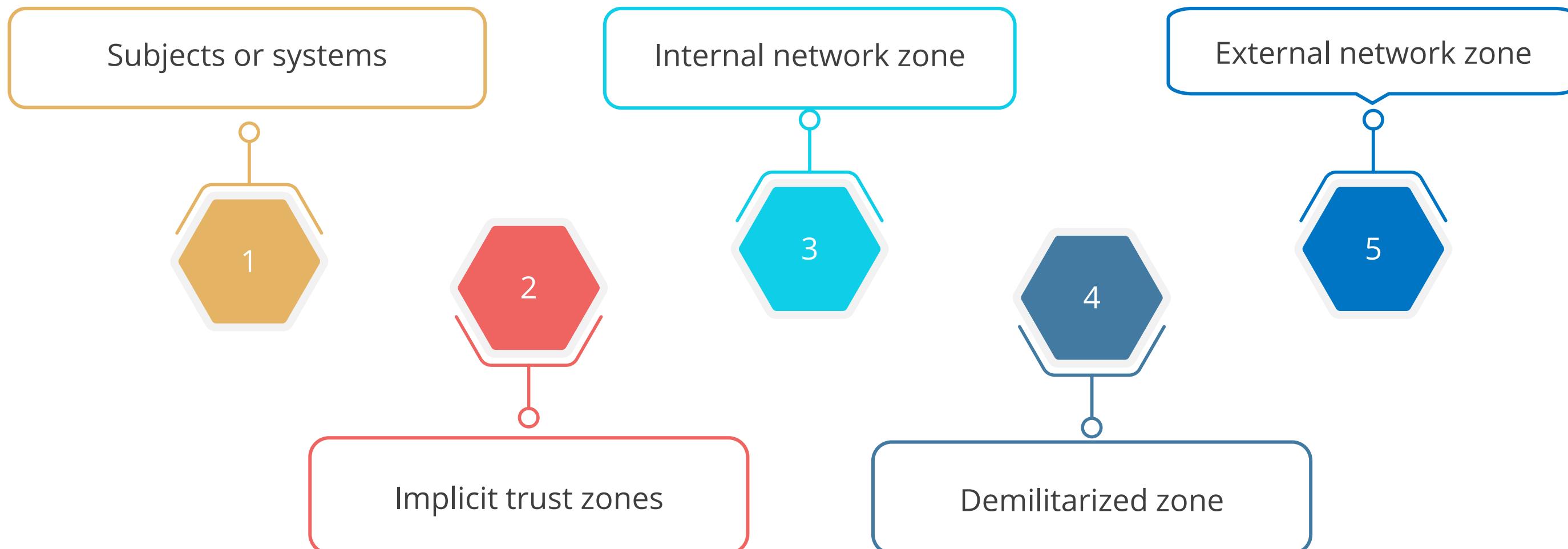
The data plane in cybersecurity is the operational core that moves and forwards data packets within a network, handling routing, switching, and packet forwarding based on predefined rules.



In a Zero Trust framework, the data plane enforces control plane policies, ensuring data packets are routed, inspected, and modified based on security protocols.

Data Planes: Components

The following are the components of data planes:



Subjects or Systems

Subjects

- Entities that initiate data communication
- Can be users, applications, or devices
- Generate data packets that need to be transmitted

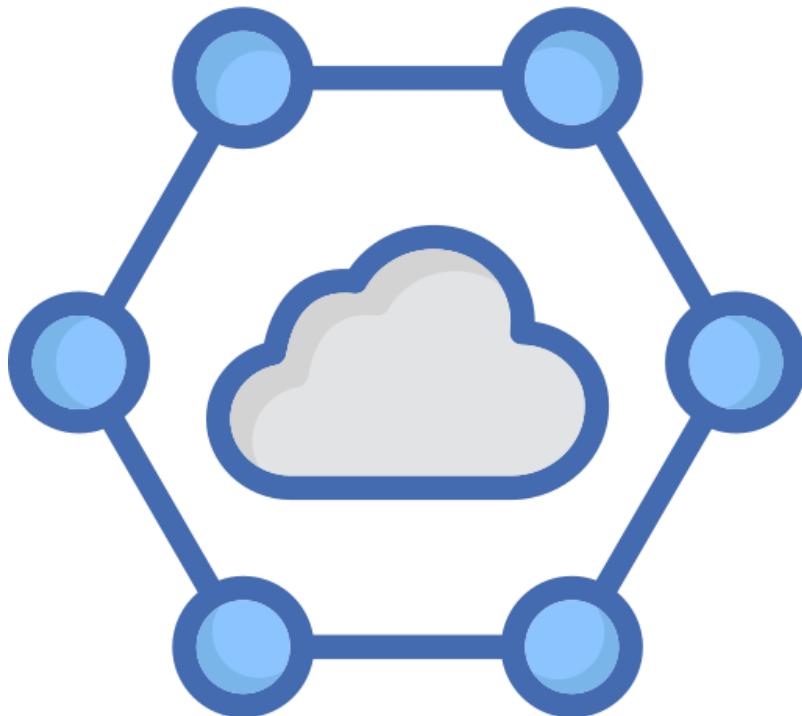
Systems

- Collective infrastructure, resources, and devices responsible for processing and forwarding data packets
- Includes routers, switches, firewalls, load balancers, and other network equipment

Subjects and systems work in tandem to ensure efficient and secure data transmission within the network architecture.

Implicit Trust Zone

An implicit trust zone refers to areas within a network or system where certain levels of trust are assumed without explicit verification.

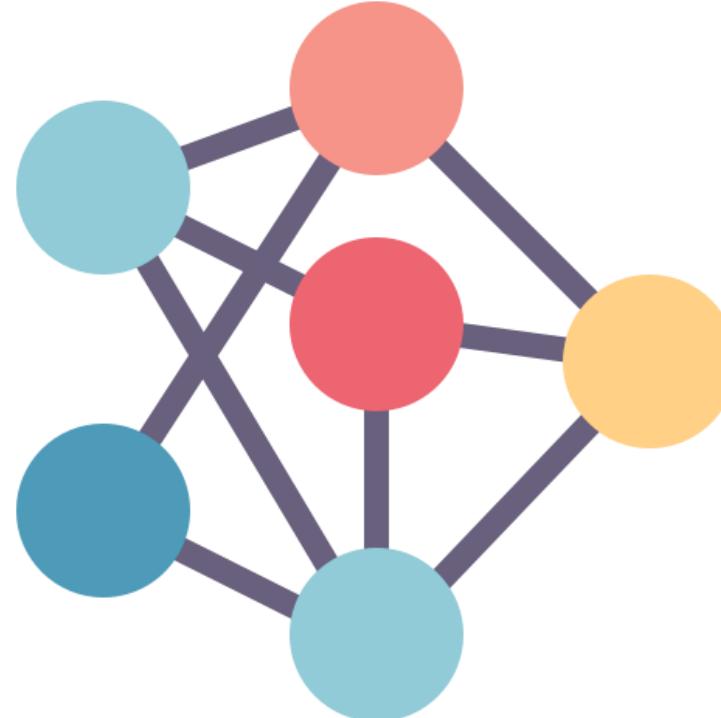


Importance:

- Simplifies communication within the zone
- Reduces the need for constant authentication and verification
- Enhances operational efficiency
- Established through predefined rules and configurations
- Ideal for trusted environments like internal corporate networks or secure cloud segments

Internal Network Zones

An internal network zone refers to a segment within a company's network where devices and resources are considered trustworthy.



Characteristics:

- Protected by the organization's firewall
- Known as the local area network (LAN)
- Typically houses critical infrastructure like domain controllers and database servers

Demilitarized Zones

The DMZ is an area that is neither fully trusted nor entirely untrusted. It's an intermediate zone that allows controlled access to certain services from the external network.



Characteristics:

- Communication between the DMZ and the internal network might be subject to more stringent controls.
- It is also known as a screened subnet, where resources accessed by untrusted and trusted networks reside.

External Zones

External networks, such as the Internet, are typically treated as untrusted zones due to their inherent risks.

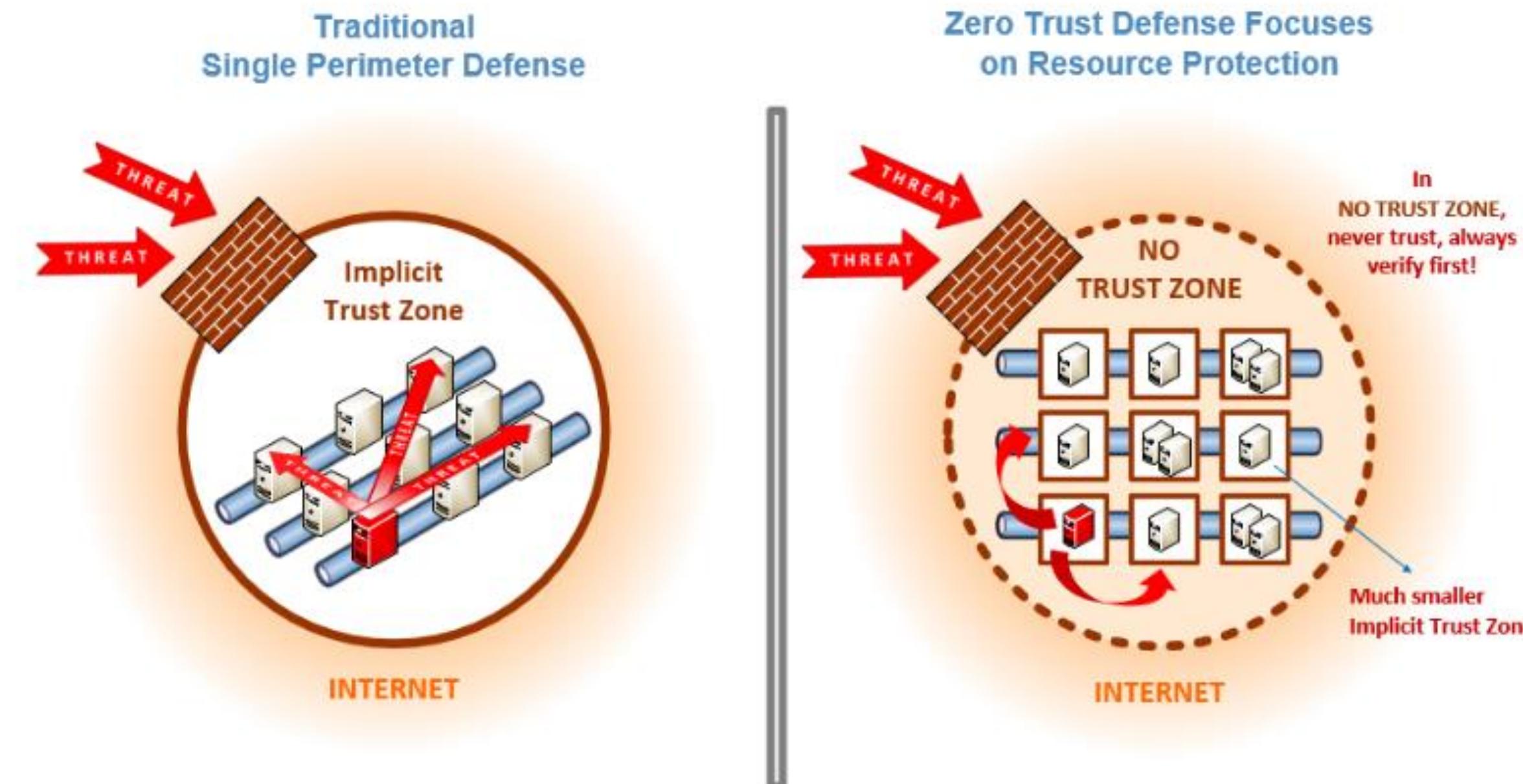


Characteristics:

- Communication from the external network into the internal network usually requires strong security measures.
- Also known as the wide area network (WAN) — an untrusted network.

Zero Trust vs. Defense in Depth

The following are the key distinctions between the traditional Defense in Depth and the modern Zero Trust security models.



TECHNOLOGY

Physical Security

Site and Facility Design Criteria

Physical security is a fundamental component of a security strategy, serving as the foundation for all subsequent safeguards including those related to personnel and information systems.

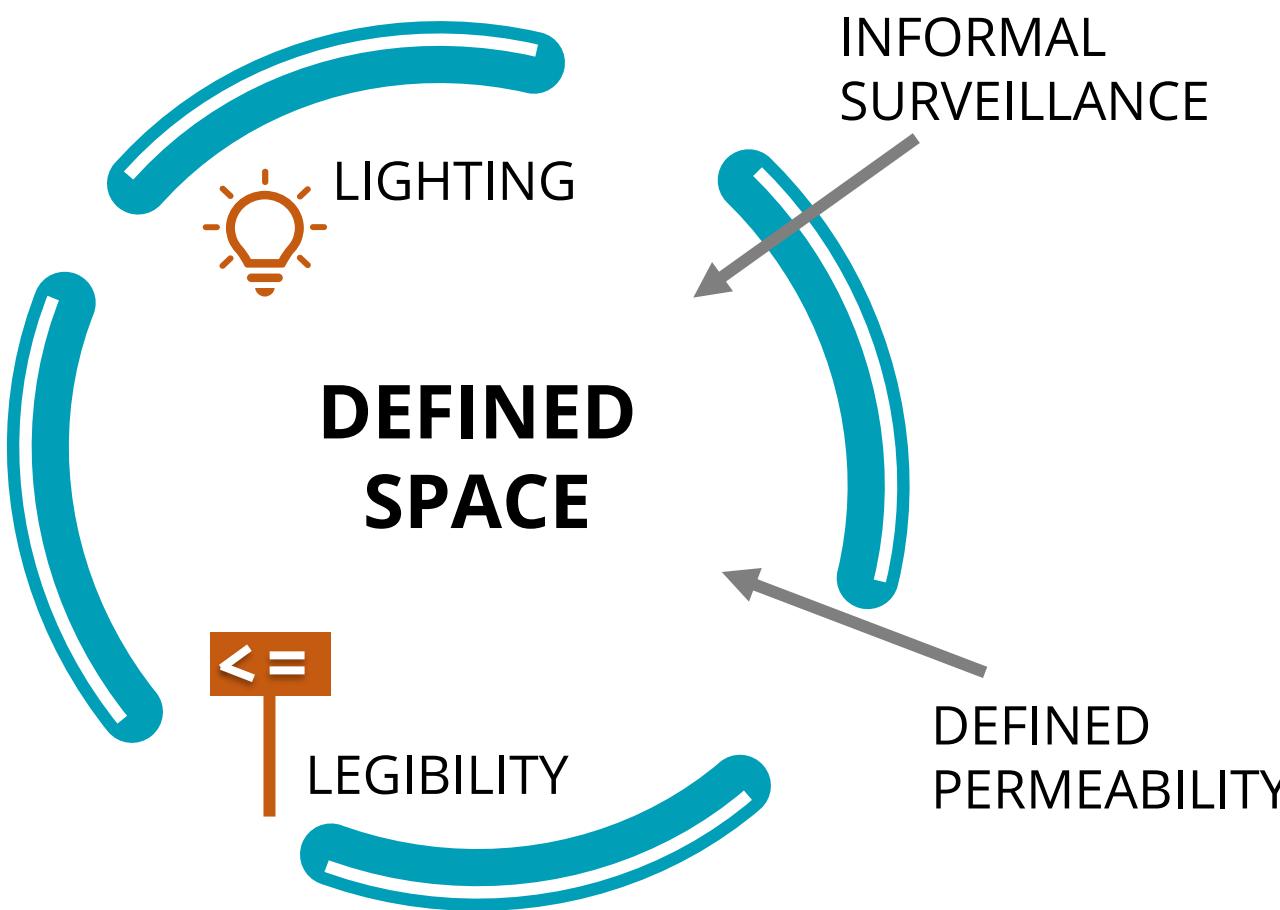


The primary objective of this security framework is to protect life, property, and the continuity of operations.

Security professionals examine all construction aspects and apply a layered security strategy from the site perimeter to individual desktop computers.

Crime Prevention Through Environmental Design (CPTED)

CPTED is a multi-disciplinary approach to deterring criminal behavior through environmental design.
Examples: Streets, parks, museums, government buildings, houses, and commercial complexes



The three environmental strategies of CPTED are:

Territoriality

Surveillance

Access Control

Support Facilities

Ensuring the proper management and maintenance of support facilities is crucial for maintaining system integrity and operational efficiency. Key factors include:

HVAC

Let IT managers know who handles heating, ventilation, and air conditioning

Water

Turn off all power, drain water, place affected equipment in an air-conditioned area, and wipe with water displacement spray

Electricity

Install surge protectors and UPS, use backup sources for critical systems, and install anti-static carpet

Earthquakes

Keep computers away from windows and high surfaces, use shock absorbers and anchors, and ensure no objects fall on them

Lightning

Switch off systems, unplug them, and store backup tapes away from the building's steel supports

Data Center Security: Guidelines

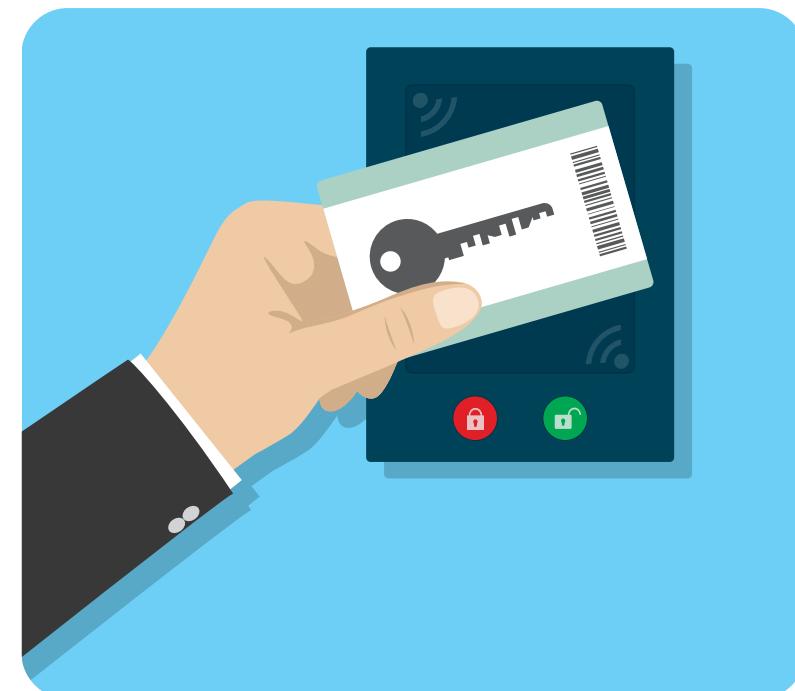
-  Place data centers, server rooms, and wiring closets at the facility's core
-  Position wiring closets directly above or below each other in multistory buildings
-  Ensure access to data centers is through a single door; use additional doors as one-way exits
-  Avoid placing data centers in basements or upper floors
-  Construct the data processing center as a single room, not multiple rooms
-  Maintain positive air pressure in data centers to prevent contaminants; install water detectors under raised floors and on dropped ceilings
-  Implement HVAC systems for temperature and humidity control

Personnel Access Control

Effective personnel access control is essential for organizational security. The differences between piggybacking and tailgating are:

Piggybacking

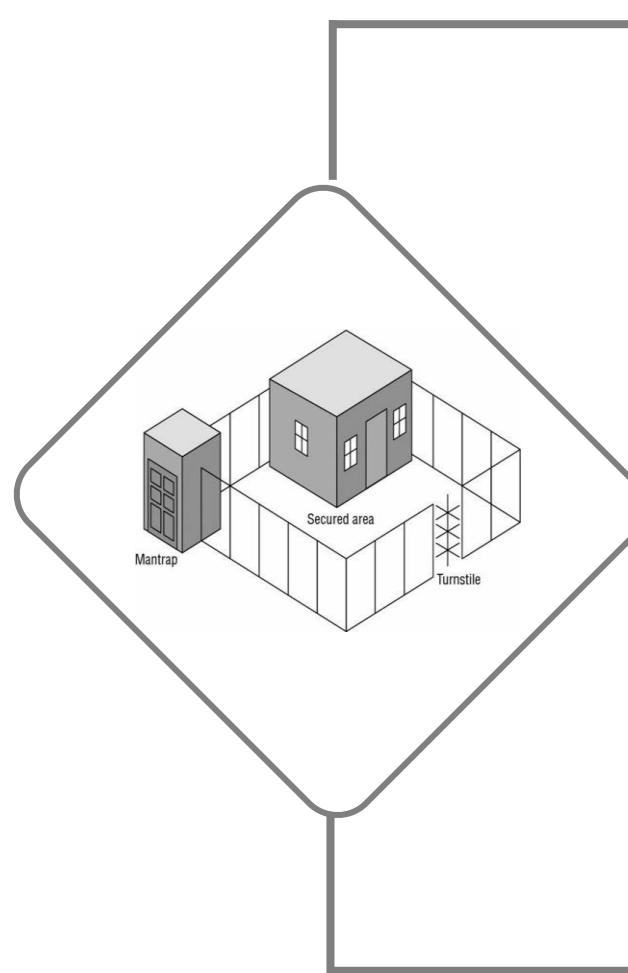
Piggybacking is when another person follows through a door with the permission of the person who has received access.



Tailgating

Tailgating is when another person, whether an employee or not, passes through a secure door without the knowledge of the person who has gained legitimate access through the secure door.

Mantraps and Turnstiles



Mantraps

It is a double set of doors often protected by a guard or some other physical layout that prevents piggybacking and can trap individuals at the discretion of security personnel.

Turnstiles

It is a form of gate that prevents more than one person at a time from gaining entry and often restricts movement in one direction, serving as the equivalent of a secured revolving door.

Access Control

Smart card

- Security ID with an embedded magnetic strip, bar code, or integrated circuit chip
- Can process information or store a reasonable amount of data in memory
- Can be used in multifactor authentication to improve security
- Vulnerable to physical security attacks

Memory card

- Machine-readable ID cards with memory sticks
- Can hold a small amount of data in memory but cannot process it
- Are easy to copy or duplicate

Proximity reader

- A passive device or transponder that can be used to control physical access
- A passive device, typically worn by an individual, that alters the magnetic field generated by the reader when detected and processed

Fire Prevention, Detection, and Suppression



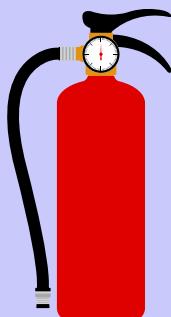
Fire Prevention

- Training employees for fire safety
- Supplying the right equipment and ensuring their working conditions
- Storing combustible materials properly



Fire Detection

- Placing fire detectors at strategic points to detect smoke or fire

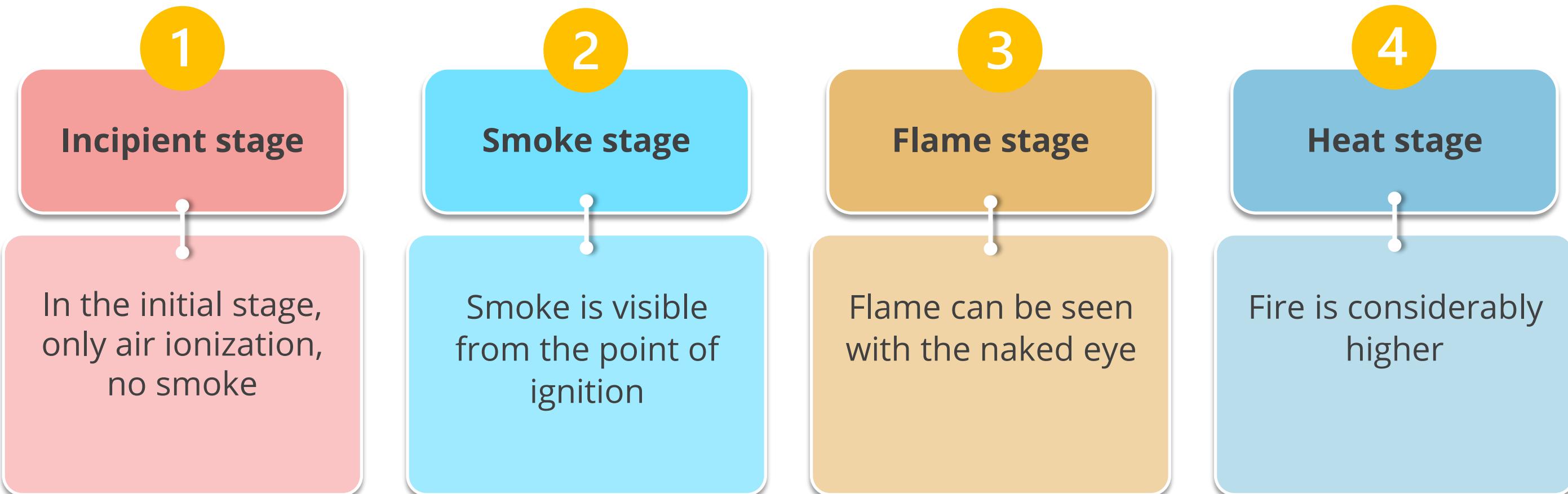


Fire Suppression Systems

- Using a suppression agent to put out a fire

Stages of Fire

The different stages of fire progression are:



The earlier the fire is detected, the easier it is to be extinguished.

Fire Detection Devices



Smoke-Activated

- Good early warning devices
- Photoelectric device
 - Detects a variation in light intensity and produces a beam of light, and if the light is obstructed, an alarm is produced

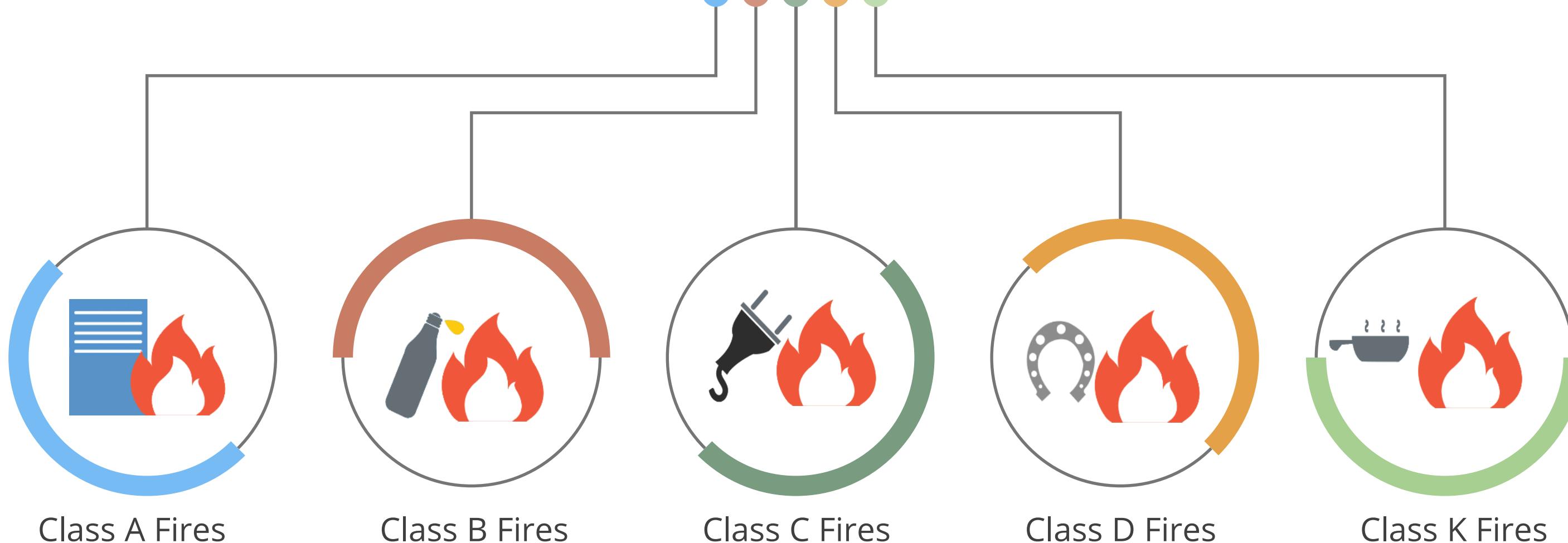


Heat-Activated

- **Fixed temperate:** Alarm is generated when a particular temperature is reached
- **Rate-of-raise:** Alarm is generated when the temperature rises over time

Environmental Controls: Fire

The following are the classes of fires:



Environmental Controls: Fire

The table given below indicates the types of fires and the corresponding extinguishing methods.

Class	Description (Fuel)	Extinguishing Method
A	Common combustibles, such as paper, wood, and clothing	Water, Foam
B	Burnable fuels, such as gasoline or oil	Inert Gas, CO2
C	Electrical fires, such as computers and electronics	Inert Gas, CO2 (Note: Most important step - Turn off the electricity first)
D	Special fires, such as chemical or metal	Dry Powder (May require total immersion or other special techniques)
K	Commercial kitchens	Wet chemical

Water-Based Suppression System

Wet Pipe

- Always full of water, usually discharged by temperature control sensors
- Also called closed-head systems

Dry Pipe

- Water is not stored in the pipe, instead, it contains compressed air
- Opening the water valve causes water to fill the pipes and discharge

Preaction

- Combination of wet and dry pipe
- Water is not held in the pipes until the fire is detected
- Released only after the sprinkler head activation triggers are melted by sufficient heat

Deluge

- Another form of dry pipe system that uses larger pipes and can deliver a significantly larger volume of water

Gas Suppression

Gas suppression is more efficient than water suppression as it quickly reduces oxygen levels, effectively extinguishing fires without collateral damage to sensitive equipment.

Usage safety

These systems remove oxygen and should not be used in occupied areas to ensure safety.

Environmental concerns

Halon is banned due to its severe environmental impact.

Eco-friendly alternatives

FM200, NAF-S-III, Argon, Inergen

Motion Detectors

Infrared

Monitors significant changes in infrared lighting patterns within a monitored area

Heat-based

Monitors significant changes in heat levels within a monitored area

Wave pattern

Emits and detects changes in ultrasonic waves within a monitored area

Capacitance

Monitors changes in the electrical or magnetic fields surrounding a monitored object

Photoelectric

Monitors changes in visible light levels within a monitored area

Passive audio

Listens for abnormal sounds within a monitored area

Alarm Types



Deterrent

- Alarms that trigger deterrent actions
- The goal is to make intrusion attempts more difficult.



Repellent

- Alarms that trigger sound or light
- The goal is to discourage intruders.



Notification

- Alarms that trigger notifications to security analyst
- Silent from an attacker's perspective, but it gives warning signals to the security team.

Emanation Security: Protecting Against Electronic Emanations

Hardware and electronic devices can emit unintentional electronic signals that, if intercepted, may disclose sensitive information.



TEMPEST is a set of standards that protects against electronic eavesdropping by securing electromagnetic emissions.

Emanation Security: Protecting Against Electronic Emanations

Various methods are deployed to mitigate risks associated with electronic emanations each tailored to specific security needs:

Faraday cage

Encloses a metal mesh that absorbs EM signals surrounding the area

White noise

Masks and conceals real emanations by broadcasting simulated traffic

Control zone

Defines areas to manage emanations, utilizing tools like Faraday cages or white noise

HVAC

Effective Heating, Ventilation, and Air Conditioning (HVAC) management maintains ideal temperature and humidity in data centers, enhancing the reliability and efficiency of electronic equipment.

HVAC standards for data center stability and efficiency

- Temperature is maintained between 68 to 77°F (20-25°C) for ideal operational conditions.
- Humidity levels are kept between 40% and 55% to prevent static electricity buildup and corrosion.
- Positive pressure and proper drainage systems are employed to stabilize environmental conditions.

By carefully controlling temperature and humidity, HVAC systems protect sensitive electronic equipment and enhance overall efficiency.

Power Supply

A reliable power supply is critical for any data center. The following are common threats to the power system:

Power excess

- **Surge:** Prolonged high voltage
- **Spike:** Momentary high voltage

Power loss

- **Blackout:** Prolonged, complete loss of electric power
- **Fault:** Momentary power outage

Power degradation

- **Brownout:** Prolonged reduction in voltage
- **Sag or dip:** Momentary reduction in voltage

Security Training and Awareness

Physical security awareness and training are very critical. It should include:

- Training on operating emergency power systems
- Training on operating fire extinguishers
- Evacuation routes should be prominently displayed
- Fire drills

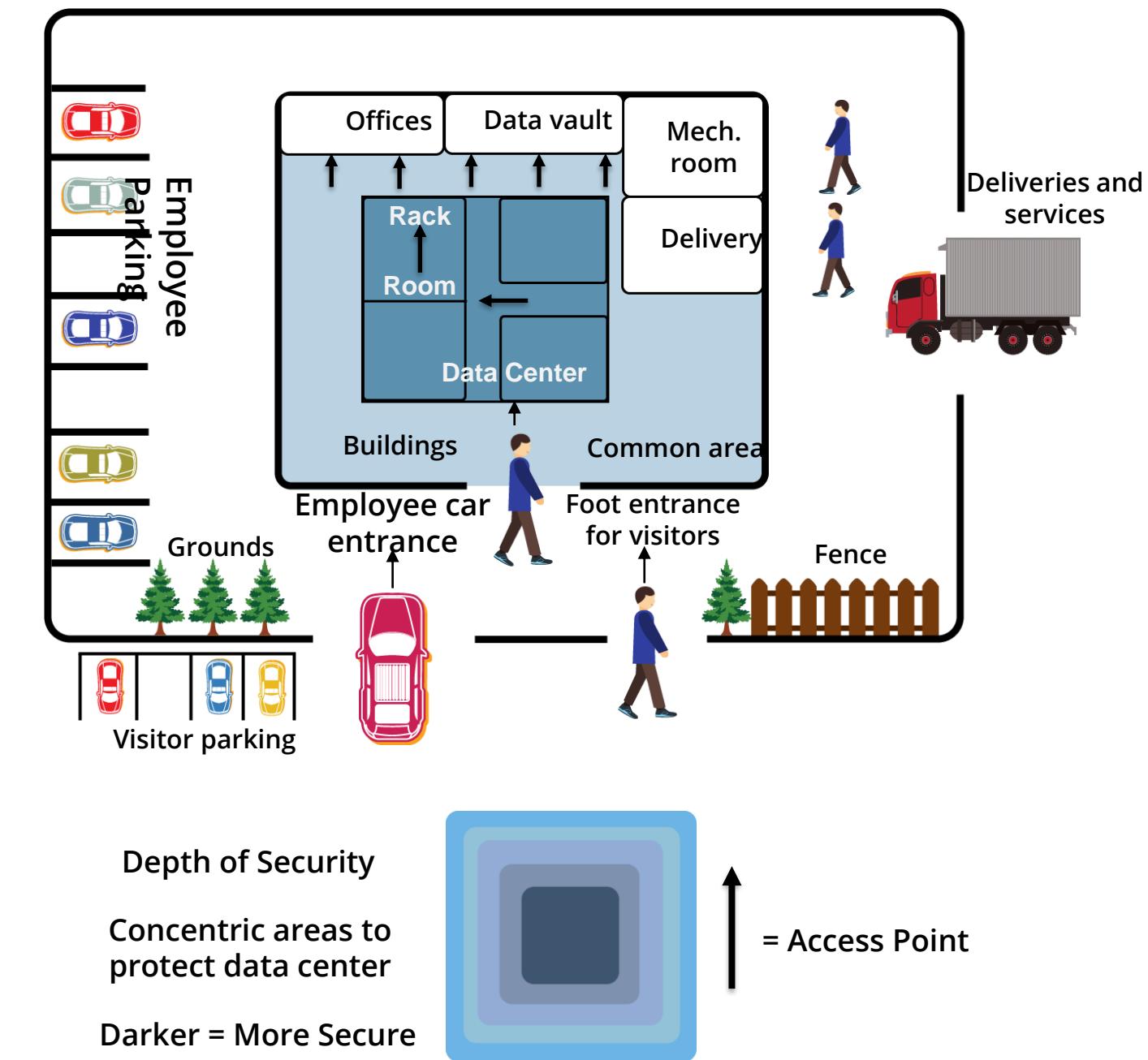


Perimeter Security Controls

Perimeter defenses are critical for preventing, detecting, and correcting unauthorized access into the facility.

Key features

- Employs the defense-in-depth concept for enhanced security
- Features layered architectural barriers where the core area is most protected
- Designs security systems with multiple barriers known as rings of protection
- Reduces the likelihood of successful attacks through layered design

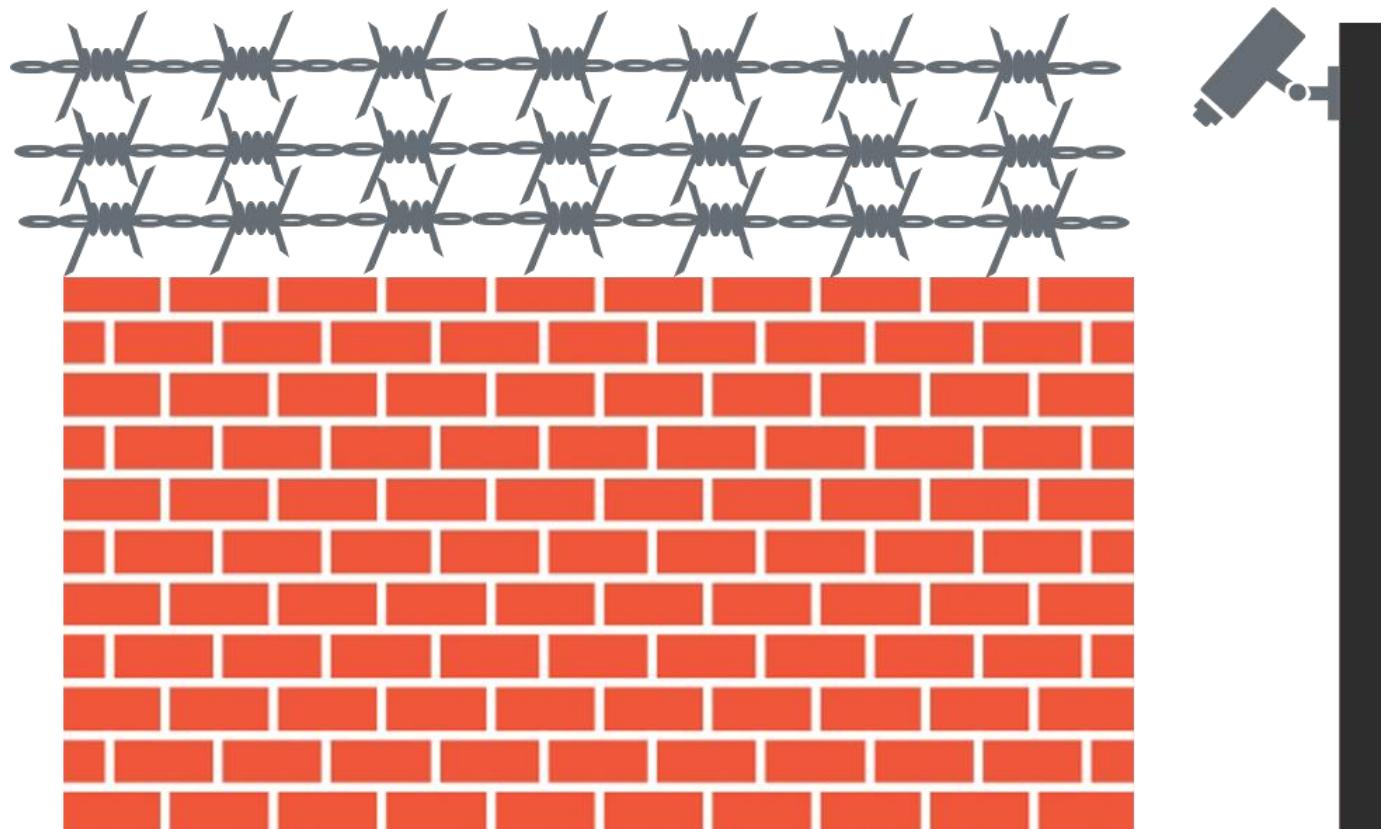


Barriers

Barriers strategically define and outline how an area should be architecturally designed and to obstruct or deny unauthorized access effectively.

Objectives of barriers include:

- Keep intruders out
- Cause delays in intrusion
- Control access points
- Enable surveillance
- Provide safe evacuation routes



Fences

Fences serve as crucial perimeter identifiers meticulously designed and strategically installed to effectively deter and prevent unauthorized access by keeping intruders out.

The various types of fences include:

- Chain link
- Barbed wire
- Barbed tape
- Concertina wire

Height	Effectiveness
3-4 ft	Deters casual trespassers
6-8 ft	Too difficult to climb easily
8 ft plus 3 strands of barbed or razor wire	Deters determined trespassers

Selecting the appropriate fence type and height is essential for maximizing perimeter security and effectively managing the specific risks associated with unauthorized entry.

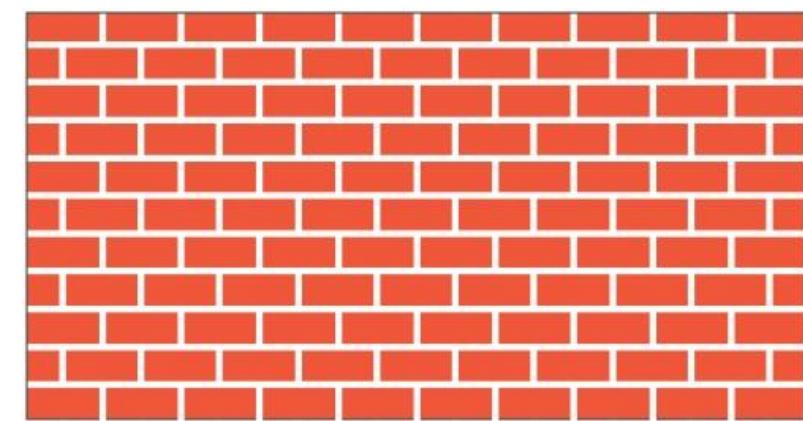
Walls and Bollards

Walls and bollards serve as crucial man-made barriers designed to enhance physical security by obstructing unauthorized access.

Walls

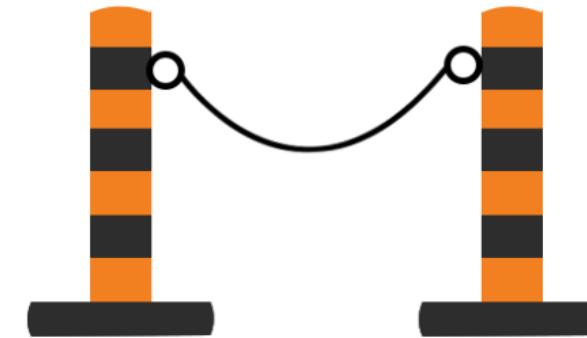
Walls are more permanent and sturdy barriers, generally resulting in higher installation costs.

Common materials include cinder blocks, masonry, brick, and stone.



Bollards

Bollards are robust concrete pillars used to restrict vehicle access while permitting pedestrian movement, often employed to control traffic.

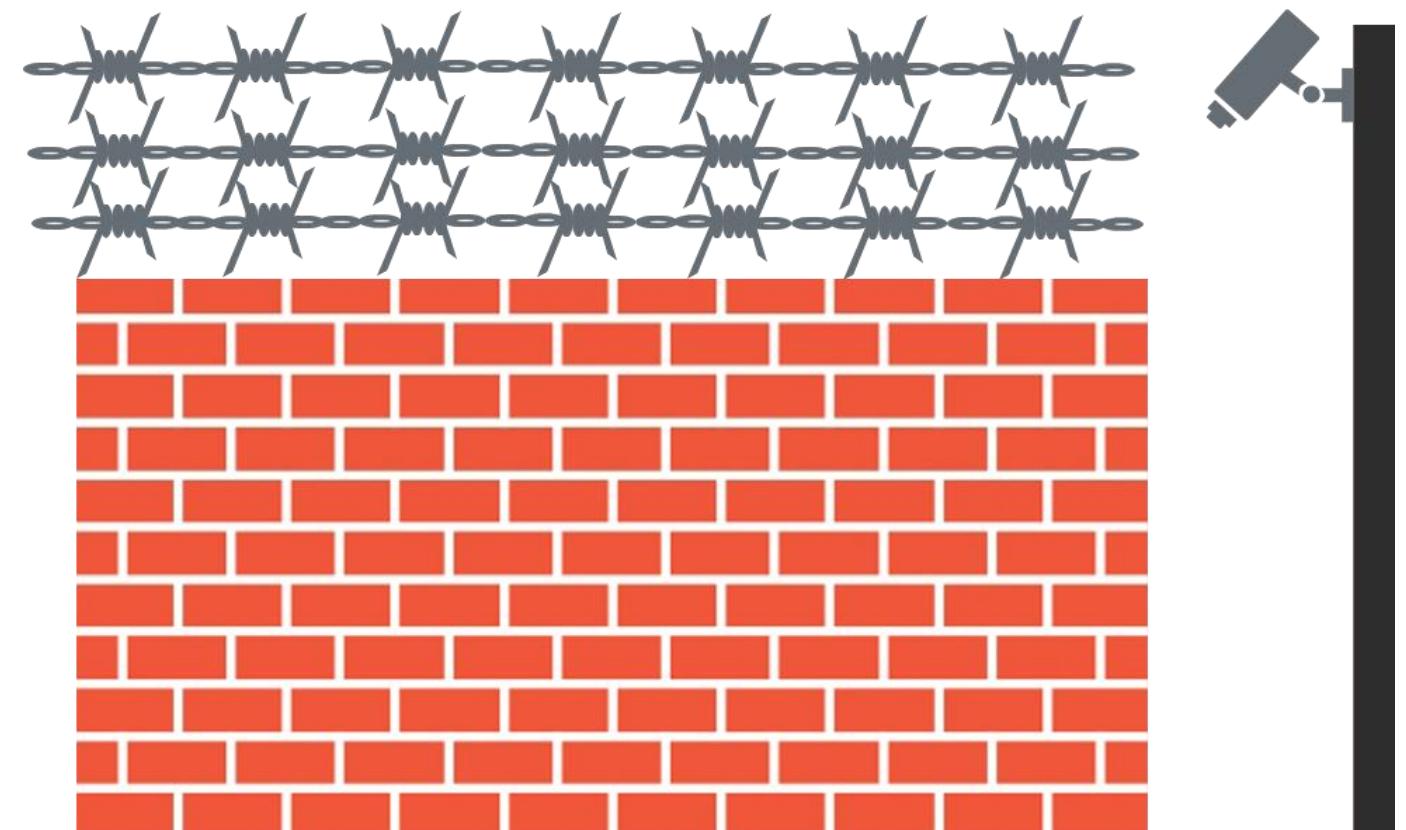


Perimeter Intrusion Detection

Perimeter sensors alert security when any intruders attempt to gain access across the open space or attempt to breach the fence line.

Open-terrain sensors include:

- Infrared
- Microwave systems
- Time-domain reflectometry (TDR) systems
- Video content analysis and motion path analysis



Importance of Lighting in Security

Effective lighting is pivotal in security, ensuring visibility and deterrence throughout low-light hours.

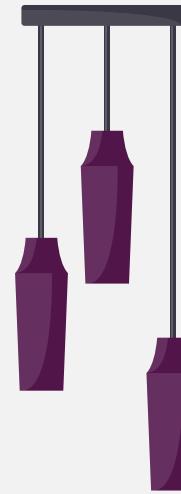
- **Improves visibility:** Allows security personnel to clearly assess surroundings during nighttime
- **Enhances surveillance:** Boosts the performance of CCTV, providing clearer footage under all conditions
- **Deters intruders:** Acts as a psychological deterrent, reducing potential security breaches
- **Cost-effective:** Maintains minimal upkeep costs, offering a sustainable security enhancement



Types of Lighting Systems

The following are the main types of lighting systems, each serving distinct functions within a security framework:

Continuous Light



Emergency light



Standby light



Movable light

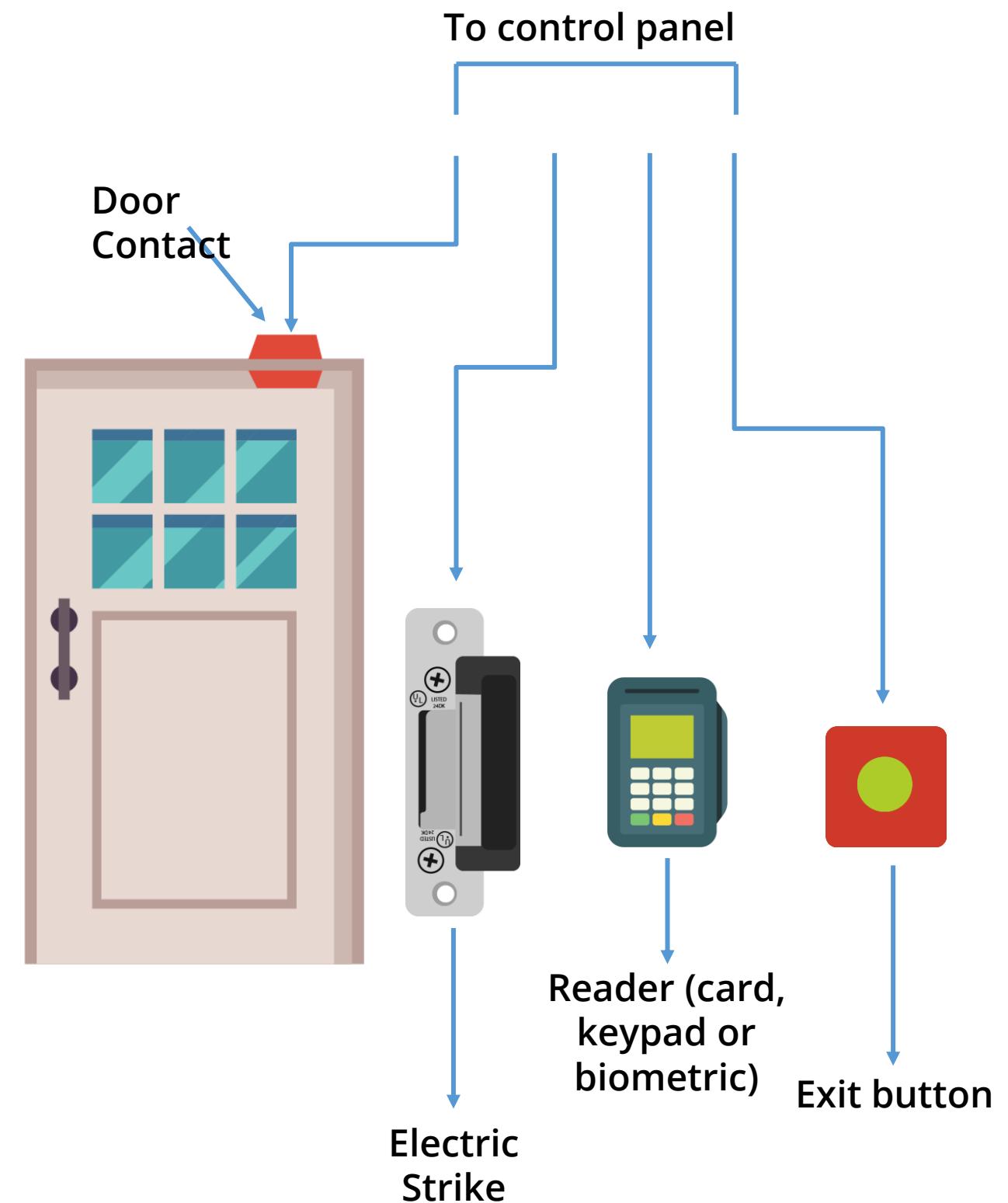


Access Control

An access control system (ACS) allows only authorized personnel into a controlled area to reduce the risk of crime.

Basic components of an ACS include:

- Card readers
- Electric locks
- Alarms
- Computer systems



Types of Access Control Systems

Access cards

Types include magnetic stripes/ proximity cards/ smart cards

Biometrics

Methods encompass fingerprint, facial image, hand geometry, voice recognition, iris patterns, retina scanning, signature dynamics, and keystroke dynamics

Closed circuit televisions

Comprise cameras, recorders, switches, keyboards, and monitors that enable the observation and recording of security events

CCTV color camera

Provides additional details, such as the color of a vehicle or a subject's clothing

Types of Access Control Systems

Digital video recorder (DVR) and monitor displays

Camera footage is downloaded to a hard drive for historical information storage.

Security patrols

Guards or officers patrol and inspect properties to safeguard against fire, theft, vandalism, terrorism, and illegal activities.

Guard dogs

Guard dogs serve as a physical control that provides detective, preventive, and deterrent security measures.

TECHNOLOGY

Deceptive Technologies

Deceptive Technologies

These are cybersecurity solutions designed to outsmart attackers by creating a web of illusions within your network.

This technology can assist in:

- Early threat detection
- Reduced dwell time
- Improved incident response
- Wasting attacker resources

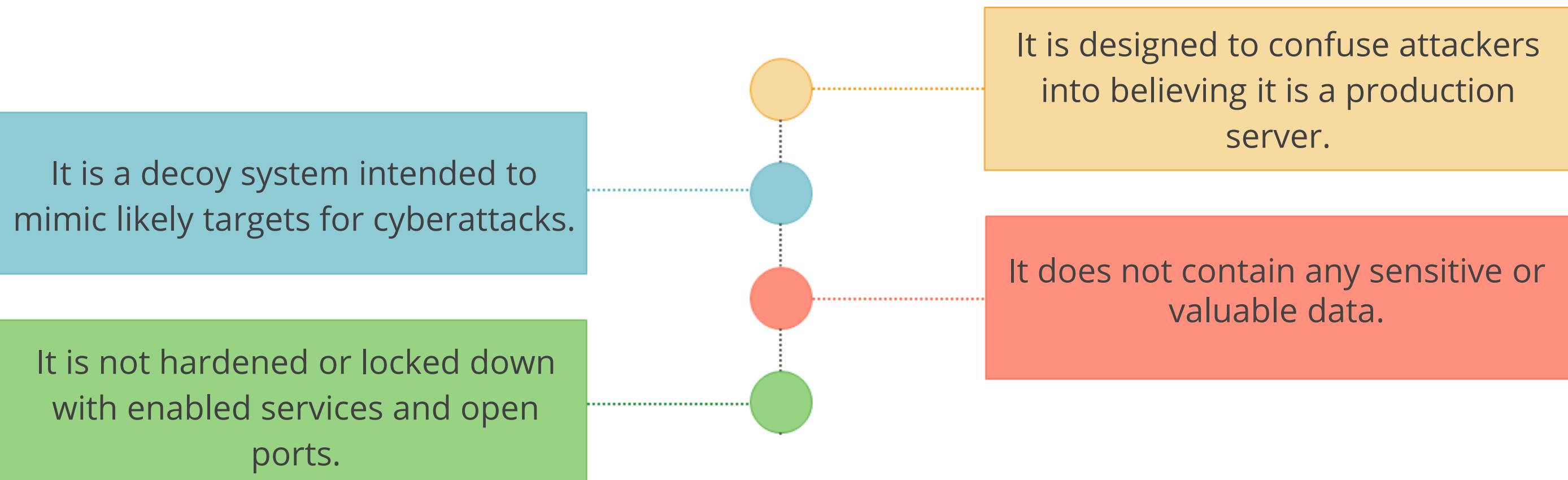


Honeypot

Honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect, and study hacking attempts to gain unauthorized access to information systems.



Features of Honeypot



Honeynet

A honeynet is a set of multiple honeypots linked together as a network or subnet that simulates a larger network installation.



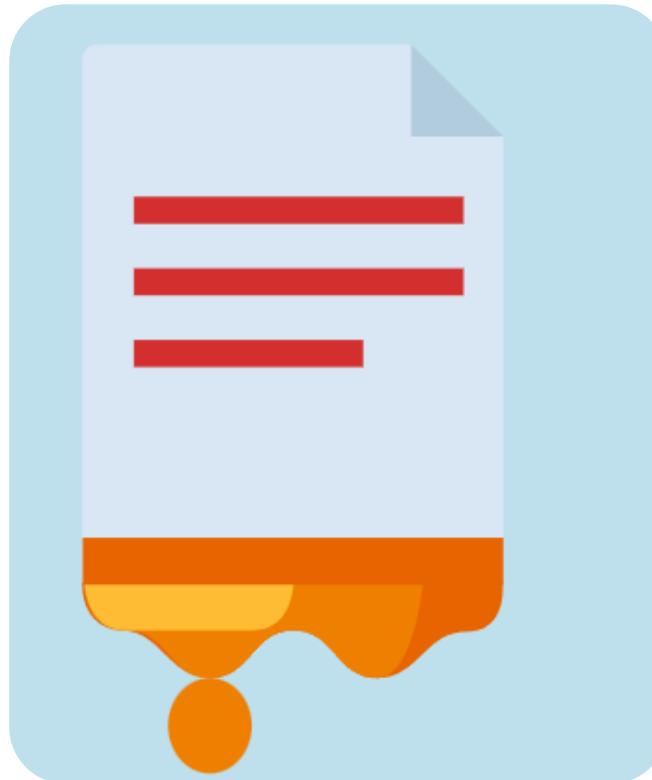
Honeytokens

Honeytokens are fictitious words or records added to legitimate databases to detect unauthorized attempts to access information.



They are characterized by properties that make them appear as genuine data items.

Honey file



- Honey files are not software applications or services but decoy files used for security purpose.
- These files are decoy files intentionally placed on a network file share to lure attackers trying to steal data.

TECHNOLOGY

Types of Security Controls

Asset

An asset is any resource that gives value to an organization.



- An asset can be tangible or intangible.
- This includes people, hardware, software, data, information, or reputation.

Vulnerability

Vulnerability refers to a condition in the system that, either intentionally or accidentally, causes a security weakness. This compromises the security of the system.



Examples: Unpatched software, buffer overflow, lack of awareness training

Threat

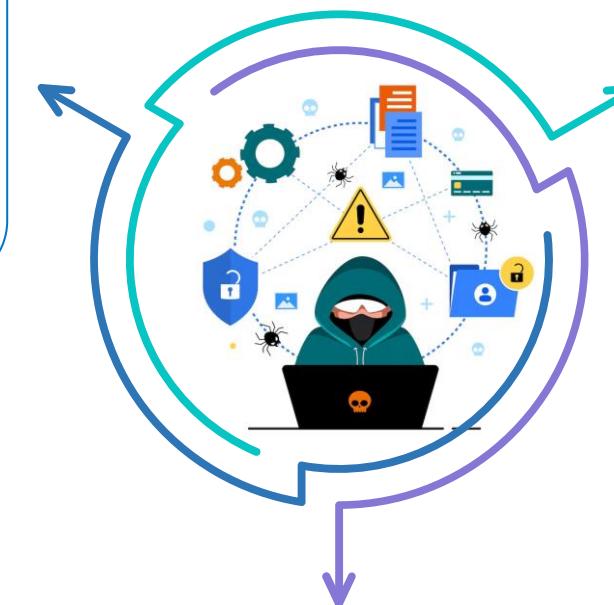
A threat is anything that has the potential to cause harm to a system or data.

Intentional threats:

These are malicious attempts to harm the system or steal data.

Natural threats:

Floods, earthquakes, fires, and other natural disasters can damage computer hardware and destroy data.



Unintentional threats:

These are accidental events that can cause damage, even if they are not malicious.

Threat Agents

A threat agent, also known as a threat actor, is an individual, group, or organization that can initiate an attack on a system or data.



Examples: Hackers, cybercriminals

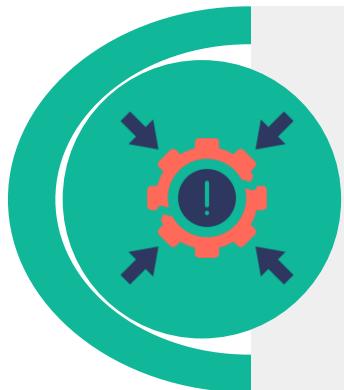
Risk



Risk is defined by the International Systems Audit and Control Association as the combination of the probability of an event and its consequences.

Key terms associated with risk are:

Impact



Magnitude of damage emerging from a threat exploiting a vulnerability

Likelihood



Probability of a threat exploiting a particular vulnerability

Examples of Risks

Threat agent	Threat	Vulnerability	Risk scenarios
Fire	Destruction of operating facility	Faulty fire detection or suppression equipment	Loss of life or property
Clueless user	Sharing of sensitive data using social engineering	Lack of security awareness training	Financial loss or reputation loss
Malicious insider	Data theft	Lack of adequate access controls on data	Legal risk, financial loss
Hacker	Unauthorized hacking	Unpatched server	Server unavailability, financial loss

Security Controls

Controls are necessary to protect the confidentiality, integrity, and availability of assets.



Security controls are put into place to reduce the risk an organization faces.

Control Categories



Administrative controls



Technical controls



Physical controls

Administrative Controls



- Administrative controls are managerial controls focusing on personal and business practices.
- These are the policies and procedures defined by an organization's security policy and other regulations or requirements.
- Examples: Security documentation, risk management, personnel security, and training

Technical Controls



- Technical controls, also known as logical controls, are implemented as systems such as hardware, software, or firmware.
- Examples: Firewalls, IPS, antivirus software, and encryption

Physical Controls



- Physical controls are implemented to protect facilities, personnel, and other physical resources.
- Examples: Security guards, CCTV, locks, doors, fencing, and lighting

Control Types



Preventive



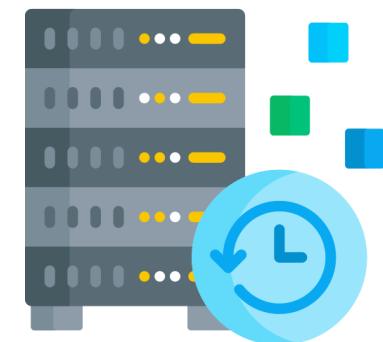
Deterrent



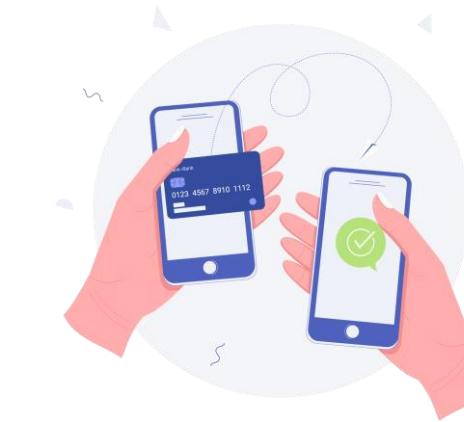
Detective



Corrective



Recovery



Compensative

Preventive Control



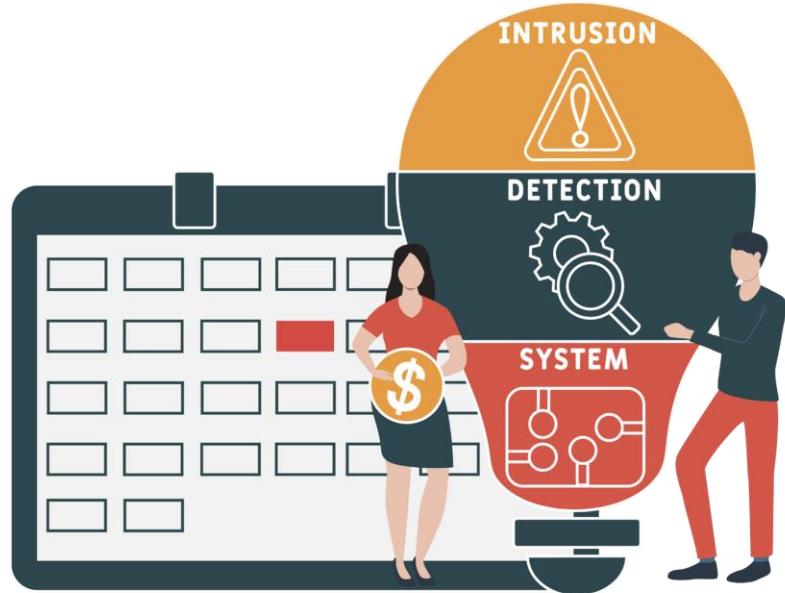
- Preventive or preventative controls are intended to stop an incident from occurring.
- Preventative control operates before an attack and eliminates or reduces the likelihood of a successful attack.
- Walls and locks can stop people from entering an area in an unauthorized manner.

Deterrent Control



- Deterrent controls are intended to discourage a potential attacker.
- These may include warning signs, policies, NDAs, and legal penalties against trespasses or intrusions.

Detective Control



- Detective controls are intended to discover or detect unwanted or unauthorized activity.
- These can include security guards, logs, intrusion detection systems (IDS), and the security team reviewing the outputs of a security information and event management (SIEM) system.

Corrective Control



- Corrective controls are intended to correct any problems resulting from a security incident.
- They reduce or eliminate the opportunity for the unwanted event to recur.
- Example: Fire extinguishers to put off fire or patching a system to fix vulnerabilities

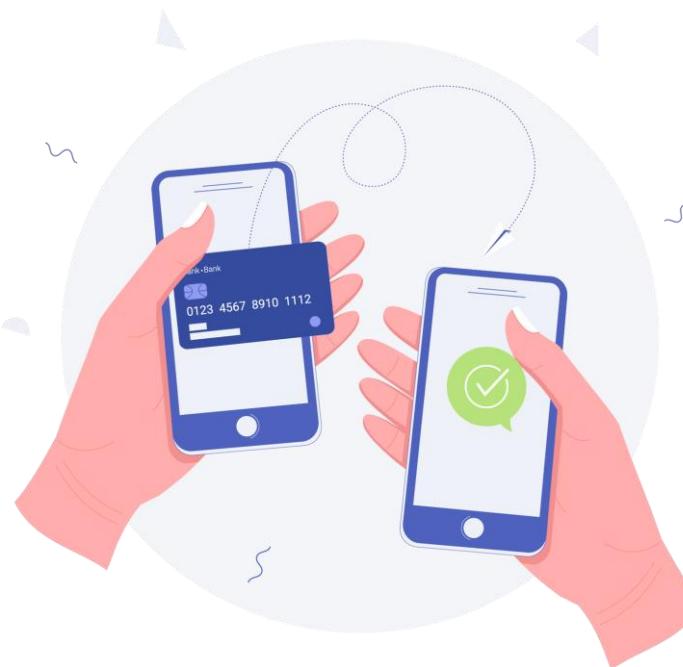
Recovery Control



- Recovery controls are intended to bring the environment back to regular operations.
- These include backups and disaster recovery plans.

Compensative Control

A compensative control, also known as an alternative control, is implemented to fulfill a security requirement deemed too difficult or impractical to implement currently.



Example:

- In a small firm, a single user has access to and performs the tasks of accepting cash payments and recording the payments.
- Due to the nature of the business and for efficiency, the same user performs both tasks.
- To prevent fraud, supervision is required.
- Therefore, compensative control is required.
- Example: A second user must perform a reconciliation, reviewing the cash against the recorded transactions.

Compensative Control

Compensative control must meet the following four criteria:

Have the intent and rigor of the original requirement

1

Provide a similar level of defense as the original requirement

2

Be above and beyond other requirements

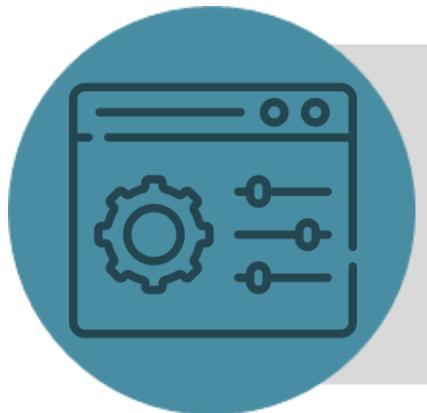
3

Be commensurate with the risk imposed by ignoring the original requirement

4



Control Selection



The selection of security controls will depend on the nature of the business, the complexity of the environment, and the assets' value.



Security control must make good business sense, which means it should be cost-effective. Its benefits must outweigh its costs.

Control Matrix

	Preventive	Detective	Deterrent	Corrective	Recovery
Administrative	Separation of duties	Audit	Disciplinary policy	Employee disciplinary actions	Disaster recovery plan
Technical	Firewall	IDS	Warning banner on login	Vulnerability patches	Data backup
Physical	Walls, fences, gates	CCTV	Beware of dog sign	Fire suppression systems	Disaster recovery site

Multiple Control Facilities

Control can provide several functionalities depending on their implementation and operation.



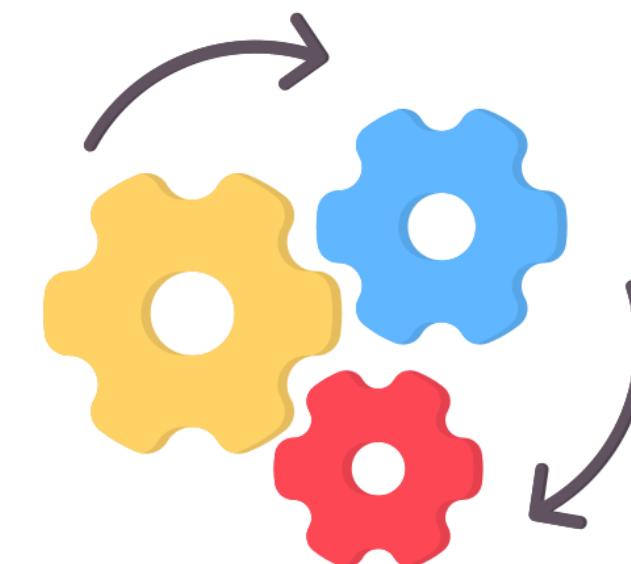
Example:

- Surveillance cameras can be considered a *deterrent control* since cameras discourage a potential attacker from doing an unauthorized action.
- It is also considered a *detective control*.
- It is also a *compensative control* since it provides an additional detection method for security guards.

Importance of Change Management Processes and the Impact to Security

Business Process Impacting Security Operations

- A business process is a series of tasks used by an organization to achieve a goal or deliver a product or service.
- Each process can affect security.
- For example, an ineffective approval process can lead to poorly vetted changes and new vulnerabilities. Performance baselines are used to measure the impact of changes on security.



Change Management

Changes to the system are tracked and approved through change control procedures, which involve identifying, controlling, and auditing all changes made to the system.

Change control:

- Ensures changes are implemented in an orderly manner through formalized testing
- Ensures awareness is created among users about the impending change
- Analyzes the effect of the change on the system after implementation
- Reduces the negative impact of the change on the computing services and resources



Change Management Process

The procedures for change control process implementation and support include:

1. Request for a change to be introduced

A request is sent to the responsible individual or group who administers and approves changes.

2. Change approval

After proper analysis and justification, the change is approved.

3. Change intended cataloging

The change control log is updated and documented.

Change Management Process

The procedures for change control process implementation and support include:

4. Change testing

Change is formally tested.

5. Change scheduling and implementation

Change is scheduled and implemented.

6. Report to the appropriate parties about the change

Change is summarized and reported to the management.

Change Types

Standard change

A pre-authorized, low-risk, and low-impact change that is well-understood, fully documented, and can be implemented without needing additional authorization is considered a standard change.

Normal change

A change must follow the entire change process. It should be scheduled, assessed, and authorized following a standard process. This includes both minor (low to medium impact) and major (high impact) changes.

Change Types

Emergency change

- A high-impact and urgent change that must be implemented as soon as possible without strictly following the standard process is known as an emergency change.

Expedited Changes

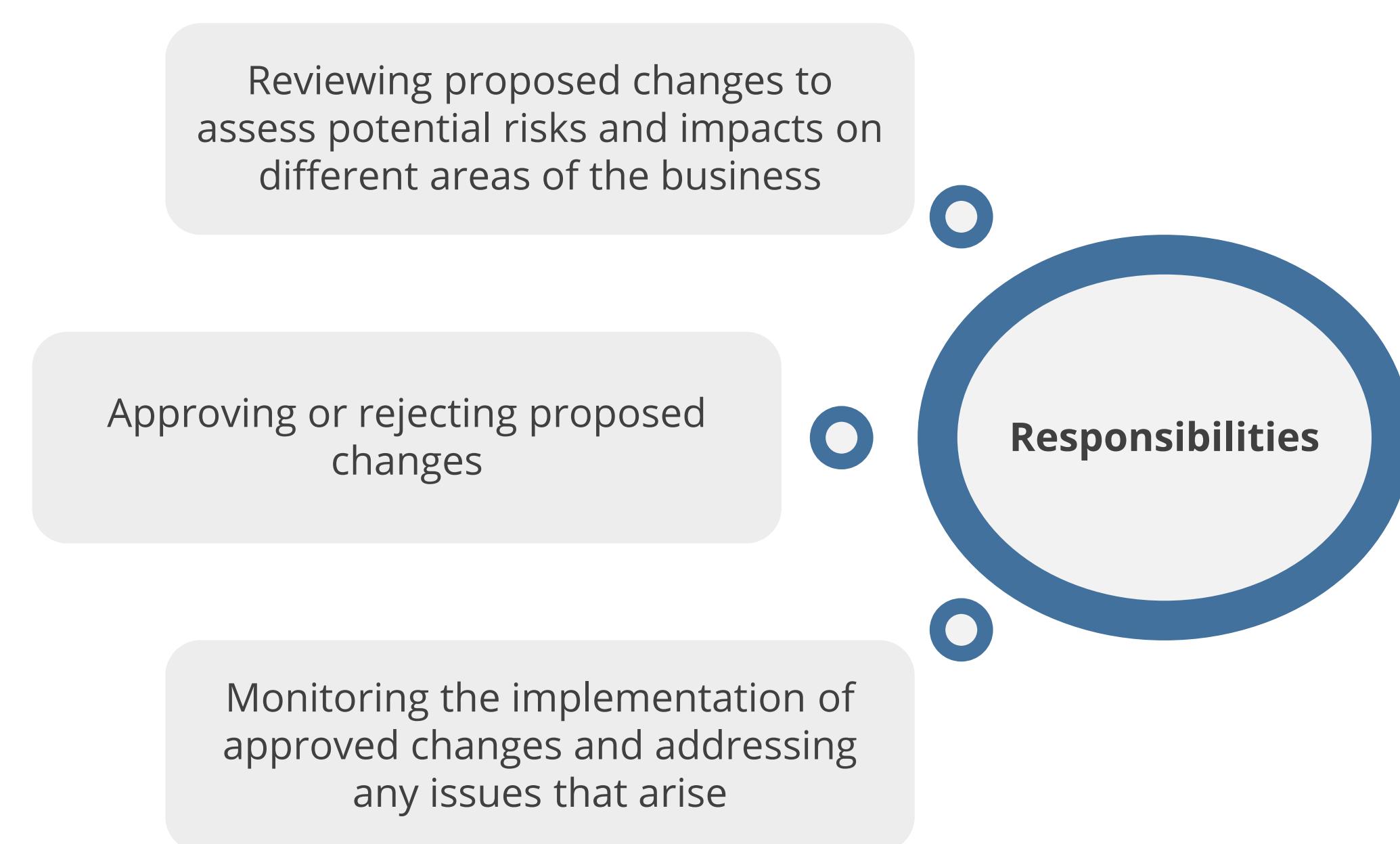
- Expedited changes are a specific type of request that require faster approval and implementation than a standard change.
- They are used for situations that require urgent implementation of a change but do not meet the criteria for an emergency change.

Change Advisory Board

- A Change Advisory Board (CAB) is a group of individuals from different departments within an organization responsible for reviewing and approving proposed changes.
- The primary objective of a CAB is to ensure that any changes made to the organization, such as IT infrastructure and processes, are implemented smoothly and with minimal disruption.
- Typically, the CAB includes representatives from IT, operations, finance, HR, and other relevant departments, although the specific members can vary based on the organization's size and structure.



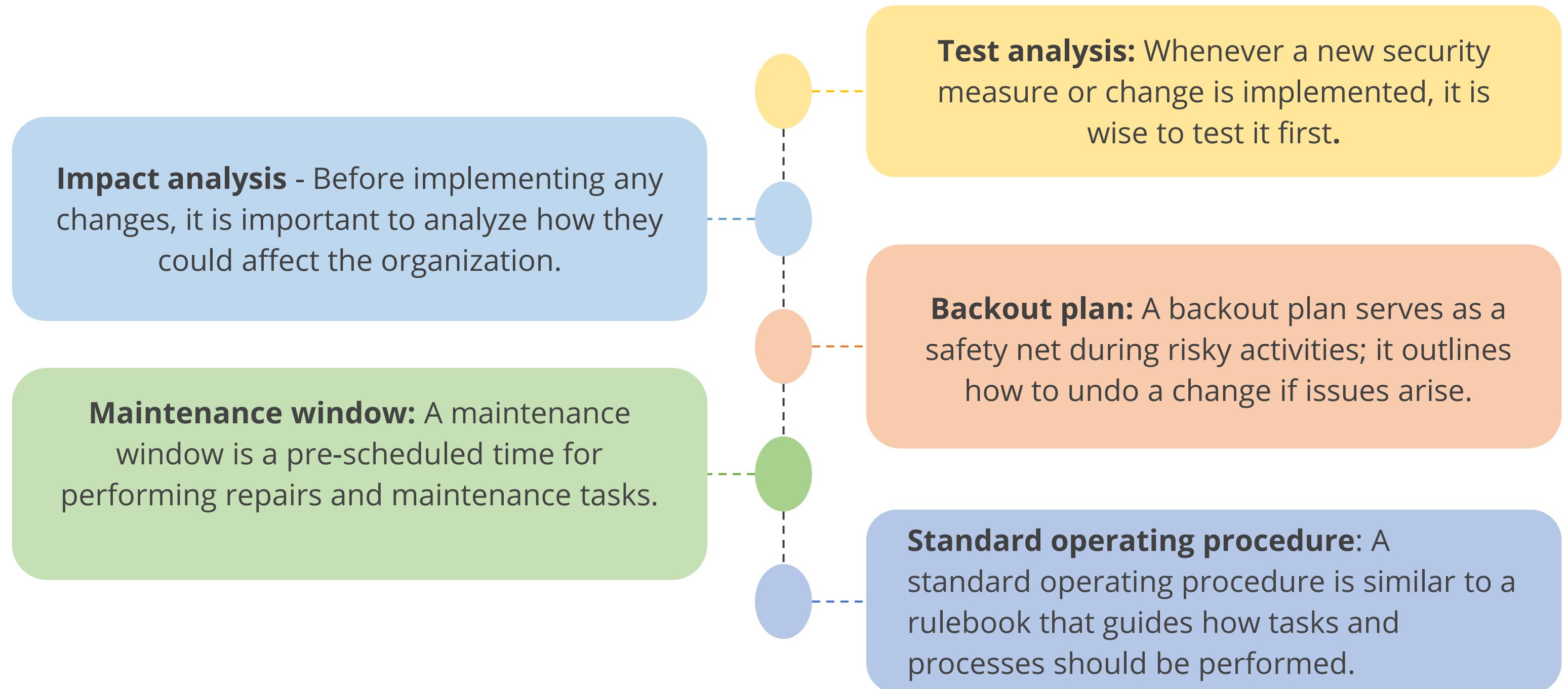
Change Advisory Board



Change Advisory Board

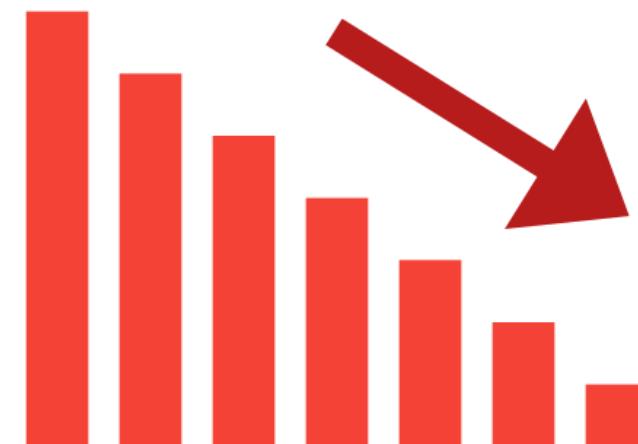


Change Management System Activities



Technical Implications

- Technical implications refer to the potential consequences of a technology-related decision or event in cybersecurity.
- They can involve changes to network infrastructure, security protocols, or additional server capacity after implementing new software or systems.
- It is essential to understand all technical implications of any new or existing system to ensure that functionality and security are maintained.



Technical Implications of Change Management

Downtime

Downtime adversely affects revenue. To minimize this, we will implement a business continuity plan to prevent it.

Service restart

Shutting down or rebooting systems can disrupt legitimate user access to computing resources and hinder incident response and recovery efforts.

Application restart

Application restart vulnerabilities refer to potential security weaknesses that may arise when an application is restarted. Inadequate restart procedures can lead to data inconsistencies or corruption.

Technical Implications of Change Management

Legacy application

These are software that has been used for a long time, often with outdated security and no vendor support.

Dependencies

Services, such as the IP Helper service, depend on other services or system components to run before they can start running.

Whitelist or Blacklist or Restricted Activities

**Whitelists or
Allow lists**

- An allow list grants access only to specified users and can be used on a firewall or by AppLocker to control which applications and files can run.
- A whitelist ensures that only approved applications can be installed or run.
- Any application absent on an allow list or whitelist will be denied access.

**Blacklist or
Deny lists**

- A deny list or blocklist prevents access to specified users and can be used on a firewall to deny access.
- A blocklist prevents harmful applications from running; it requires you to specify which applications should be denied.
- A blocklist also prevents unauthorized users from gaining access to your network.

Whitelist or Blacklist or Restricted Activities

Restricted activities

- Restricted activities prevent actions that could potentially lead to vulnerabilities or disruptions.
- These activities include unauthorized software installations, unauthorized system modifications, direct access to critical servers, and unauthorized access to sensitive data or data transfers.

Documentation



- Documentation plays a critical role in successful change management.
- Comprehensive documentation of changes promotes transparency, accountability, and a clear understanding of the modifications being made.
- Well-documented changes facilitate tracking of modifications, making it easier to identify the individuals responsible for the changes and the reasons behind the modifications.
- This, in turn, enhances security by minimizing the risk of unauthorized or unaccounted alterations.

Change Management Documentation

Change management framework:

This document outlines the overall approach your organization takes to change management.

Change request forms:

These forms capture details about proposed changes, including the nature of the change, its rationale, potential impacts, and resource requirements.

Change approval process:

This document outlines the steps involved in getting a change proposal approved, including who needs to review it and the criteria they will use.

Change Management Documentation

Implementation plans:

These plans detail the specific steps involved in implementing a change, including timelines, responsibilities, training needs, and communication strategies.

Change impact assessments:

These assessments evaluate the potential impact of a change on different areas of the business, such as costs, resources, and employee morale.

Metrics and evaluation criteria:

These documents define how the success of a change initiative will be measured, including factors such as user adoption rates and cost savings.

Version Controls

- Version control is a system that records changes to a file or set of files over time, enabling you to recall specific versions later.
- It allows you to track modifications, pinpoint when and by whom changes were made, and, if necessary, revert to an earlier version.
- Organizations that lack proper version control face challenges in tracking bug fixes and applying security patches.



Version Controls

- It also makes it difficult for consumers to correlate, triage, and patch security vulnerabilities.
- Proper version control is a best practice to maintain a secure and efficient operational environment.

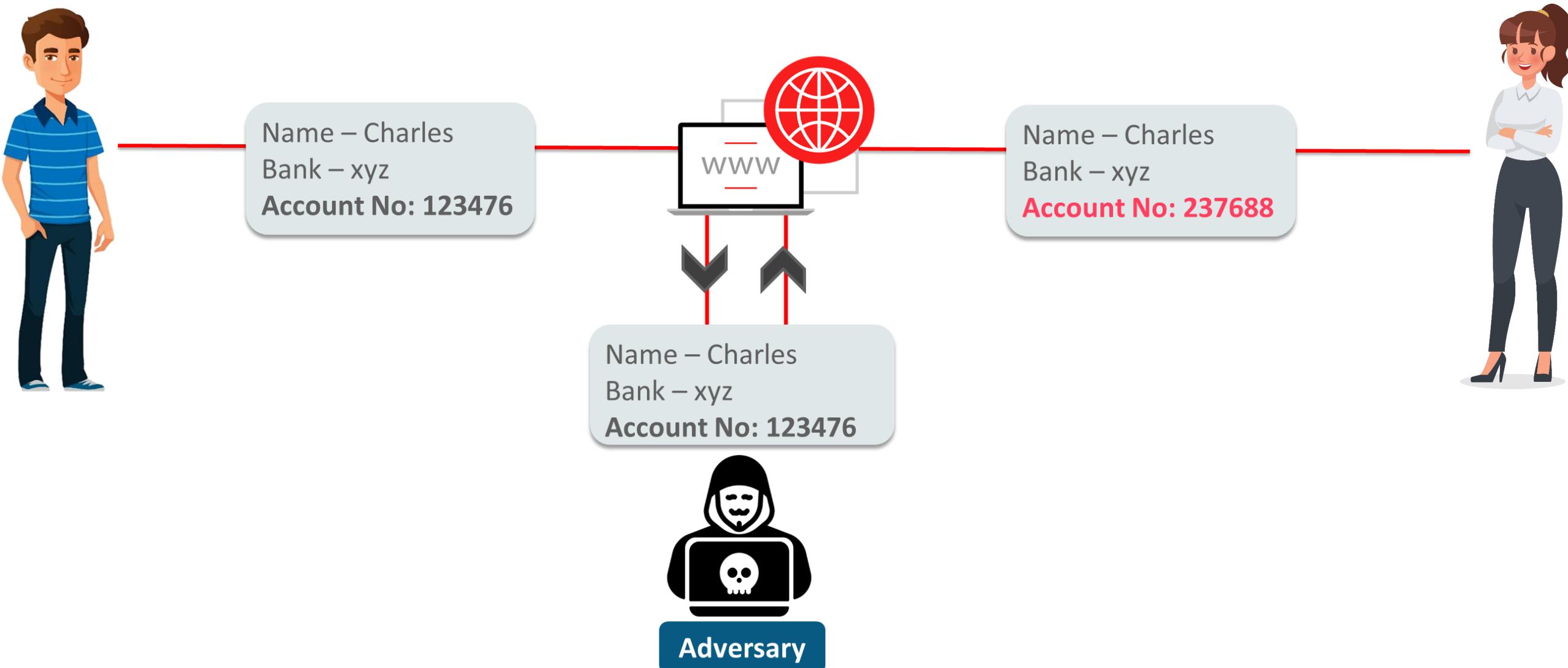


TECHNOLOGY

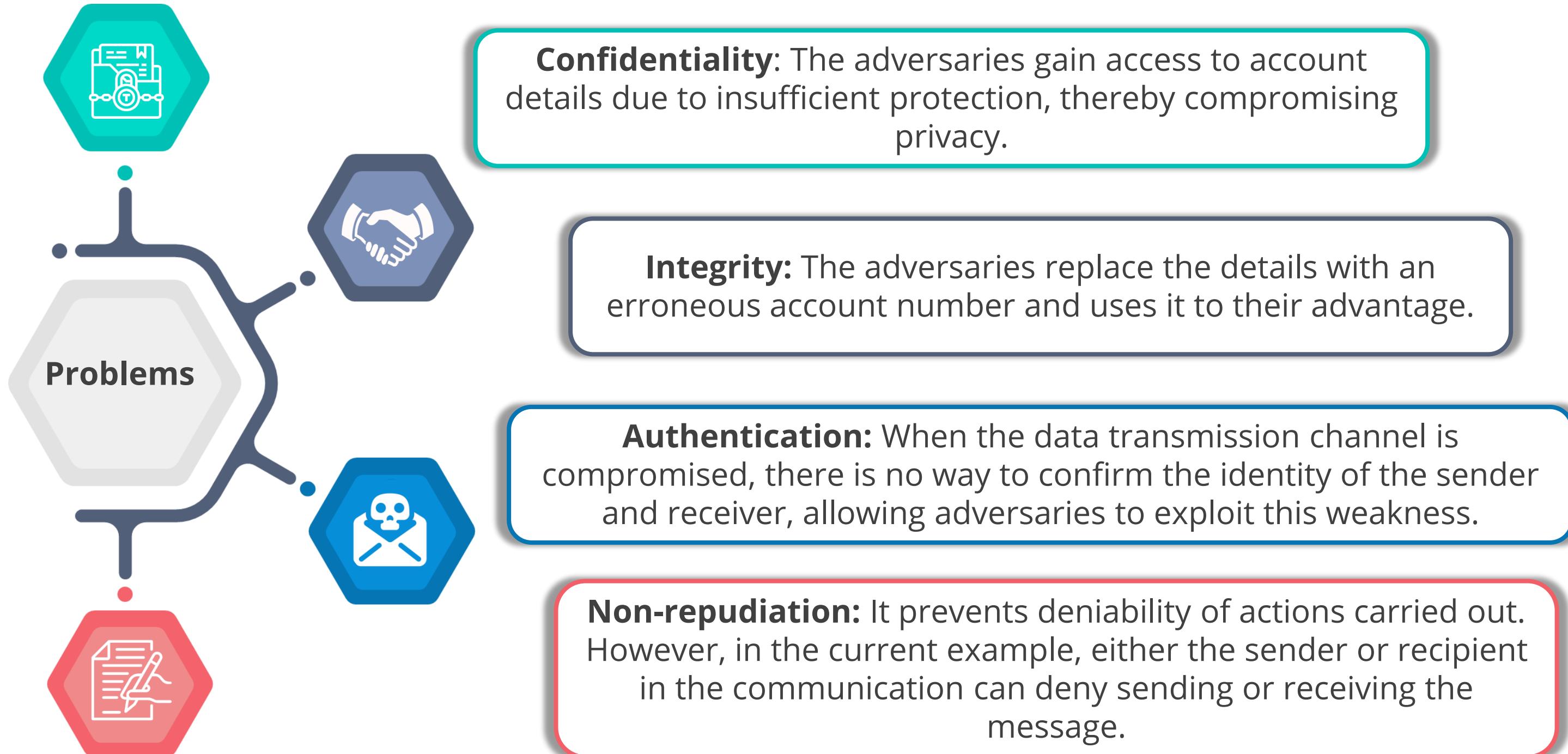
Introduction to Cryptography

Scenario (Without Cryptography)

- Consider an example where Charles requests Alice to lend him some money. He shares his bank account details with her through an insecure connection. An attacker intercepts the connection, retrieves the data, and modifies the account details.



Problems Faced When Cryptography Was Not Used



What Is Cryptography?



Cryptography is the study of securing communication and data using algorithms to prevent exposure to unintended parties.



It is the science of transforming valuable information for secrecy.

Hi, welcome to XYZ post-graduate program on cybersecurity

Cryptographic algorithm

Kl, zhoфрph wr Hgxuhnd'v srvw judgxdwh surjudp rq fbehuvhxulwb

Original text

Coded text

Features of Cryptography



Data confidentiality

Confidentiality and privacy of data is maintained through **encryption**. The encrypted data is practically useless to an adversary without the decryption key.



Authentication

The **authenticity** of the message is verified through **digital signatures**, which confirm the sender's identity.



Data integrity

The **integrity** of a message is preserved using **hashing algorithms**, where the same message always results in the same hash.

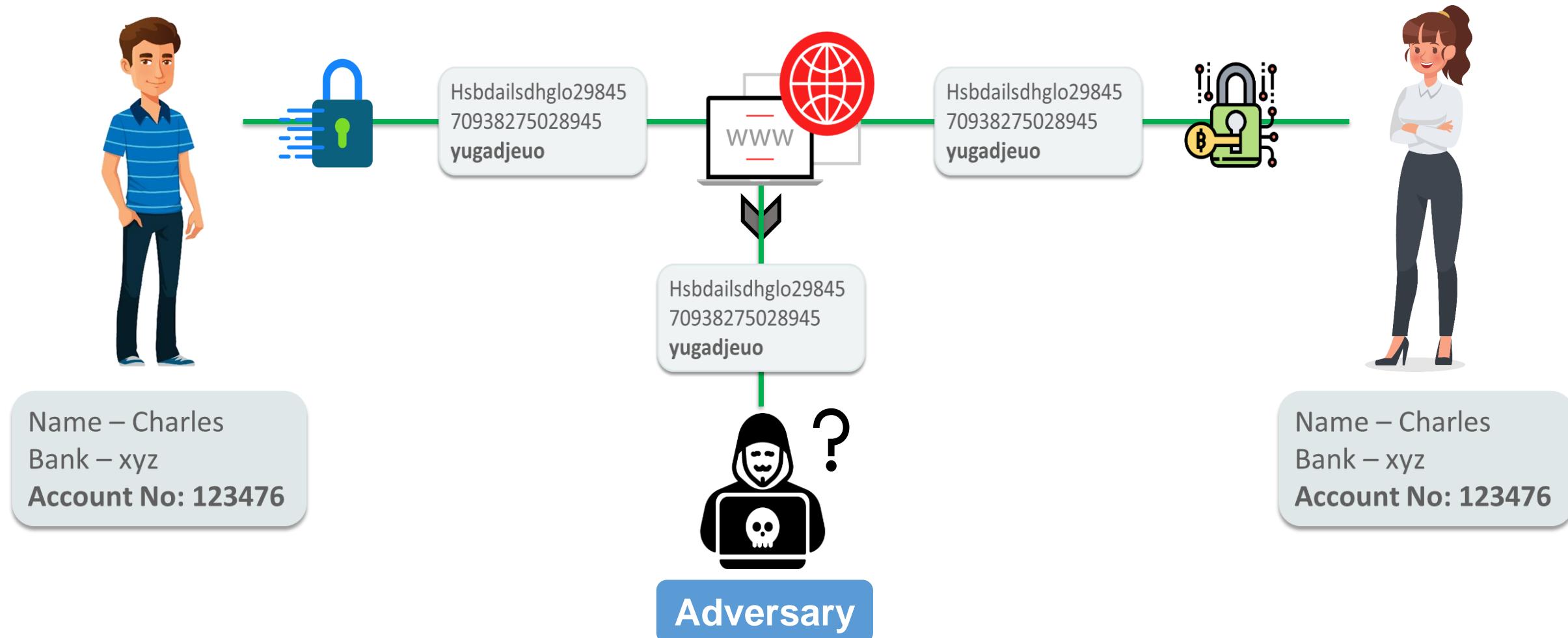


Non-repudiation

Non-repudiation is ensured through **digital signatures or digital certificates**, preventing a user from denying sending the message.

Solution Strategy to Solve the Problem

When your credentials and data are protected with cryptographic algorithms, even if a hacker breaches the security layer or hacks the server, the data remains unintelligible.



Basic Definitions

Cryptography

The science of secret writing that enables an entity to store and transmit data accessible only to the intended individuals

Cryptosystem

Hardware or software implementation of cryptography that contains all the necessary software, protocols, algorithms, and keys

Cryptology

The study of both cryptography and cryptanalysis

Algorithm (Cipher)

A set of mathematical and logical rules used in cryptographic functions

Kerckhoffs's principle

The concept that an algorithm should be known and only the keys should be kept secret

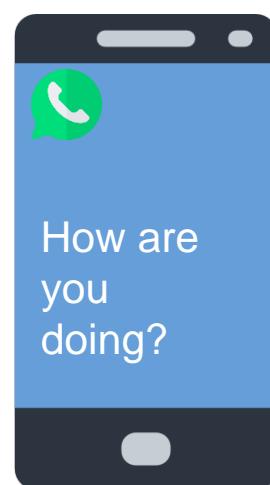
TECHNOLOGY

Cryptography Around Us

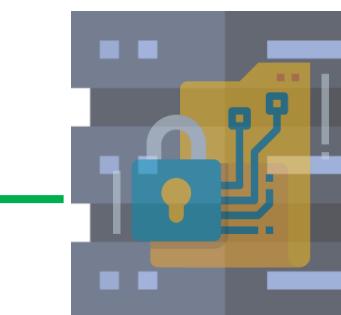
WhatsApp

WhatsApp uses end-to-end encryption to transfer messages between two users.

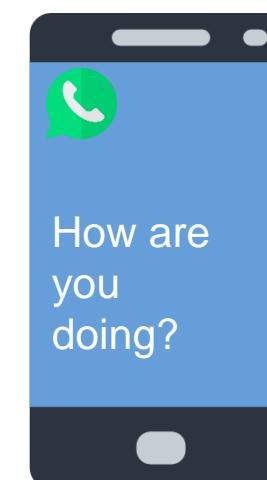
End-to-end encryption ensures that the message encrypted at the sender's end can only be decrypted at the receiver's end.



Sender



WhatsApp Server



Receiver

Third parties or even WhatsApp cannot read the users' messages due to end-to-end encryption.

E-Banking



Online transactions

In 2002, financial institutions began using the AES algorithm for electronic transactions and creating security infrastructures to protect data stored in computer systems.



Automated Teller Machine (ATM)

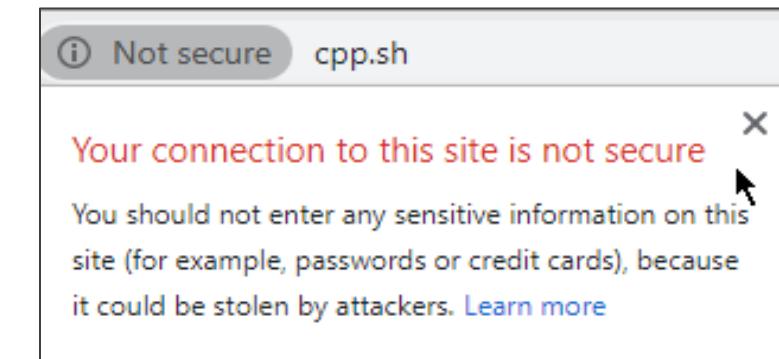
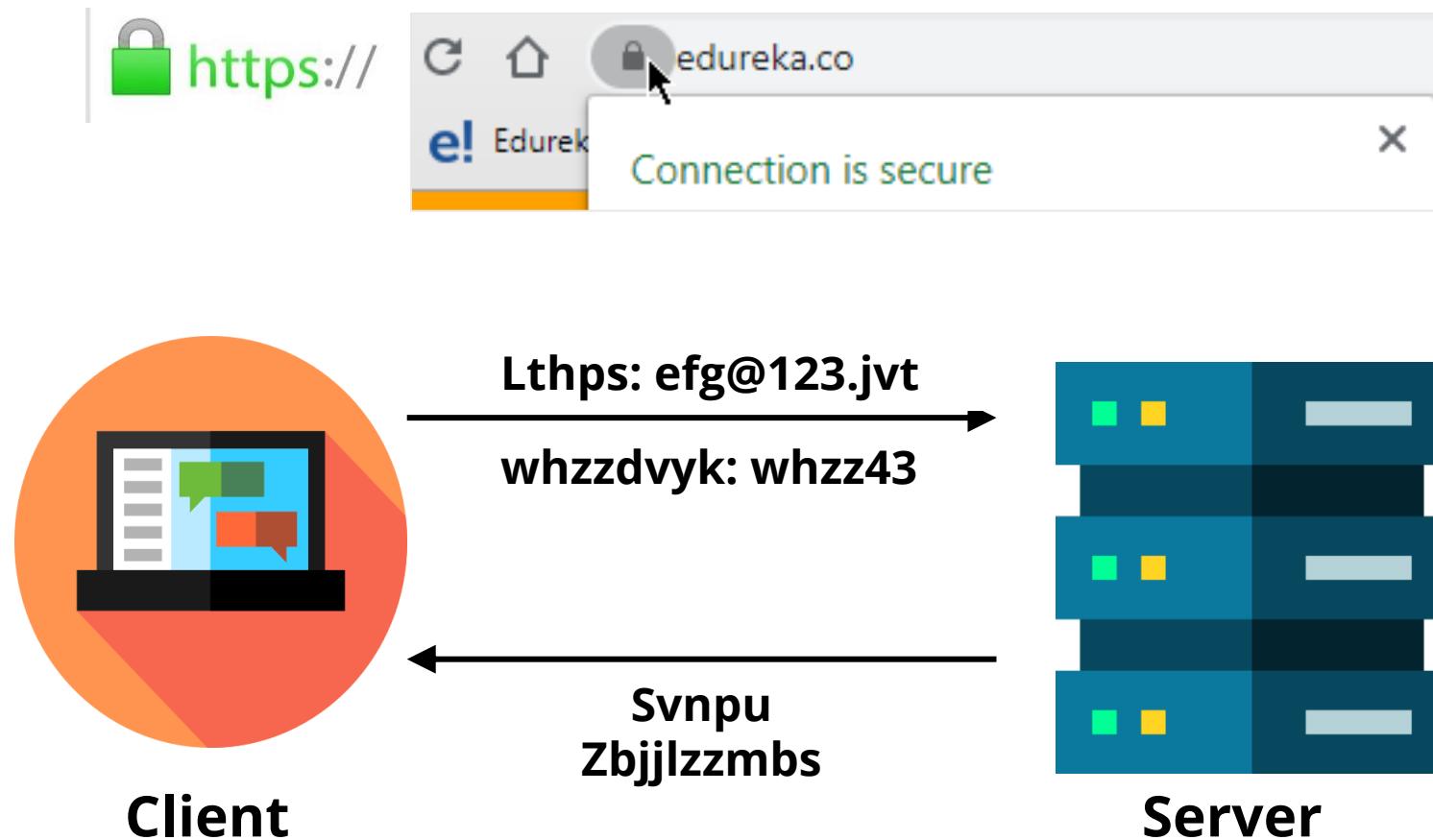
All ATMs have encryption pads that encrypt the PIN code and send it to the bank, ensuring authorization and security.



One-time password

- One-time password (OTP) is generated to facilitate two-level authentication.
- The OTP is valid for only one transaction; the user sends it to the bank to authorize a transaction.
- The OTP can only be decrypted by the bank's terminal when the user enters the correct PIN.

HTTPS



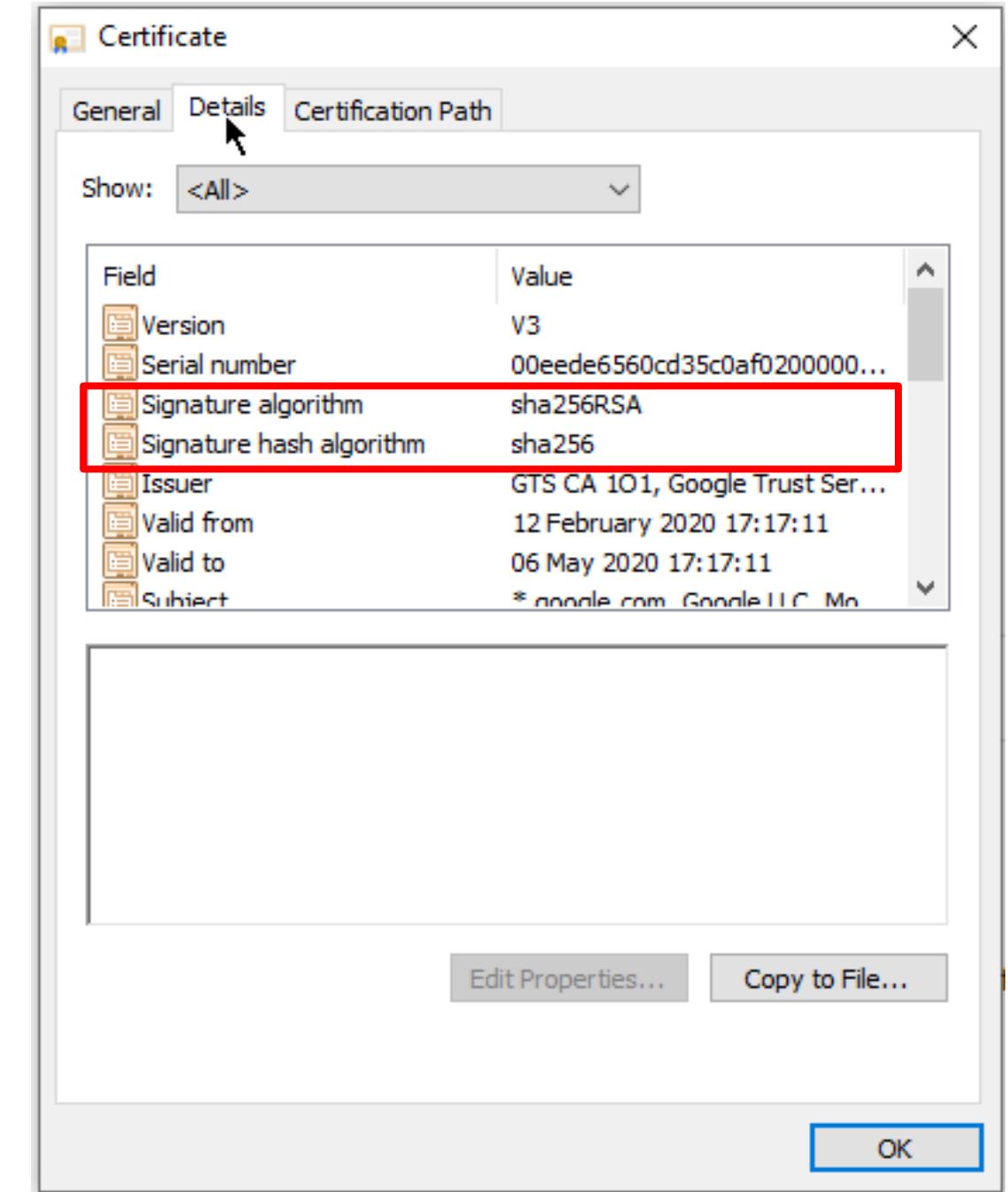
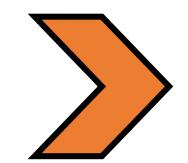
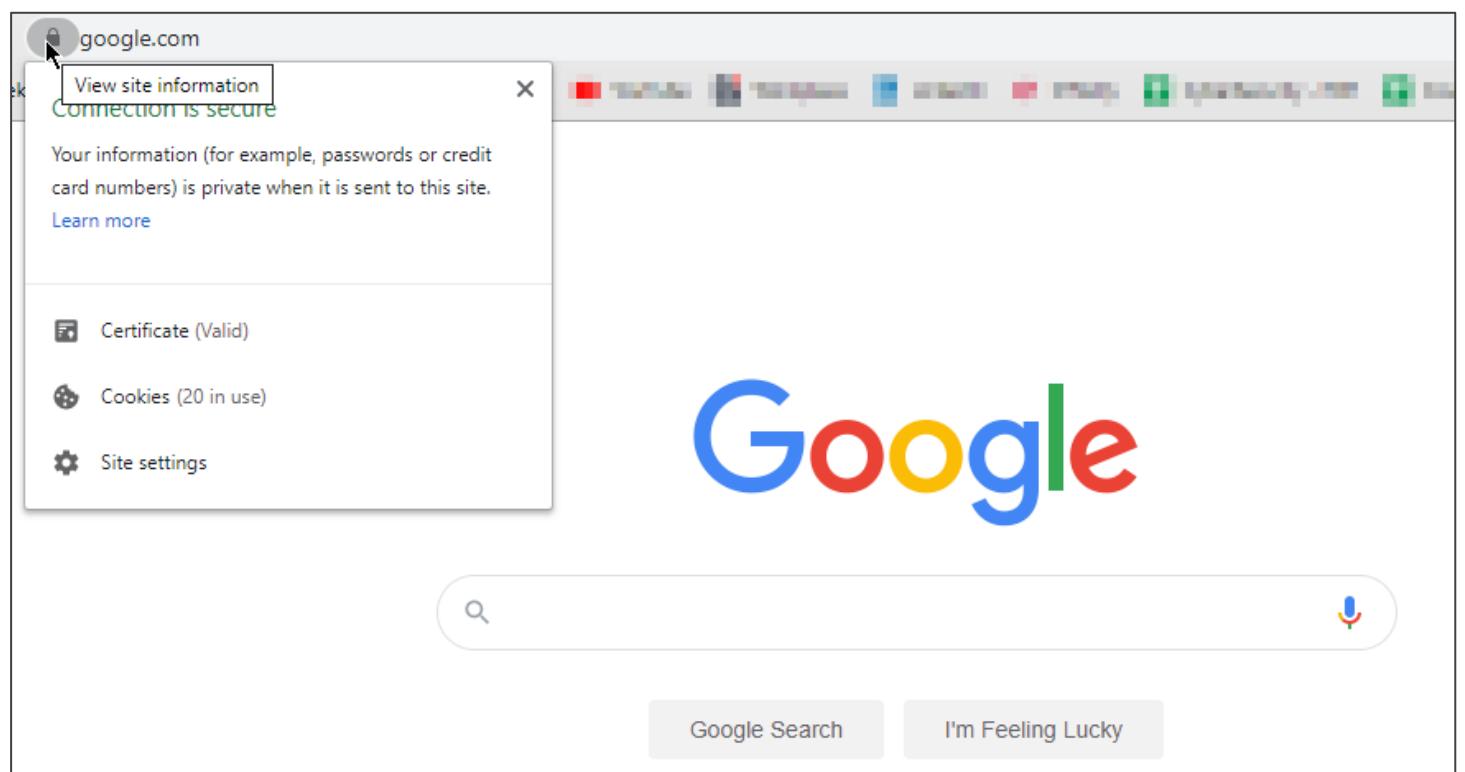
- When you browse the internet while connected to a network, people connected to the same network can eavesdrop on your packets.

- HTTPS indicates that your connection to the web browser is encrypted.

- Packets are encrypted, and only the server has the decryption key to respond to your request.

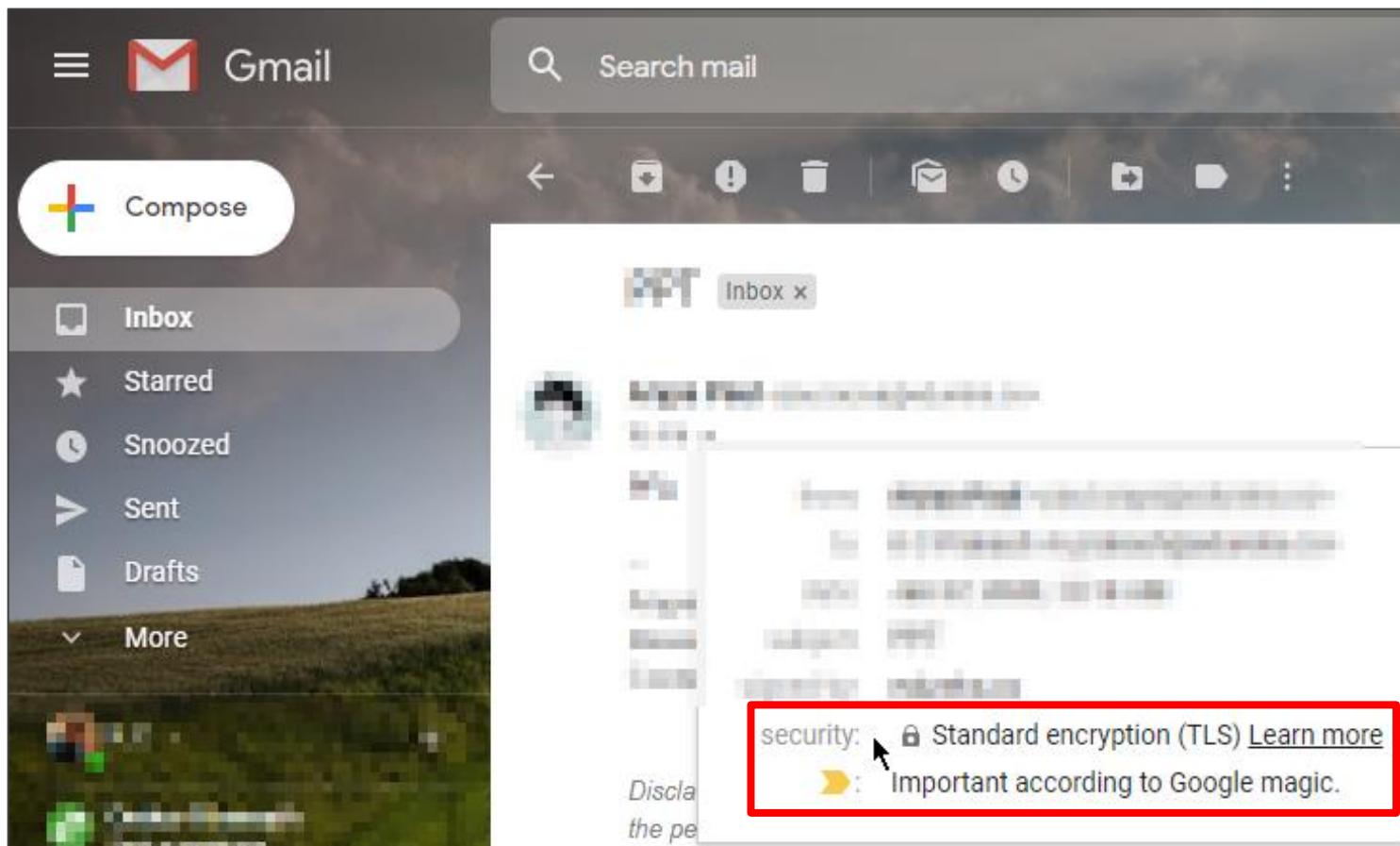
HTTPS (Cont.)

- Several cryptographic algorithms are incorporated into protocols when you try to establish a secure connection.
- To view these algorithms in your web browser, simply click the **Lock** icon on the address bar, then click **Certificate**, and finally click **Details**



Gmail

TLS is a standard cryptographic protocol that secures communication over the internet. It ensures data authenticity and integrity by establishing a cipher suite for each communication session.



- Cryptographic algorithms coupled with e-mail protocols provide the following security services for electronic messaging applications:
 - Authentication
 - Message integrity
 - Non-repudiation of origin (SHA256)
 - Data security (ECC256)

A primary use case of TLS is encrypting communication between a web browser and a server.

Disk Encryption



Disk encryption

This technology provides data at rest encryption. Symmetric encryption algorithms are used for encryption and decryption.



Full-Disk Encryption (FDE)

All contents of the disk are encrypted and converted into unreadable text with the help of symmetric ciphers (AES 256).



Popular FDE software -
BitLocker



File-Based Encryption (FBE)

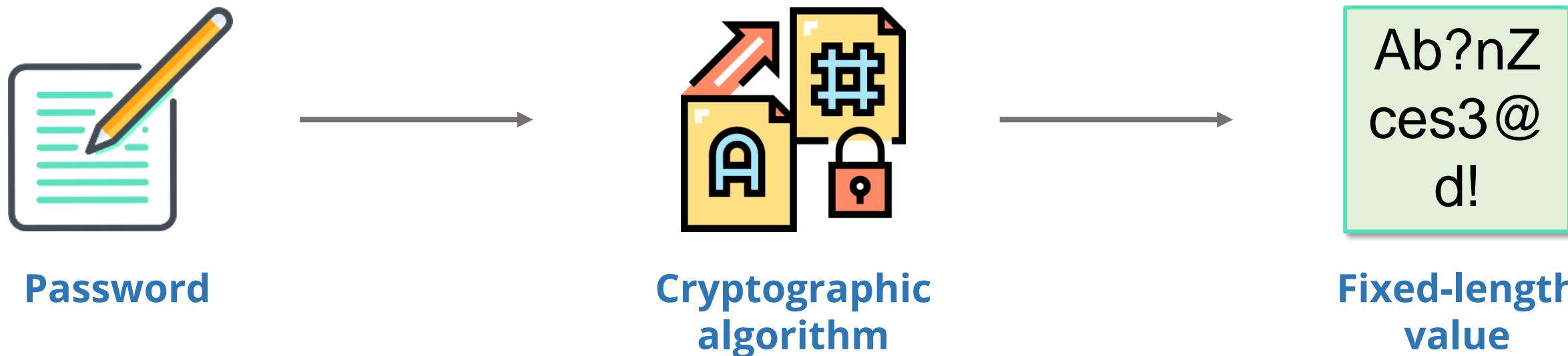
Each file (photos, notes, etc.) is encrypted individually using separate keys. Apple iOS uses FBE for data encryption on iPhones.



Popular FBE software -
eCryptfs

Storing Passwords

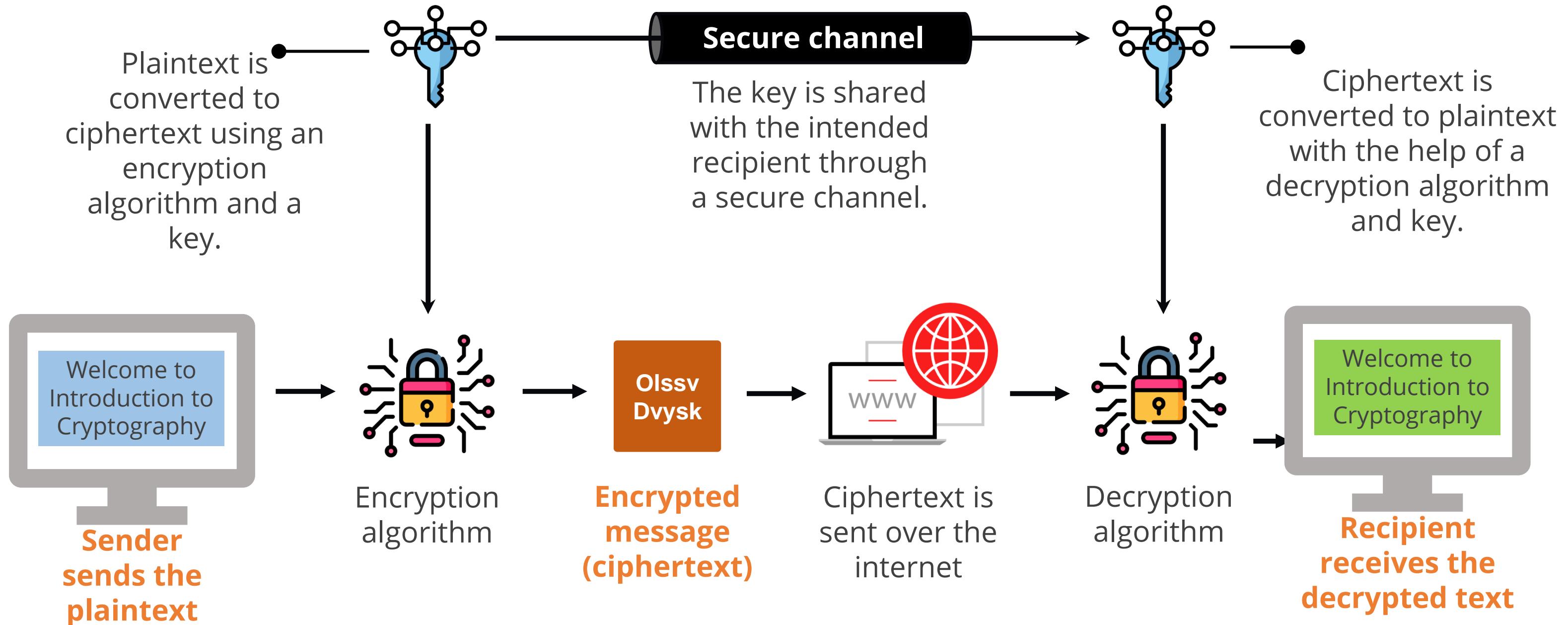
- If passwords are stored in the form of plain text in a database, the admin or an attacker can access your password and use it for malicious intent.
- For this reason, passwords are mapped to a **fixed-length value** (hash) by a cryptographic relationship.
- A system will take the password on login, convert it to a fixed value, and compare this value to existing ones in the database for successful authentication.
- It is nearly impossible to decrypt this stored hash value to retrieve the original plaintext password.



TECHNOLOGY

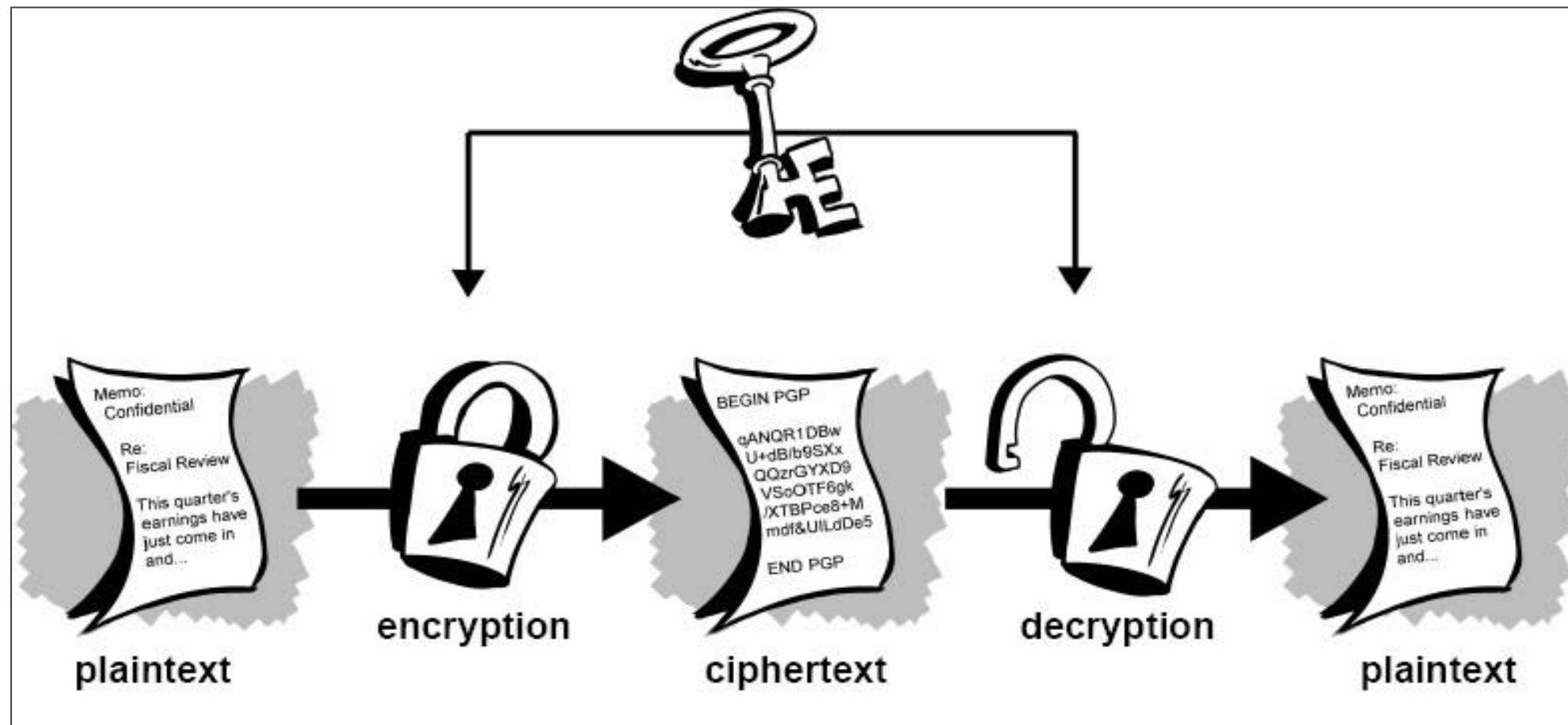
Cryptography Fundamentals

Cryptography Methodology



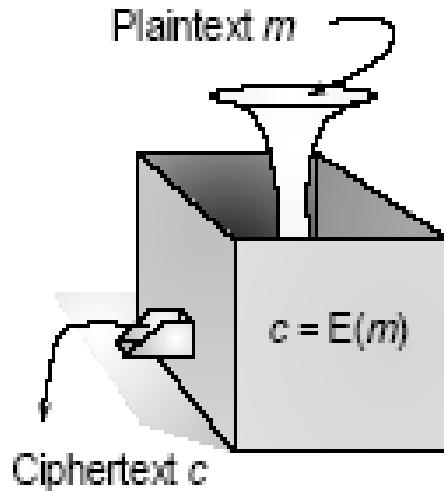
Conventional Encryption

Conventional encryption is illustrated below:



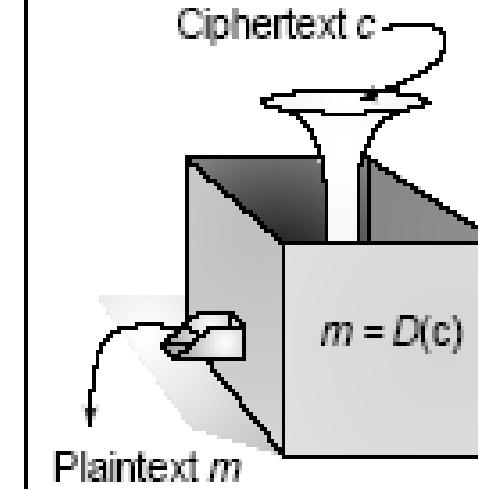
Encryption and Decryption

Encryption



The conversion of a original message, referred to as *plaintext* or *cleartext*, into a different message known as *ciphertext* (the word cipher comes from an old Arabic word meaning empty or zero), or *cryptogram*.

Decryption



The extraction process by which the intended receiver extracts the plaintext from the ciphertext

Encryption is converting plaintext into cipher text with the help of key and algorithm. Cipher text is something that is in an unreadable format.

Decryption is the process of converting ciphertext into plaintext using a key and algorithm. Ciphertext is the encrypted form of data that needs to be converted back into readable plaintext.

Cryptographic Key

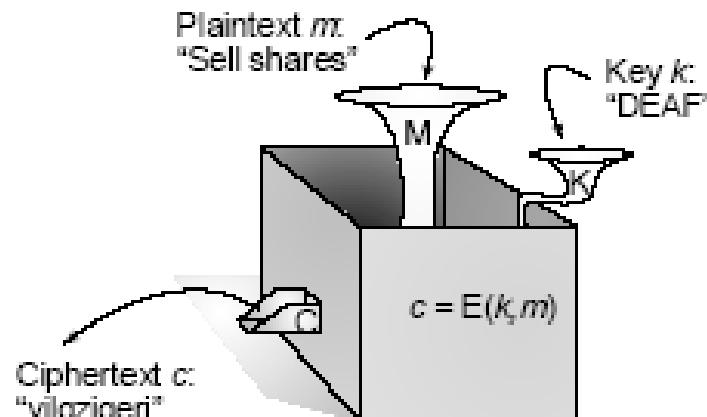
A **key** is a piece of information that determines the functional output of a cryptographic algorithm.

Key clustering is when two different keys generate the same ciphertext from the same plaintext using the same algorithm.

Keyspace is a range of possible values used to construct keys.

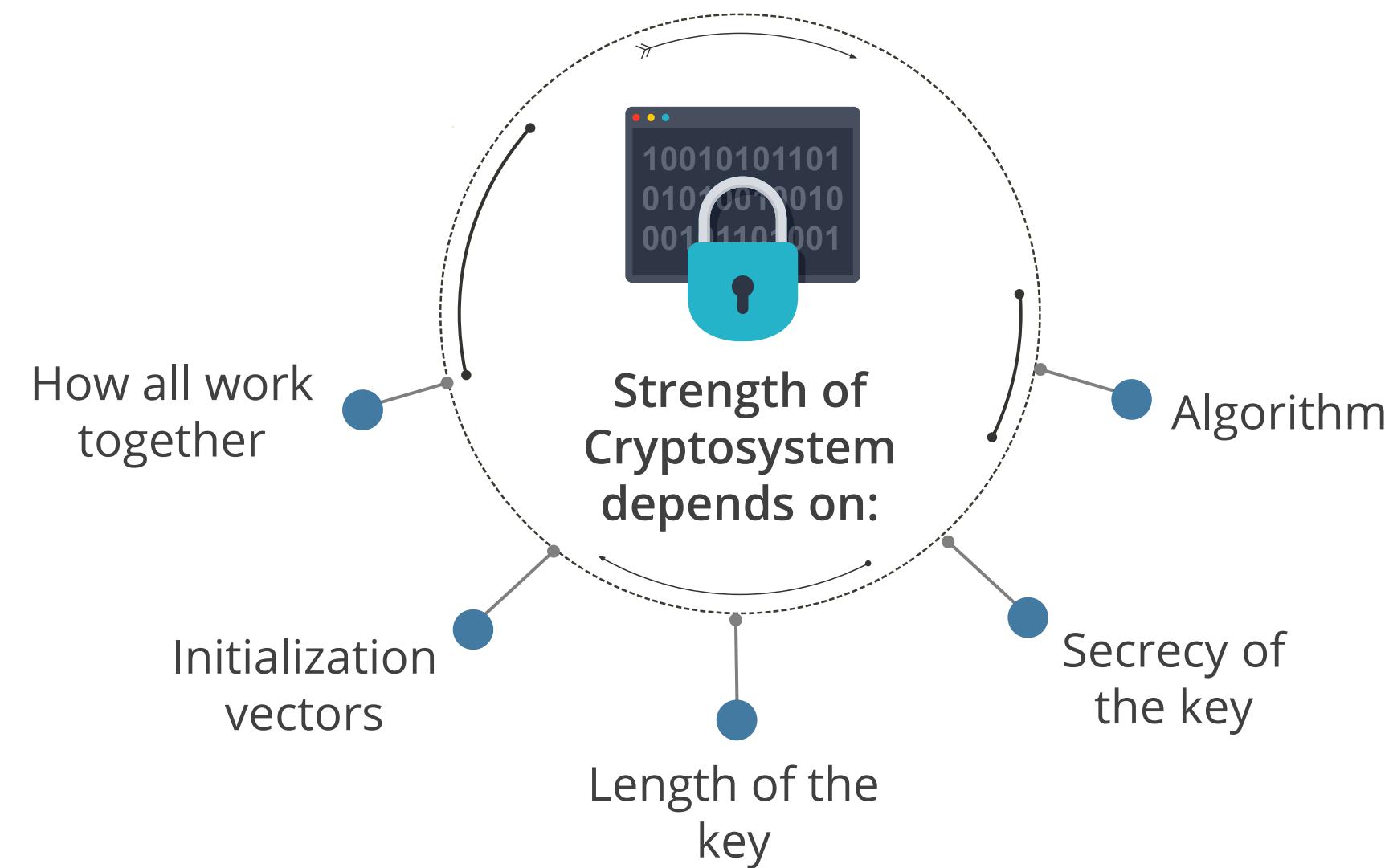
Cryptographic key

P A sequence of letters, symbols or numbers rather like a password.



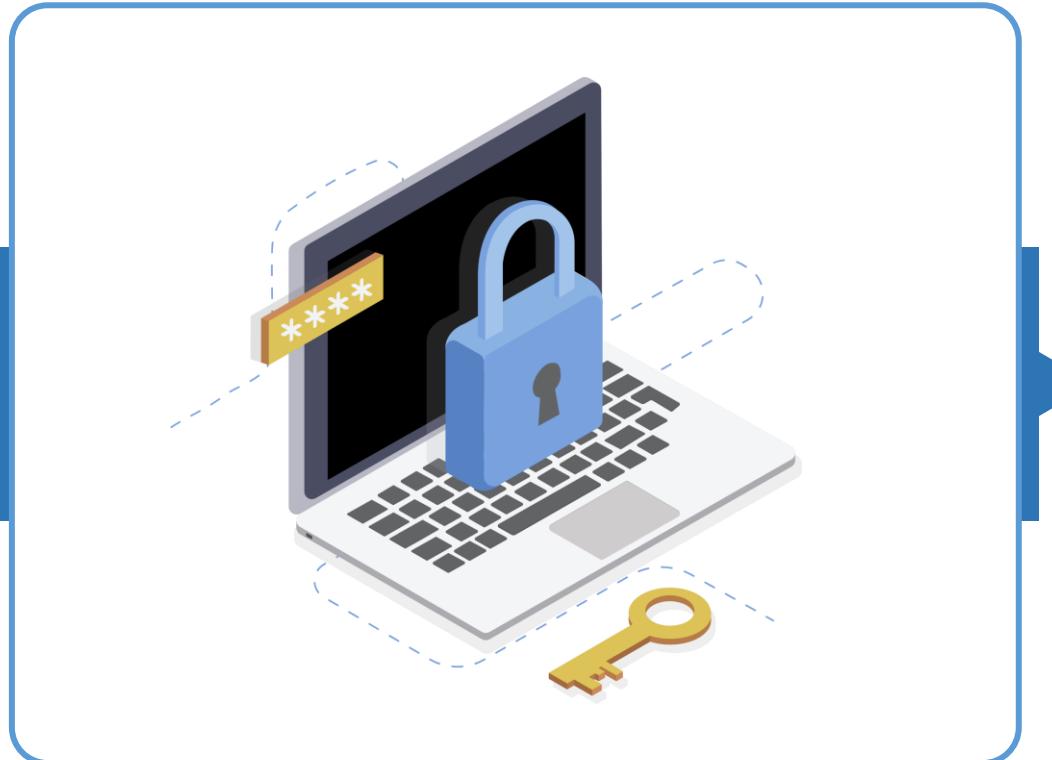
Strength of Cryptosystem

The strength of a cryptosystem refers to its ability to resist various attacks and keep the information it protects confidential, authentic, and tamper-proof. Key factors that determine the strength of a cryptosystem include:



Strength of Cryptosystem

Work factor is an estimate of the effort and resources it would take an attacker to penetrate a cryptosystem.



- A good cryptosystem should be cost-efficient and less time-consuming.
- A brute force attack is used to break a cryptosystem.

Cryptosystem Elements

- Use an algorithm without known flaws
- Use a large key size
- Use all possible values within the key space as randomly as possible
- Protect the actual key



Cryptosystem Services

Cryptosystem services ensure:

Confidentiality



Renders the information unintelligible except by authorized entities

Integrity



Ensures the data has not been altered in an unauthorized manner since it was created, transmitted, or stored

Authentication



Verifies the identity of the user or the system that created the information

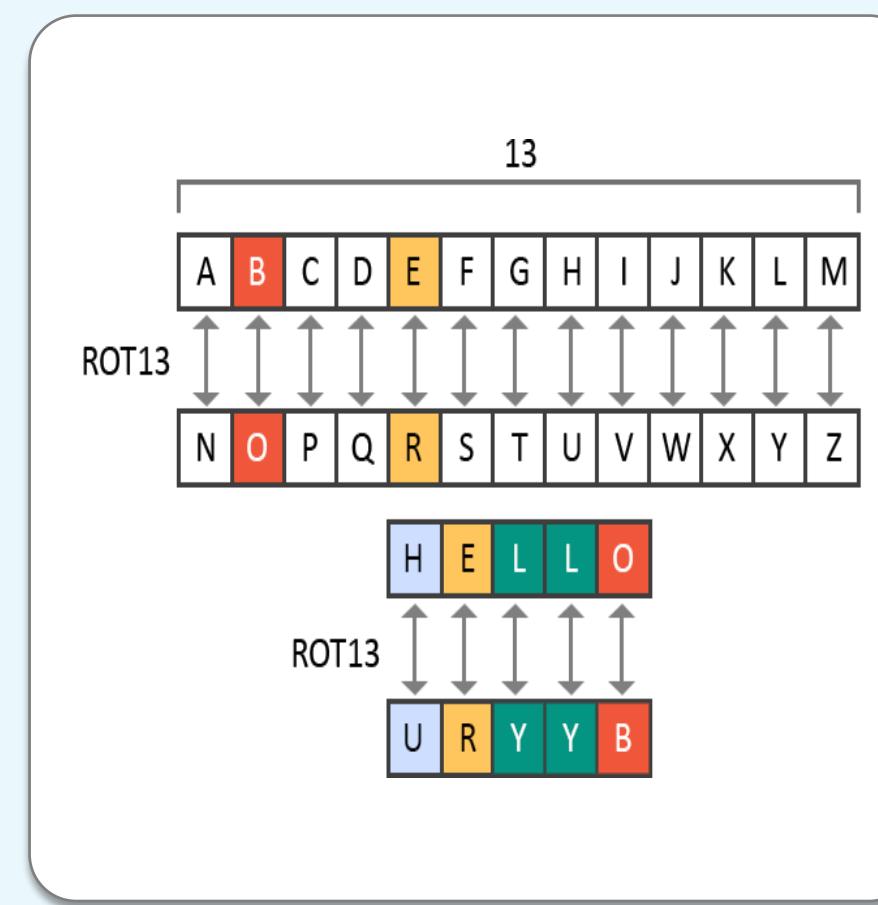
Non-repudiation



Ensures that the sender cannot deny sending the message

Cryptography Methods: Substitution Cipher

- It works by substituting one letter for another letter based on a key.
- Example: Caesar cipher or ROT13, in which the alphabet is rotated by 13 steps
- The message **HELLO** becomes **URYYB** after the ROT13 substitution.
- Substitution Cipher is generally used on blogs to filter certain words and in combination with other ciphers.



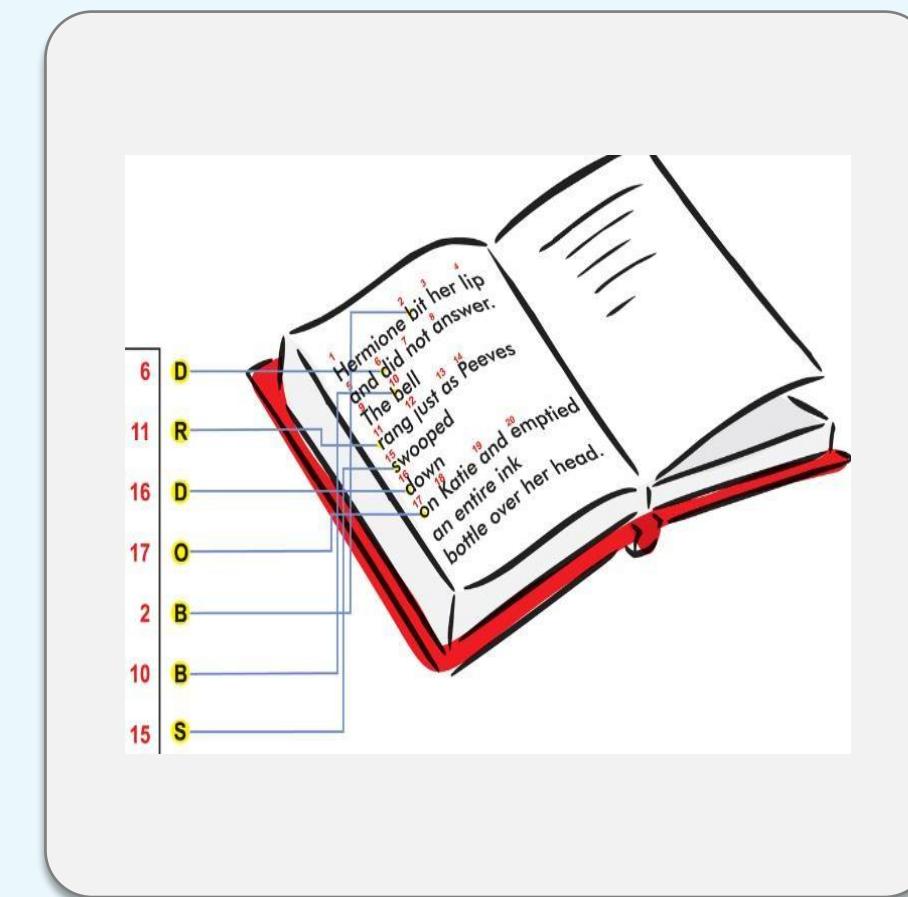
Cryptography Methods: Transposition Cipher

- Transposes the original text with long sequences of complex substitutions and permutations
- Uses a key to determine the positions the characters are moved to
- Is used in combination with substitution cipher in standard ciphers

S	E	C	U	R	I	T	Y
E	S	U	C	I	R	Y	T

Cryptography Methods: Running Key Cipher

- It could use a key that does not require an electronic algorithm and bit alterations but cleverly uses components in the physical world around you.
- For instance, the algorithm could be a set of books agreed upon by the sender and receiver. The key in this type of cipher could be a book page, line number, or column count.



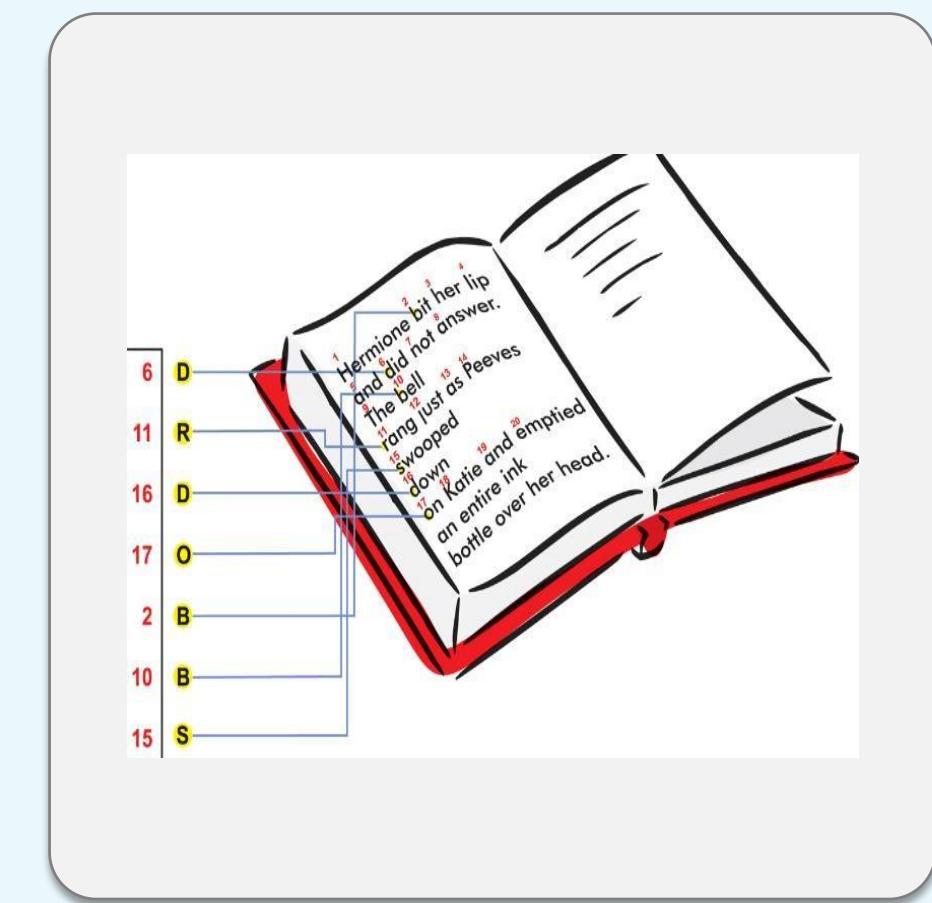
Cryptography Methods: Running Key Cipher

- For example, you get a message from your super-secret spy buddy, and the message reads **CRYPTOGRAPHY 149l6c7.299l3c7.911l5c8.**
- This could mean for you to look at the 1st book in your predetermined series of books, the 49th page, the 6th line down the page, and the 7th column.



Cryptography Methods: Concealment or Null Cipher

- A concealment cipher is a message within a message. If your super-secret spy buddy and you decide the key value is every third word, then when you get a message from him, you will pick out every third word and write it down.
- Example: Suppose he sends you a message that reads, **The saying, The time is right is not cow language, so is now a dead subject**
- Because your key is every third word, you produce **The right cow is dead**



XOR Function

XOR function returns a true value when only one of the input values is true.

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

If both values are false or both values are true, the output of the XOR function is false.

MOD Function

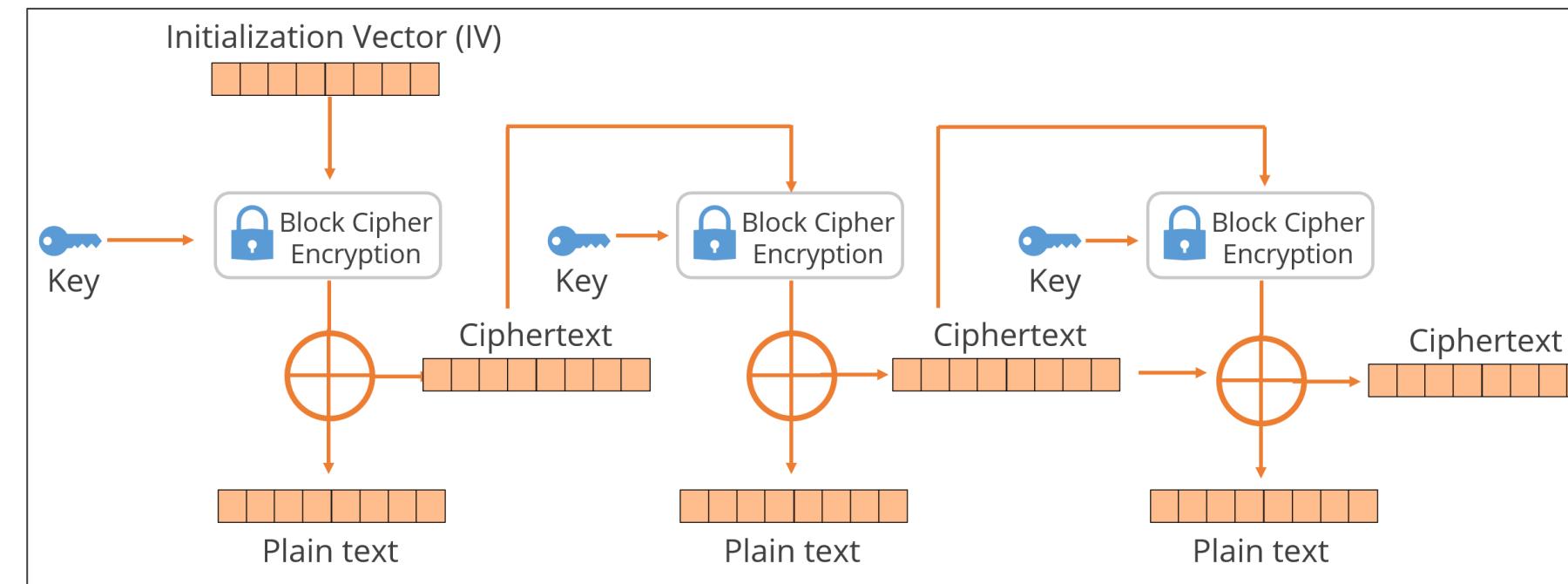
The modulo function is quite simply the remainder value after a division operation is performed.

Number	Divisor	MOD Function
15	4	3
10	2	0
7	3	1
90	10	0
77	8	5

The modulo function is just as important to cryptography as logical operations.

Initialization Vector (IV)

- Random values are used with algorithms to ensure patterns are not created during the encryption process.
- They are used with keys and need to be encrypted when being sent to the destination.
- If IVs are not used, then two identical plaintext values encrypted with the same key will create the same ciphertext.
- The IV and the key are both used by the algorithm to provide more randomness to the encryption process.



TECHNOLOGY

Steganography

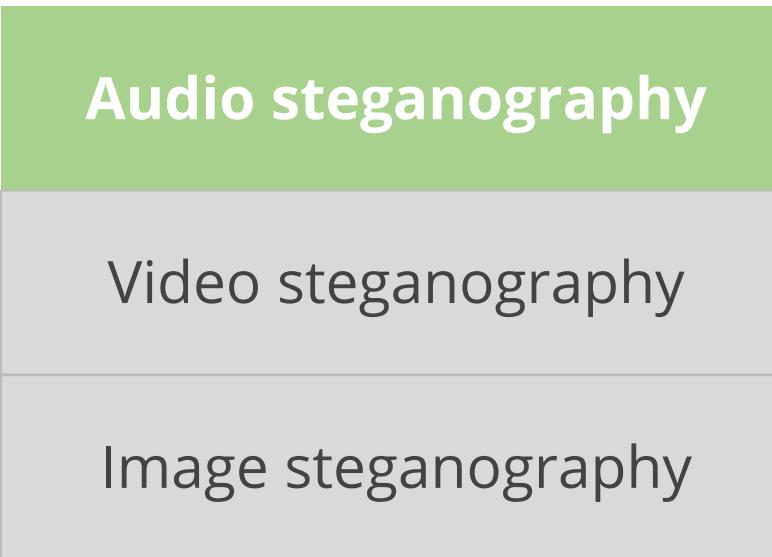
Steganography

Steganography is the art of hiding the existence of a message.

- It is used to insert digital watermarks on images to identify illegal copies.
- It is used to send secret messages through emails.
- It involves concealing the very existence of data by hiding it in other media such as picture, audio, and video files.

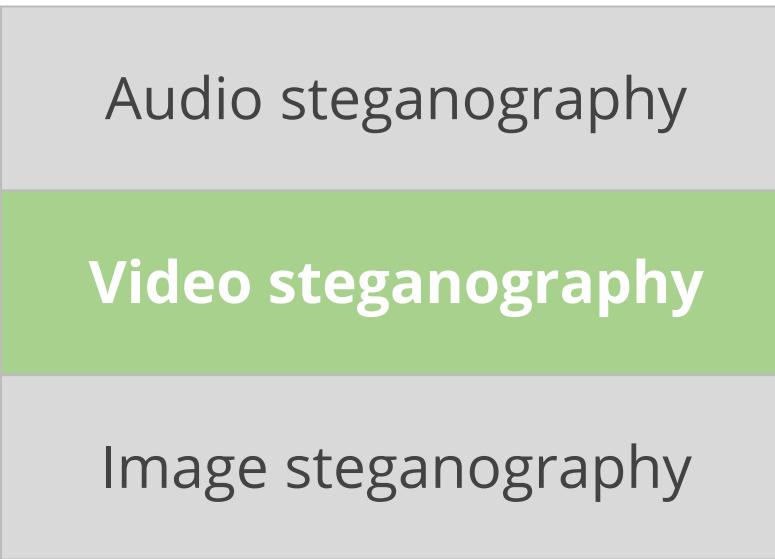


Types of Steganography



Audio steganography involves hiding secret information within an audio signal without altering its quality.

Types of Steganography



Video steganography hides files within a cover video file. It's more secure than other methods due to video size and complexity. Frames are used to store data using the Least Significant Bit (LSB) steganography method.

Types of Steganography

Audio steganography

Video steganography

Image steganography

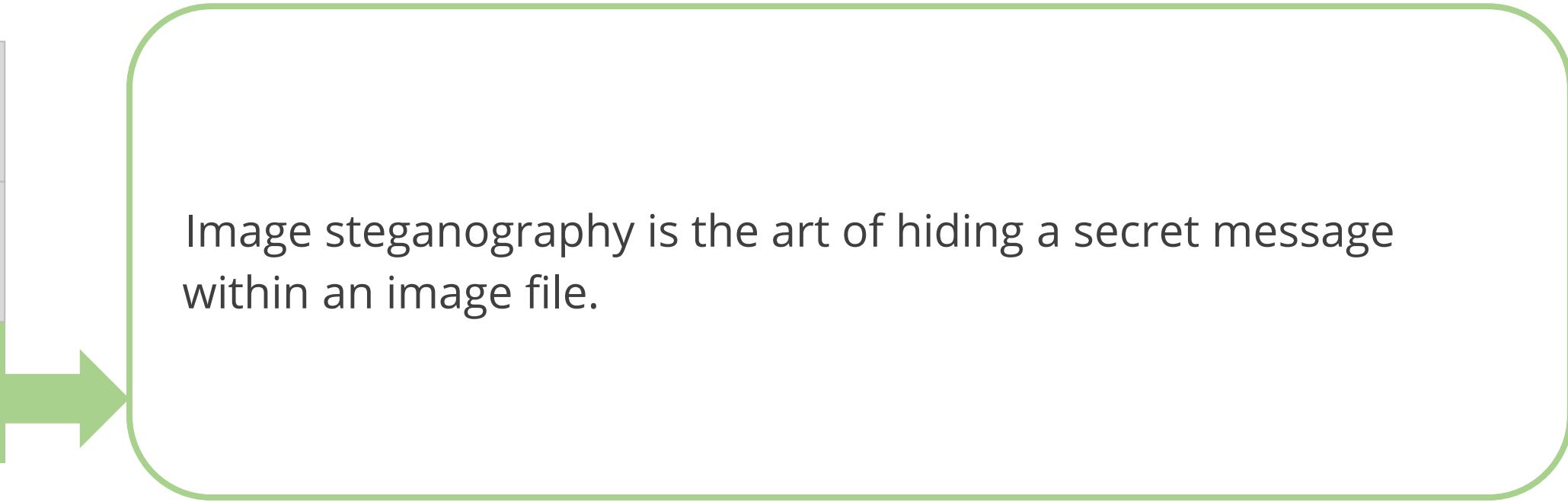


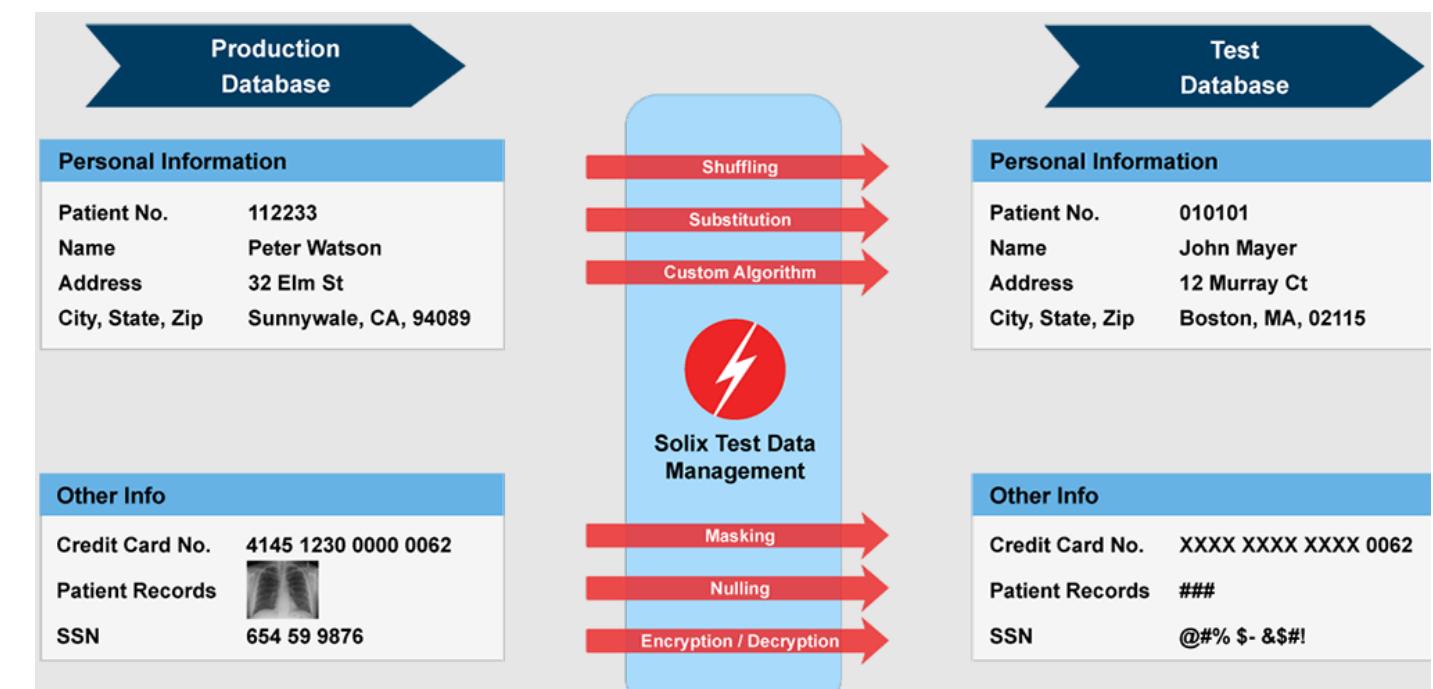
Image steganography is the art of hiding a secret message within an image file.

Masking, Obfuscation, and Tokenization

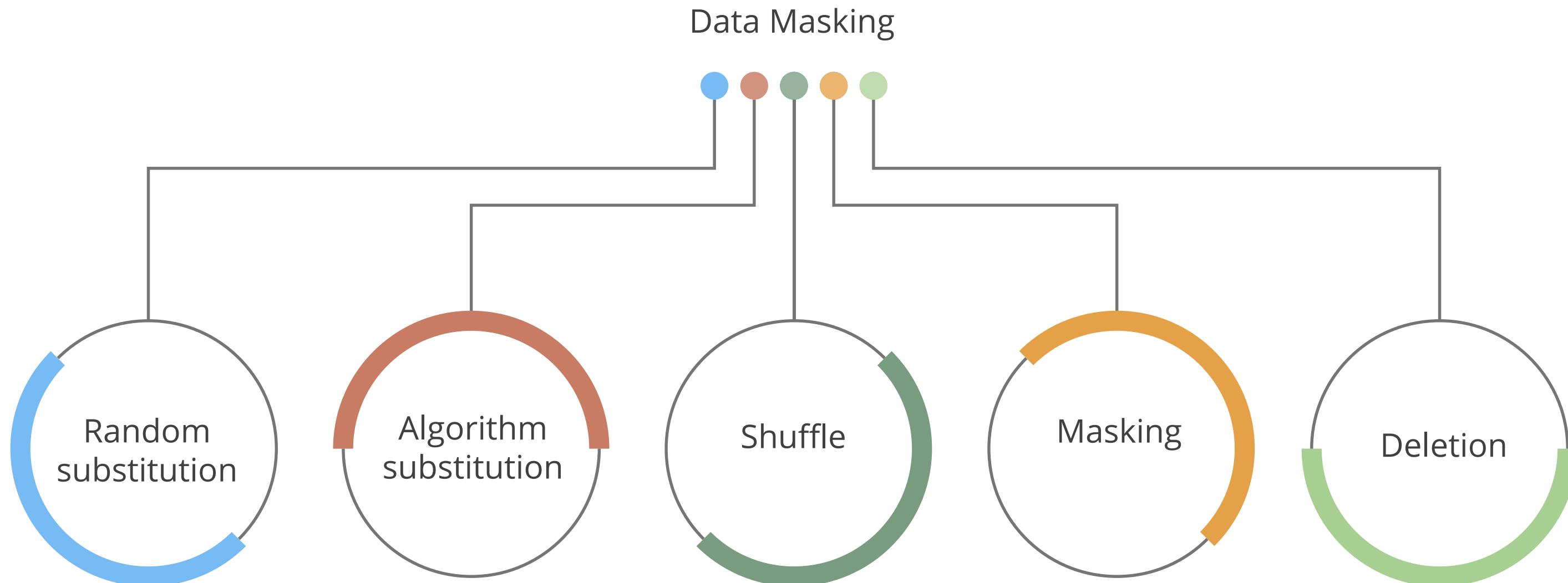
Data Masking or Obfuscation

Data masking

- Data masking or obfuscation is the process of hiding, replacing, or omitting sensitive information from a specific data set.
- Data masking is typically used to protect specific data sets such as PII or commercially sensitive data or to comply with certain regulations such as HIPAA or PCI DSS.
- Data masking or obfuscation is also widely used for test platforms where suitable test data is unavailable.
- Both techniques are typically applied when migrating tests or development environments to the cloud or when protecting production environments from threats such as data exposure by insiders or outsiders.



Data Masking Methods



Data Masking Methods

Random substitution

The value is replaced (or appended) with a random value.

Algorithm substitution

The idea of replacing (or appending) the value with an algorithm-generated value is called algorithmic substitution.

Shuffle

This shuffles different values from the data set. It is usually from the same column.

Data Masking Methods

Masking

This uses specific characters to hide certain parts of the data. It usually applies to credit card data formats: XXXX XXXX XX65 5432.

Deletion

This simply uses a null value or deletes the data.

Types of Data Masking

Static data masking

- Static data masking (SDM) permanently replaces sensitive data by altering data at rest within database copies.
- Static Data Masking is designed to help organizations create a sanitized copy of their databases where all sensitive information has been altered in a way that makes the copy sharable with non-production users.
- In static masking, a new copy of the data is created with the masked values.
- Static masking is typically efficient when creating clean non-production environments.

Types of Data Masking

Dynamic data masking

- Dynamic data masking (DDM) aims to replace sensitive data in transit, leaving the original at-rest data intact and unaltered.
- Dynamic masking, sometimes referred to as on-the-fly masking, adds a layer of masking between the application and the database.
- This type of masking is efficient when protecting production environments.
- It can hide the full credit card number from customer service representatives, but the data remains available for processing.

Protecting Privacy: Pseudonymization

Pseudonymization

- It refers to the process of using pseudonyms to represent other data.
- This approach prevents direct identification of an entity, such as a person.
- For instance, in a medical record held by a doctor's office, instead of including personal information, the patient could be referred to as **Patient 23456**. The doctor's office would retain the personal information in a separate database linked to the patient's pseudonym.

Name	Token/Pseudonym	Anonymized
Clyde	qOerd	Xxxxx
Marco	Loqfh	xxxxx
Lex	McV	Xxxxx
Les	McV	Xxxxx
Marco	Loqfh	xxxxx
Raul	BhQI	xxxxx
Clyde	qOerd	xxxxx

Protecting Privacy: Data Anonymization

Direct identifier

- This includes information that relates specifically to an individual and can be used in isolation to uniquely identify that individual.
- Examples include social security number, full name, email address, telephone number, health insurance number, medical record number, full-face photographs, or biometric records such as fingerprints.

Indirect identifier

- This includes information that can be combined with other information to identify specific individuals.
- For example, a combination of gender, date of birth, geographic indicators, and other descriptors can be used to identify specific individuals.

Data anonymization

- Anonymization removes indirect identifiers to prevent data analysis tools or other intelligent mechanisms from collating or pulling data from multiple sources to identify sensitive information.

Example : Anonymization

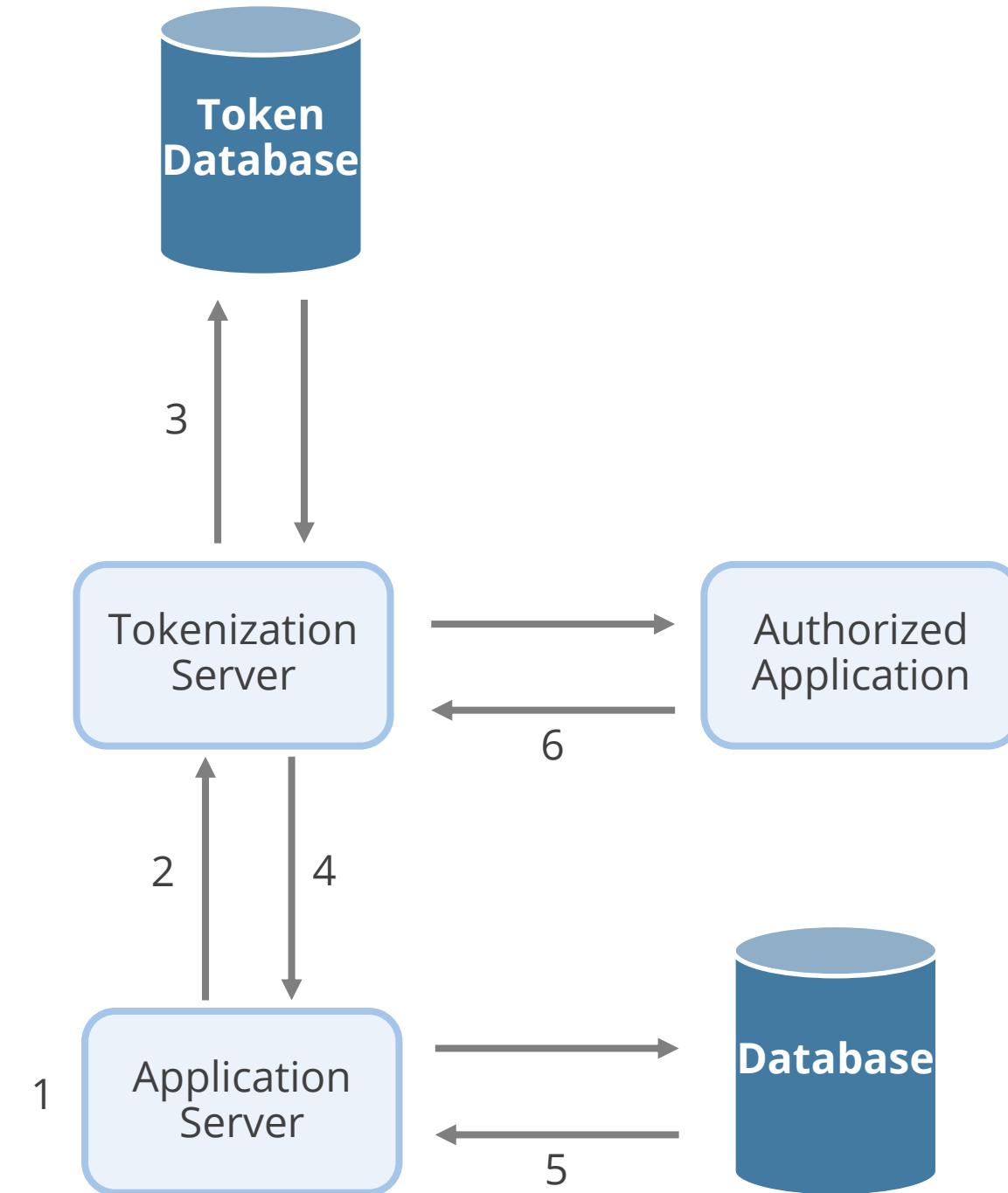
Example

- Let's take an example of a person.
- **Direct Identifier:** Adhaar card, Phone number, Credit card
- **Indirect Identifier:** Place of birth, Company name, Designation
- In today's world, even if you don't have information about direct identifiers but a bunch of indirect identifiers, you can find information about a person using modernized tools.

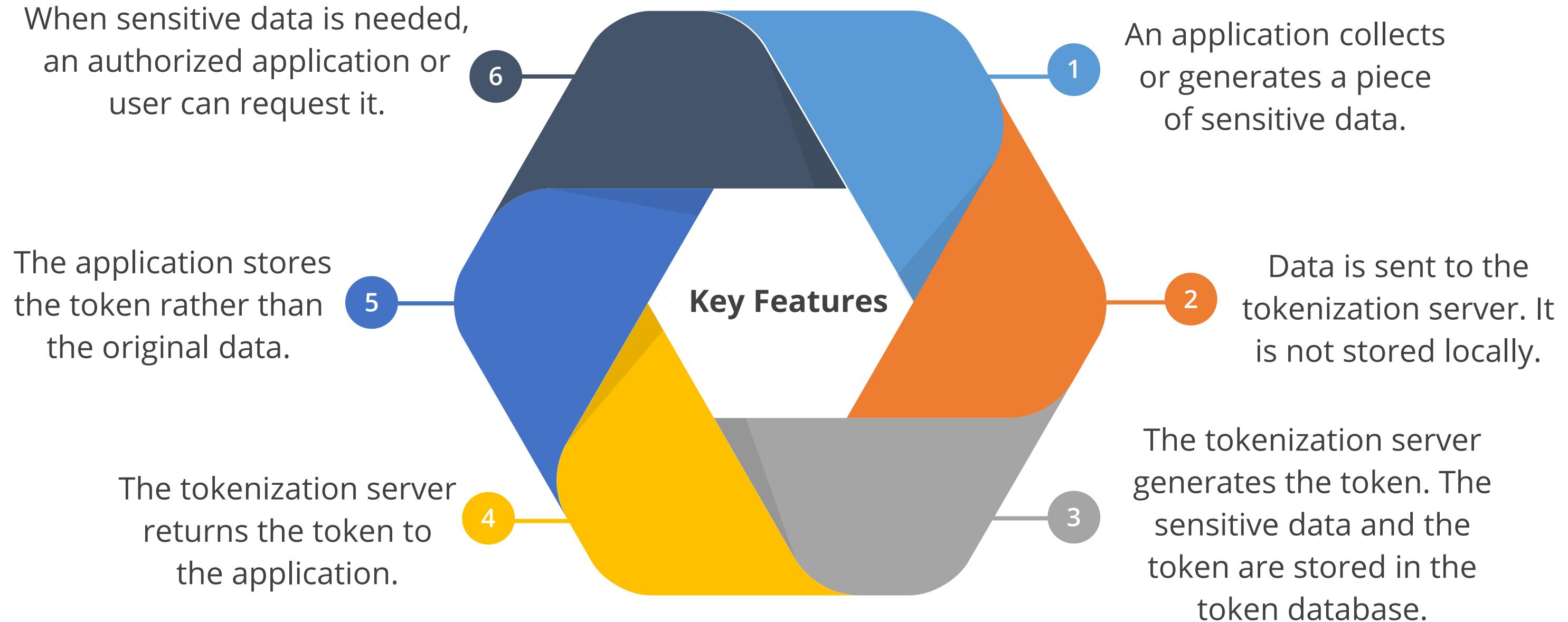
Protecting Privacy: Tokenization

Tokenization

- It is the process of substituting a sensitive data element with a non-sensitive equivalent known as a token.
- Tokenization is a technology that:
 - Replaces the original data with non-sensitive placeholders
 - Is used to safeguard sensitive data in a secure, protected, and regulated environment



Protecting Privacy: Tokenization



Example : Tokenization

Example

- Let's take the example of Netflix, which collects credit cards from customers.
- Netflix uses tokenization to secure credit card information.
- The credit card details are sent to a tokenization database and replaced with a token.
- Netflix stores the token instead of the actual credit card information.
- When needed, Netflix uses the token to retrieve the credit card information from the tokenization database.

Symmetric and Asymmetric Cryptography

Encryption Methods

Symmetric key algorithm

- A symmetric key, also known as a secret key or private key, is a fundamental element in symmetric key cryptography.
- It serves two purposes: encryption (scrambling plain text) and decryption.

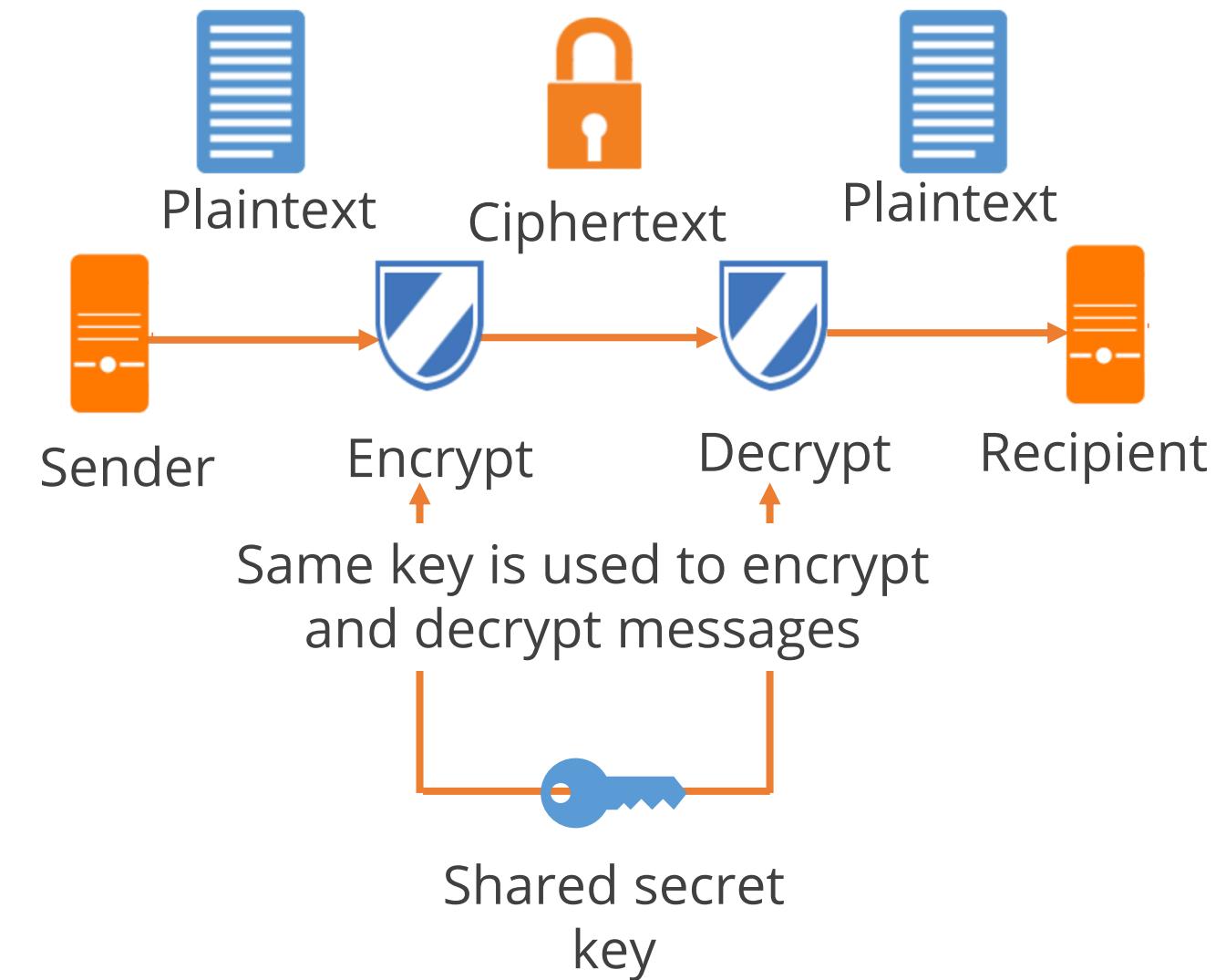


Asymmetric key algorithm

- Asymmetric key cryptography is also known as public-key cryptography.
- It uses two keys: private keys, which are private, and public keys, which can be shared.

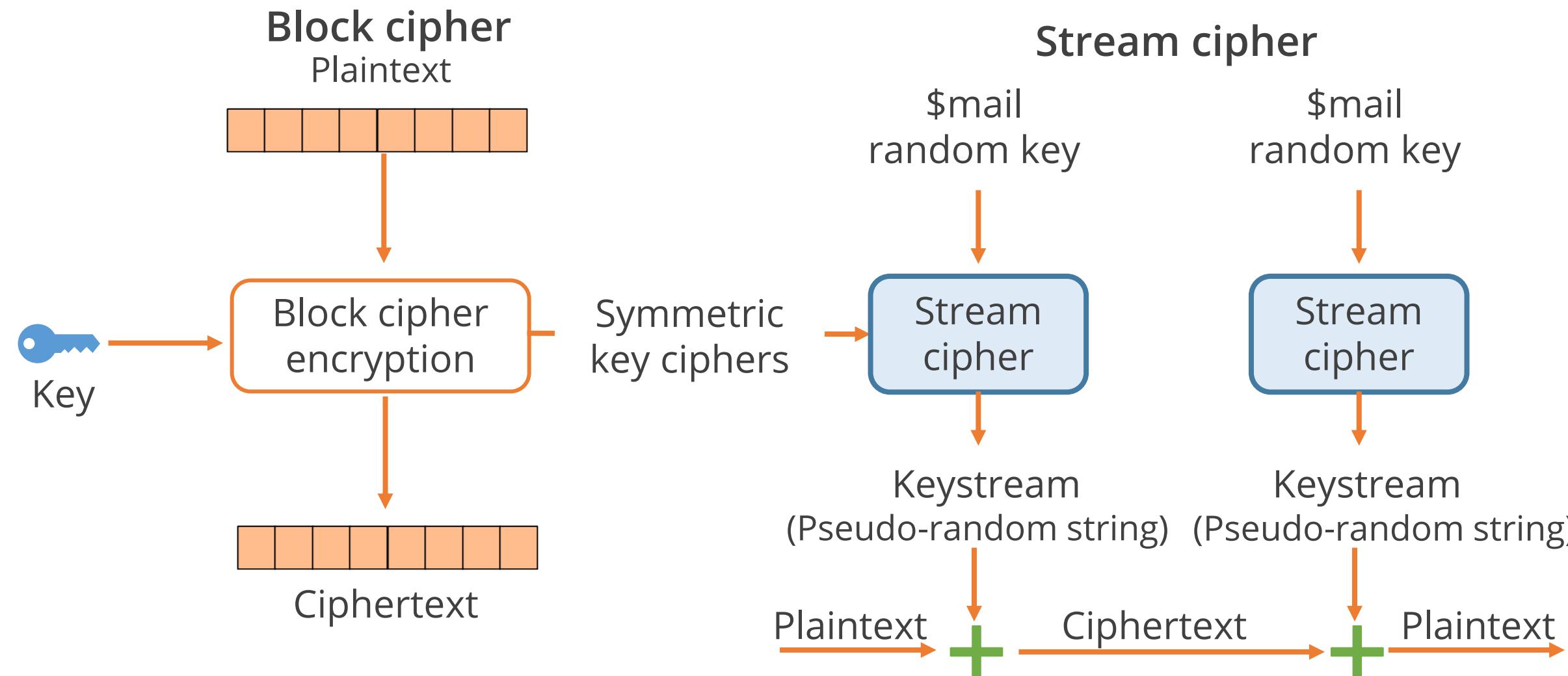
Introduction to Symmetric Cryptography

- Performs both encryption and decryption of a message using only a single cryptographic key
- Requires each pair of communicating users to have a copy of the key
- Provides confidentiality because of the same key, but not authenticity or non-repudiation
- Utilizes secret messages where confidentiality is the main criterion
- Applies to wired and wireless networks
- Involves $n(n-1)/2$ keys for secure communication
- Demands keys to be securely shared between communicating parties
- Includes examples such as Blowfish, AES, IDEA, RC4, RC5, RC6, DES, and 3DES



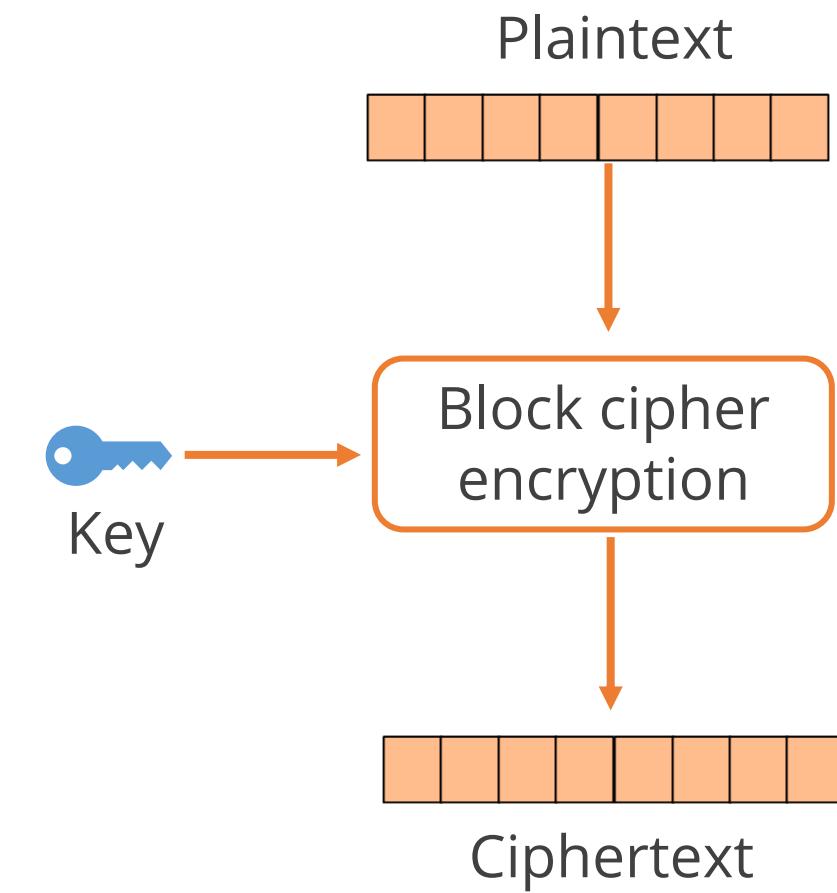
Symmetric Key Ciphers

The two primary types of symmetric key ciphers are:



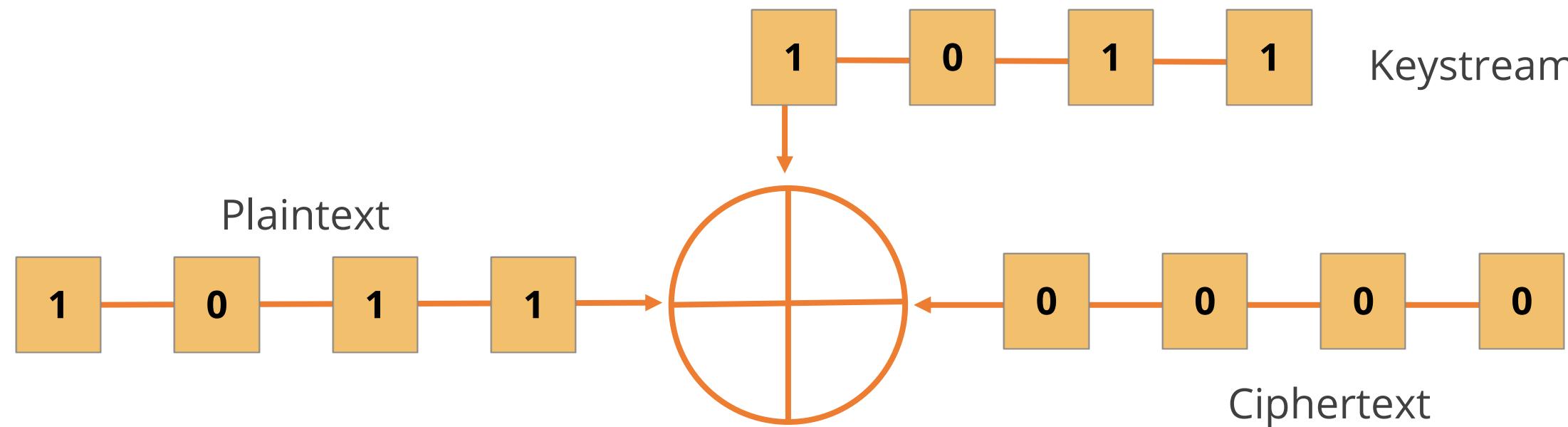
Block Cipher

- Converts a fixed-length block of plaintext data to a block of ciphertext data of the same length
- Operates on preset blocks (64, 128, 192 bits, etc.)
- Uses a combination of substitution and transposition
- Is more expensive and computationally more exhaustive, although stronger than stream-based ciphers
- Is mainly implemented in software
- Is used in ciphers like DES and AES



Stream Cipher

- A stream of ciphertext data is generated by combining the keystream (sequence of bits) with plaintext data bit by bit using XOR operations.
- The keystream must have a non-repeating pattern of bits to ensure security.
- Stream ciphers are mainly implemented in hardware.
- They are most commonly used in voice or video communications.



Stream Cipher vs. Block Cipher

Stream cipher

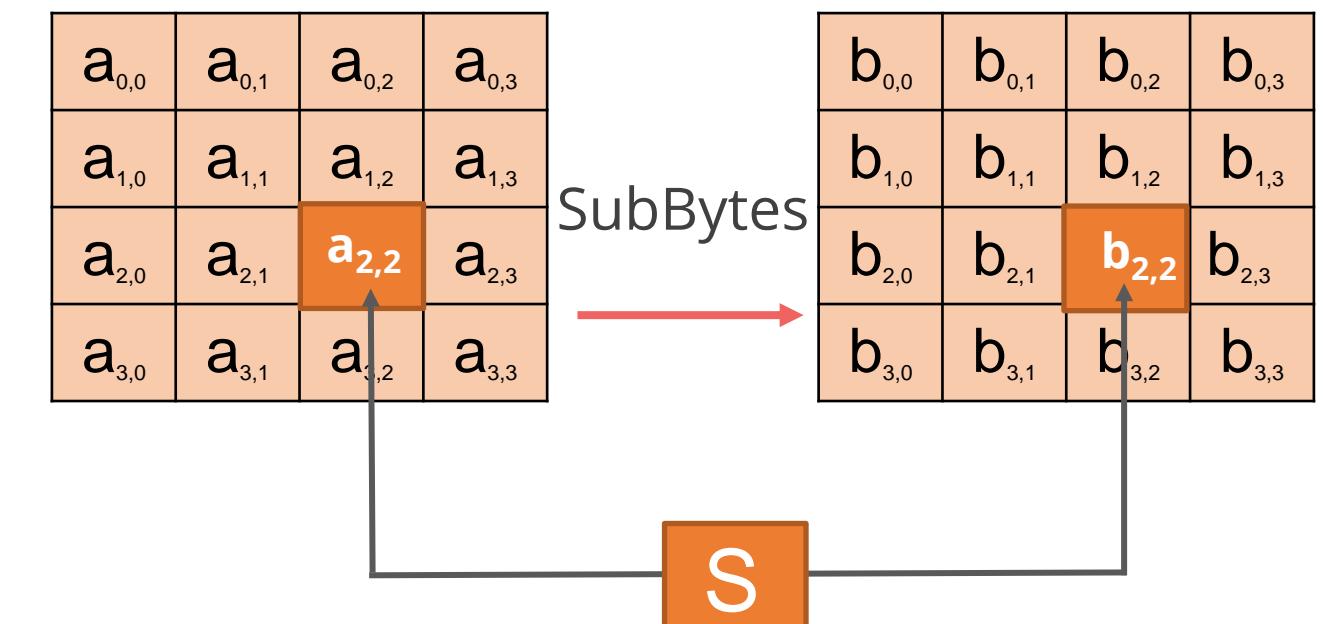
- Faster than block cipher
- Processes the input element continuously producing output, one element at a time
- Requires less code
- With steam cipher, keys can be used only once
- Application: SSL (Secure connection on the Web)
- Easier to implement in hardware

Block cipher

- Operates on a larger block of data
- Slower than stream cipher
- Processes one block at a time, producing output for each input block
- Requires more code
- Reuse of key is possible
- Example: DES encryption
- Application: Database, file encryption
- Easier to implement in software

Advanced Encryption Standard (AES)

- Advanced Encryption Standard (AES) is a symmetric block cipher.
- AES is the current U.S. standard.
- For encryption, it uses:
 - 128-bit keys (10 rounds of encryption)
 - 192-bit keys (12 rounds of encryption)
 - 256-bit keys (14 rounds of encryption)
- AES uses the Rijndael algorithm with variable block sizes (128, 192, and 256-bit) and key lengths (128, 192, and 256-bit).



Other Symmetric Systems

IDEA

- Stands for International Data Encryption Algorithm
- Uses 64-bit blocks, a 128-bit key, and 8 rounds of computations
- Used in e-mail encryption software, pretty good privacy (PGP)

Blowfish

- Uses a 64-bit block size
 - 32 – 448 bits (in steps of 8 bits) key size and 16 rounds of computation
- Optimized for 32-bit microprocessors

Twofish

- Is a modification of Blowfish using 128-bit blocks
- Uses variable key lengths up to 256 bits

Other Symmetric Systems

RC5

- Uses block sizes of 32, 64, or 128 bits, with a key length of up to 2040 bits
- Created as a candidate algorithm for AES

RC6

- Uses key sizes of 128, 192, and 256 bits and has a block size of 128 bits
- Based on RC5, and is also a candidate for AES

Symmetric Keys: Round Up

Algorithm	Block Size	Key Length	Comments
DES	64 bit	56 bit + 8-bit parity	16 rounds of processing
2DES	64 bit	112 bit	Compromised by meet-in-the-middle attack
3DES	64 bit	168 bit	
Rijndael	128,192,256 bits	128,192,256 bits	Performs variable rounds of operation
IDEA	64 bit	128 bit	<ul style="list-style-type: none">• 8 rounds transposition and substitution• Used in PGP
CAST	64 bit	40 to 128 bits	
SAFER	64 to 128 bit	64 to 128 bit	A version used in Bluetooth
Blowfish	64 bit	Variable key size	
Twofish	128 bit	128, 192, 256 bits	
RC5	16,32,64 bits	0 to 2040 bits	
AES	128 bit	128, 192, 256 bits	

Business Scenario

Hilda Jacobs, the general manager of IT Security, assigned Kevin Butler the task of selecting a good encryption system to secure the confidentiality of the company's data. She requested a symmetric block cipher system capable of encrypting with a 128-bit encryption key.



Kevin started gathering information about the existing encryption standards. Based on the current and future requirements, he had to choose between DES, 3DES, and AES.

Question: Which encryption standard should Kevin select: the DES, 3DES, or AES?

Business Scenario

Hilda Jacobs, the general manager of IT Security, assigned Kevin Butler the task of selecting a good encryption system to secure the confidentiality of the company's data. She requested a symmetric block cipher system capable of encrypting with a 128-bit encryption key.



Kevin started gathering information about the existing encryption standards. Based on the current and the future requirements, he had to choose between DES, 3DES, and AES.

Question: Which encryption standard should Kevin select: the DES, 3DES, or AES?

Answer: With the given requirement, AES is the best choice as it supports a 128-bit key.

Introduction to Asymmetric Cryptography

In asymmetric cryptography, two keys are used that are mathematically linked but mutually exclusive. One key is for encryption, and the other is for decryption.

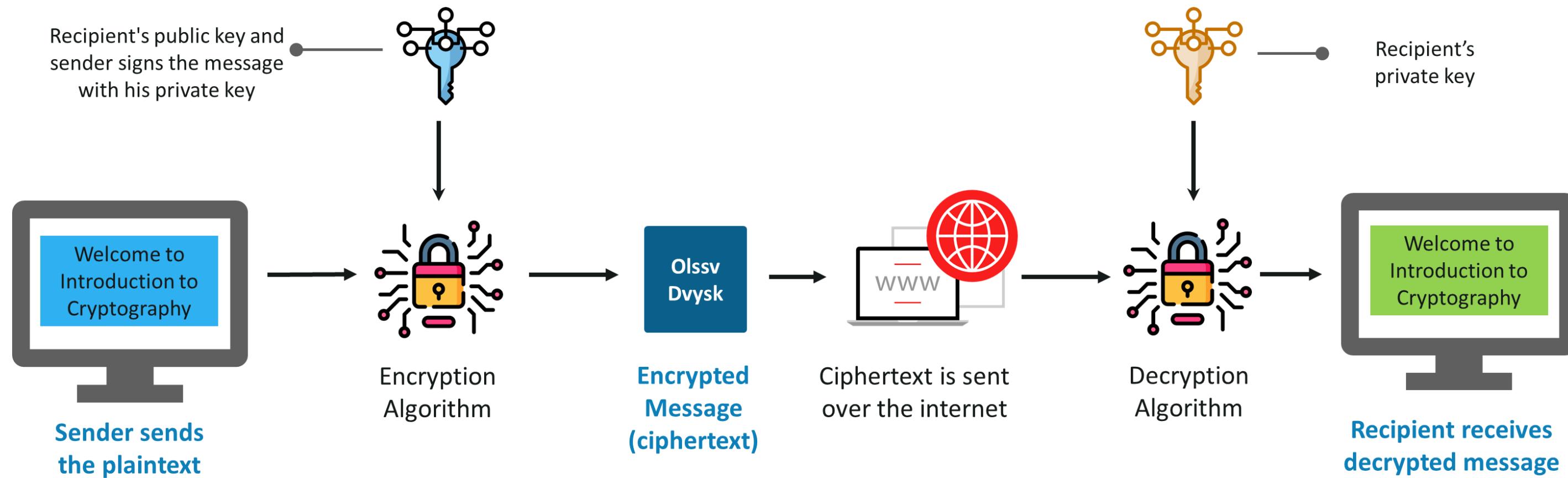


The private key can be used by an individual or entity, while the public key can be freely shared with anyone you want to communicate.

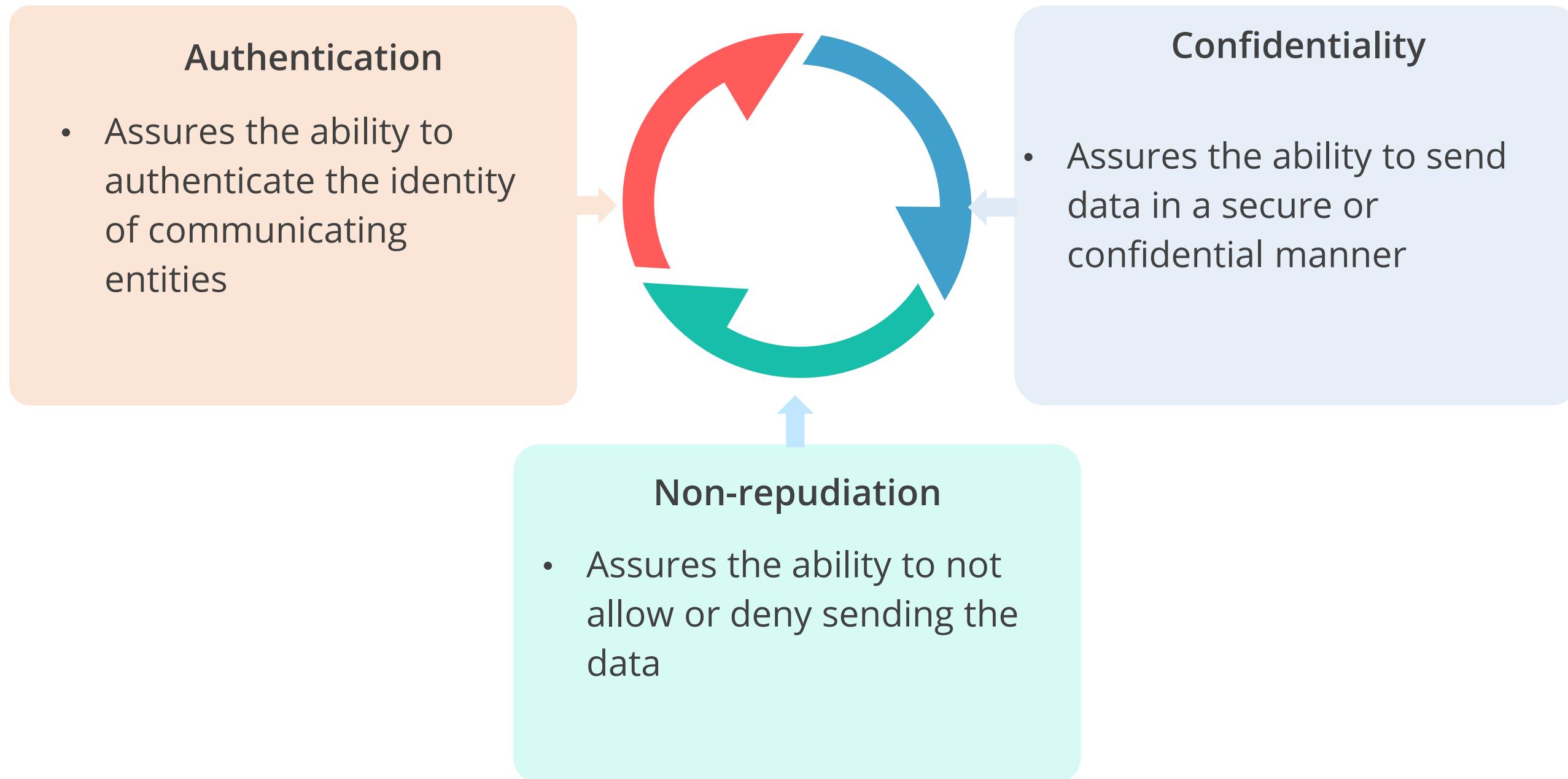
Introduction to Asymmetric Cryptography

- Asymmetric cryptography is also called public-key encryption, as one key is made public.
- A pair of keys is required for encryption or decryption.
- The keys are mathematically related.
- Each key is used to encrypt or decrypt.
- You cannot encrypt or decrypt with only one key. The public key is usually shared, while the private key is secured by the owner.
- **Secure Message format:** The message is encrypted with the receiver's public key (confidentiality).
- **Open Message format:** The message is encrypted with the sender's private key (authenticity).
 - These formats ensure authenticity, confidentiality, and non-repudiation.
 - **Examples:** RSA (Rivest-Shamir-Adleman), Diffie-Hellman, Elliptic curve cryptosystem (ECC), El Gamal, and Digital signature algorithm (DSA)

Introduction to Asymmetric Cryptography—Diagram



Goal of Asymmetric Cryptography



Asymmetric Cryptography -Pros and Cons

“

Pros

- Scalable
- Provides confidentiality, authentication, and non-repudiation
- Better key distribution mechanism

“

Cons

- Slower than symmetric key
- Mathematically complex and intensive

”

”

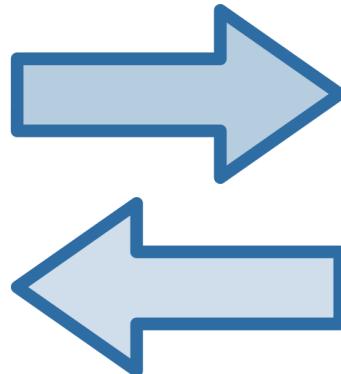
Secure Message Format

1

Charles wants to send data to Alice that should only be read by her.



Charles



Alice

Secure Message Format

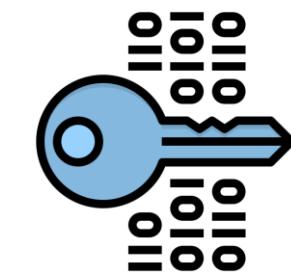
Charles generates a private and public key pair and exchanges his public key with Alice's public key.



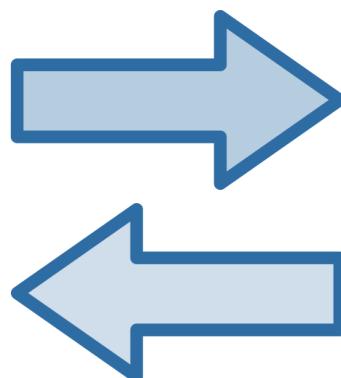
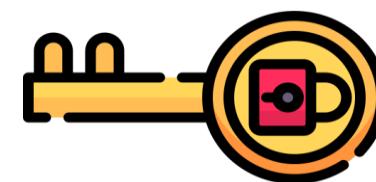
Charles

2

Alice Public Key

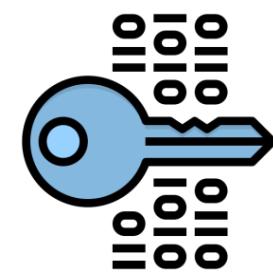


Charles Private Key

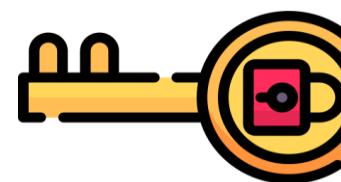


2

Charles Public Key



Alice Private Key

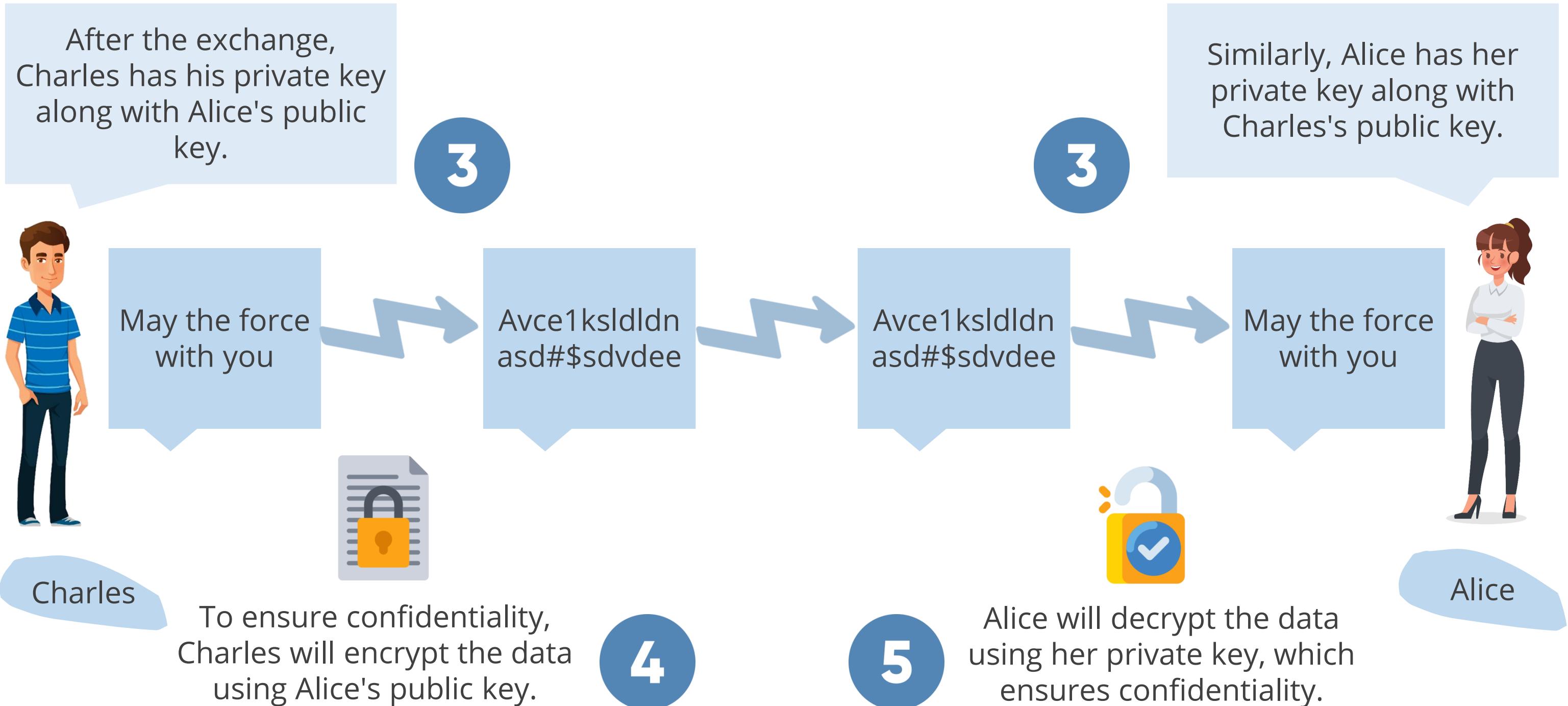


Similarly, Alice will also generate a private and public key pair and exchange her public key with Charles's public key.



Alice

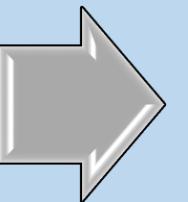
Secure Message Format



Secure Message Format- Summarized View

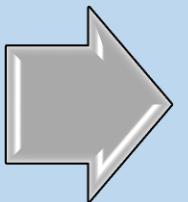
Step 1

- User A and User B want to communicate using asymmetric cryptography.



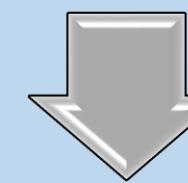
Step 2

- User A will generate a private key and a public key on their system.



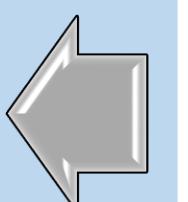
Step 3

- User B will generate a private key and a public key on their system.



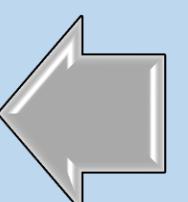
Step 6

- User B will use their private key to decrypt the data, ensuring confidentiality.



Step 5

- User A will encrypt the data using User B's public key and send it to User B.



Step 4

- User A and User B exchange each other's public keys.

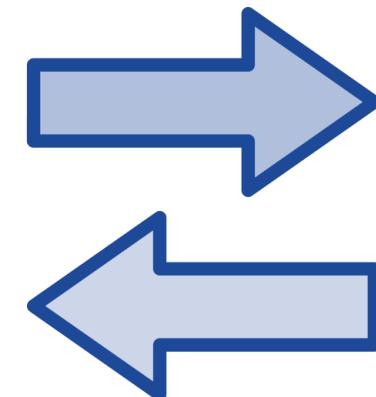
Open Message Format

1

Charles wants to send data to Alice, ensuring she can authenticate him as the sender and cannot deny receiving the message.

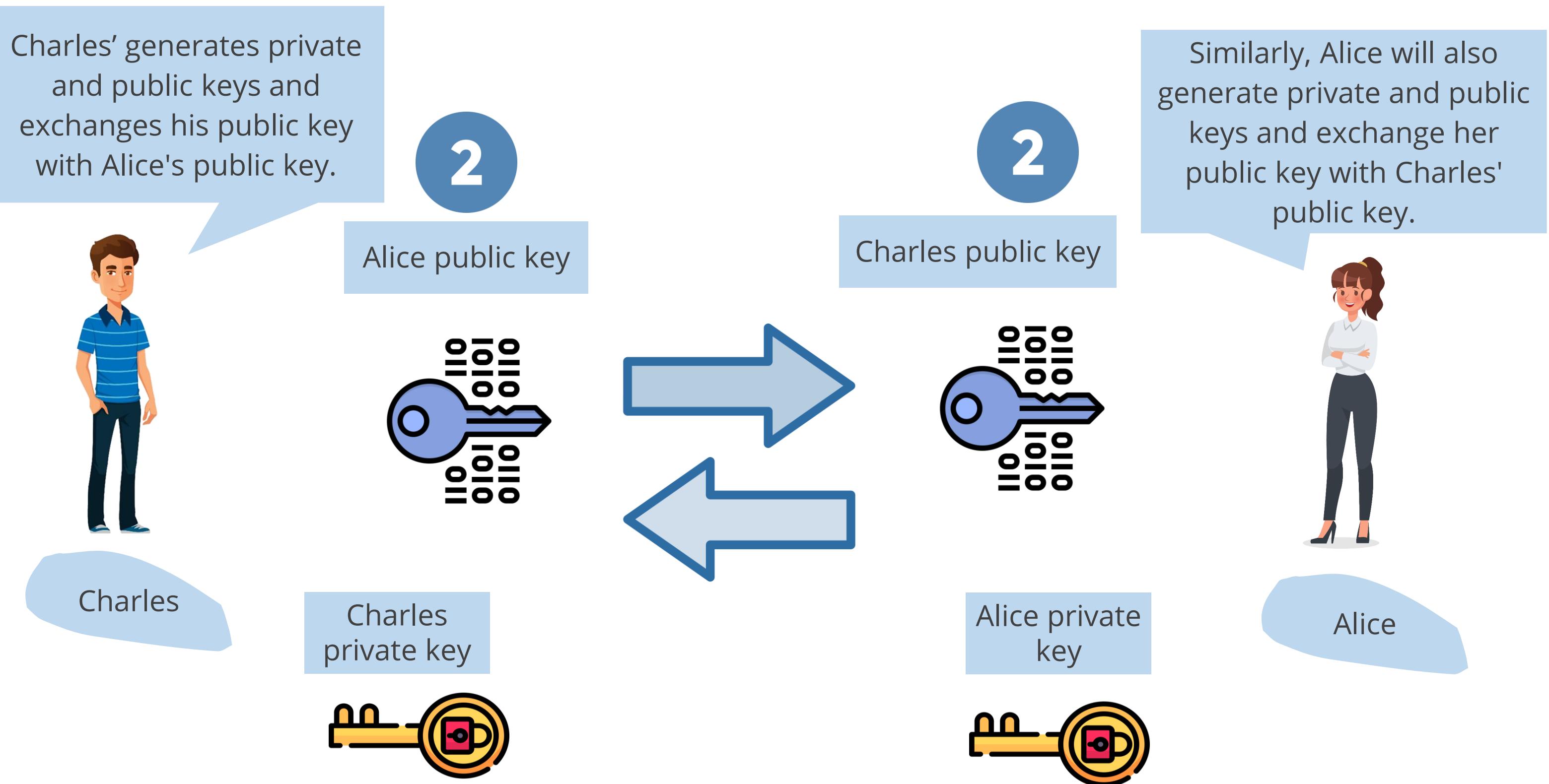


Charles

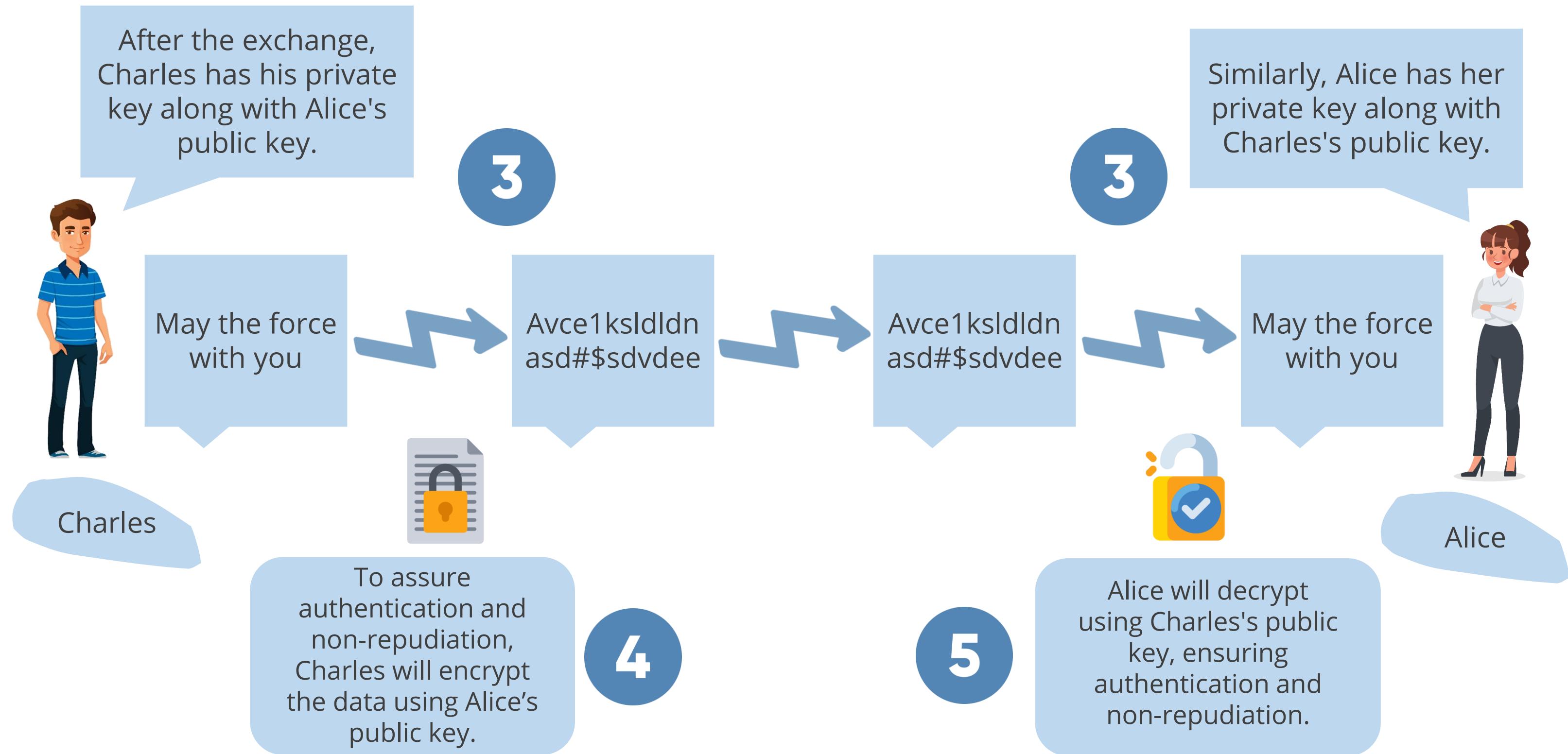


Alice

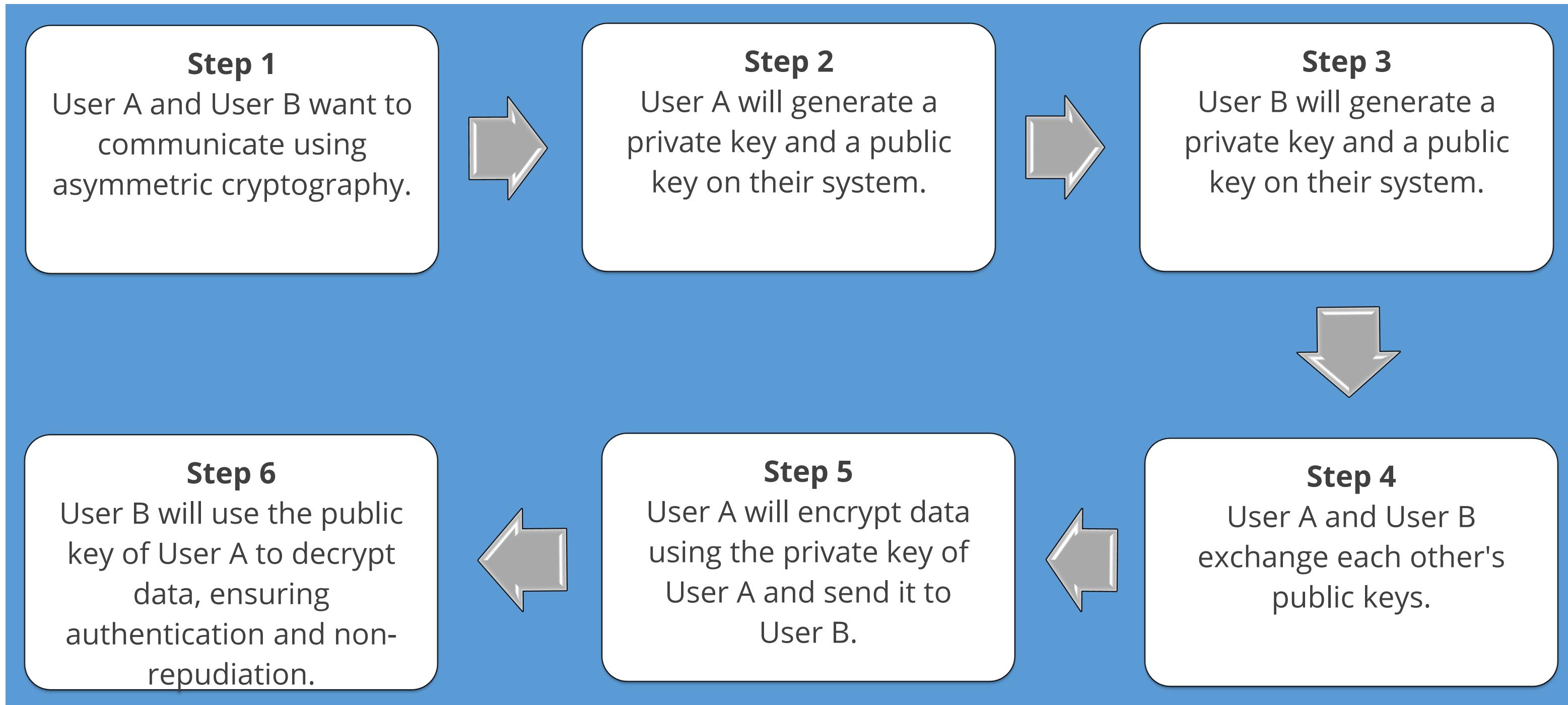
Open Message Format



Open Message Format



Open Message Format- Summarized View



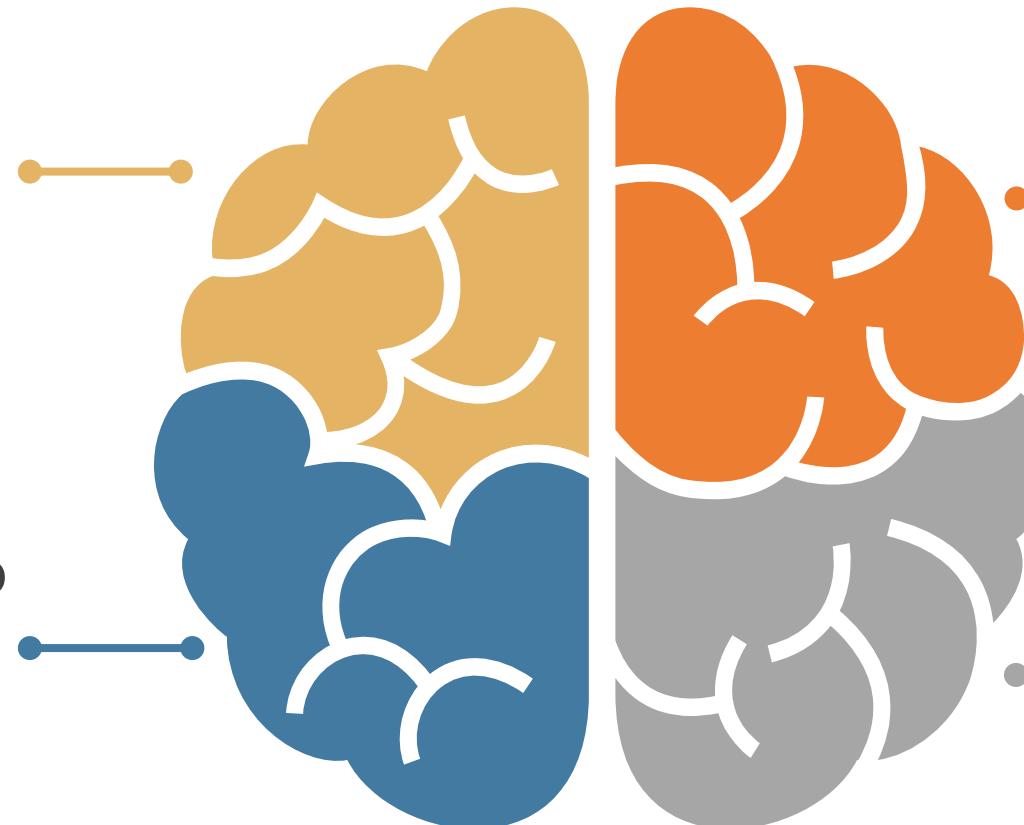
Introduction to RSA Algorithm

RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, the inventors of this algorithm.

RSA:

Is a worldwide de facto standard

Is based on the difficulty of factoring the product of two large prime numbers (up to 200 digits long), thereby making the cryptosystem difficult to crack

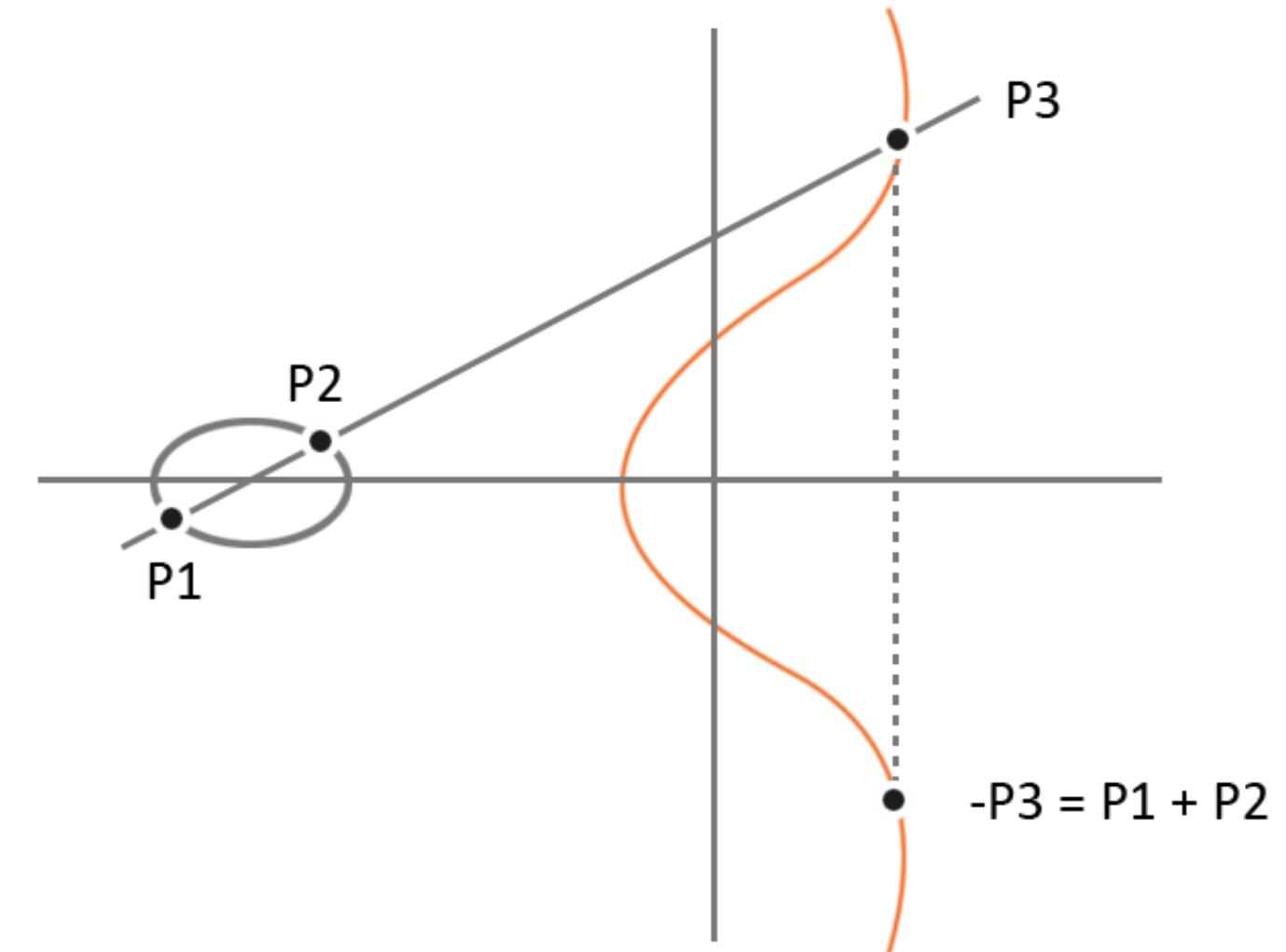


Provides digital signatures, encryption, and secret key distribution

Is used in web browsers with SSL, systems that use public-key cryptosystems

Other Types of Asymmetric Cryptography: Elliptic Curve Cryptosystems

- Instead of generating keys as the product of very large prime numbers, ECC generates keys through the properties of the elliptic curve equation.
- An ECC key of 160 bits provides the same protection as a 1024-bit RSA key.
- ECC is more efficient than RSA.
- It provides encryption, digital signature, and key exchange.
- It is used in devices with limited processing, storage, and bandwidth capacity.
- Examples: Wireless and cell phone

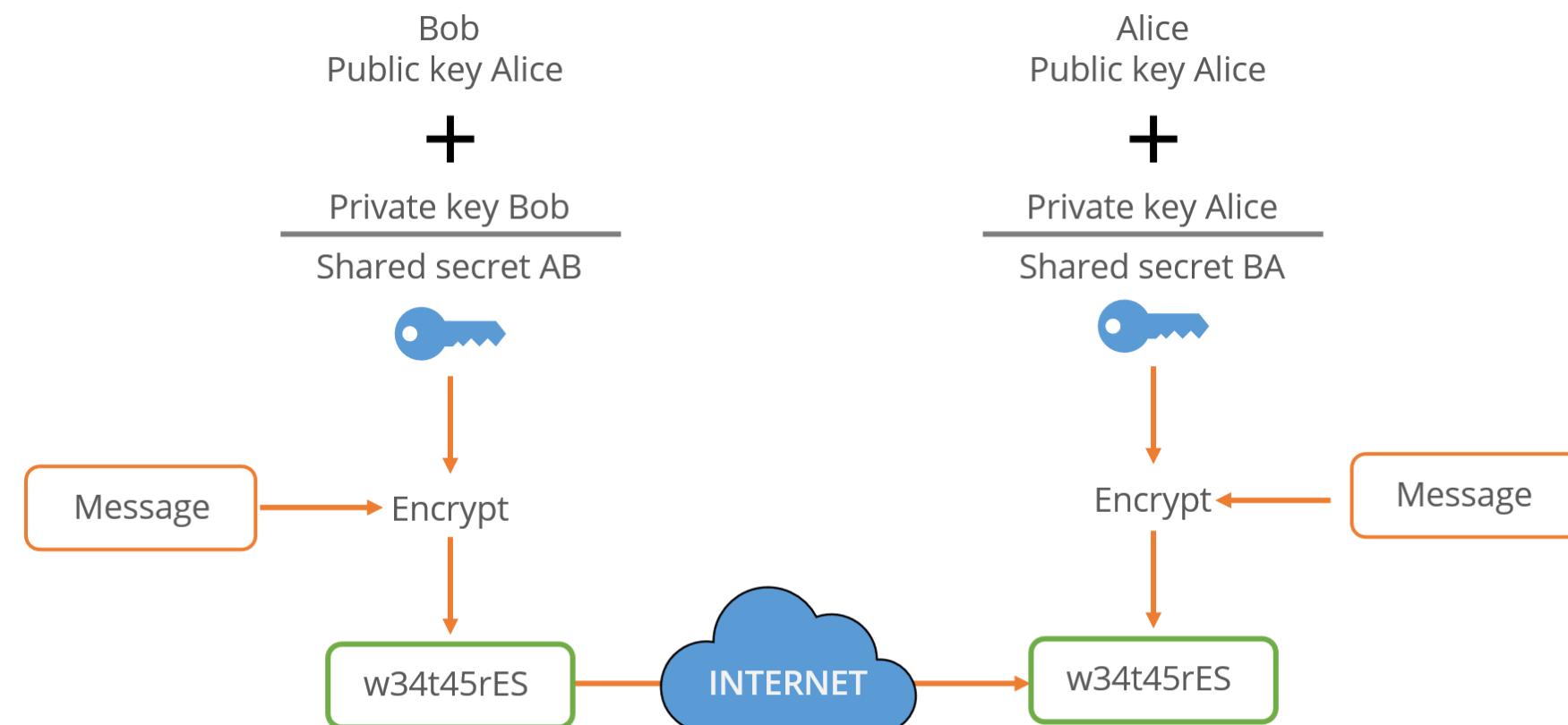


Advantages and Disadvantages

Types of cryptography	Advantages	Disadvantages
Symmetric cryptography	<ul style="list-style-type: none">Very fast to encrypt or decrypt, secure, and affordableOptimal for encrypting large files	<ul style="list-style-type: none">Presents the challenge of key managementLacks authenticity and non-repudiation
Asymmetric cryptography	<ul style="list-style-type: none">Provides better key distribution than symmetric systemsProvides better scalability due to ease of key distributionProvides authenticity and non-repudiation, in addition to confidentiality	<ul style="list-style-type: none">Much slower operation than symmetric systemsMore vulnerable to man-in-the-middle attacks

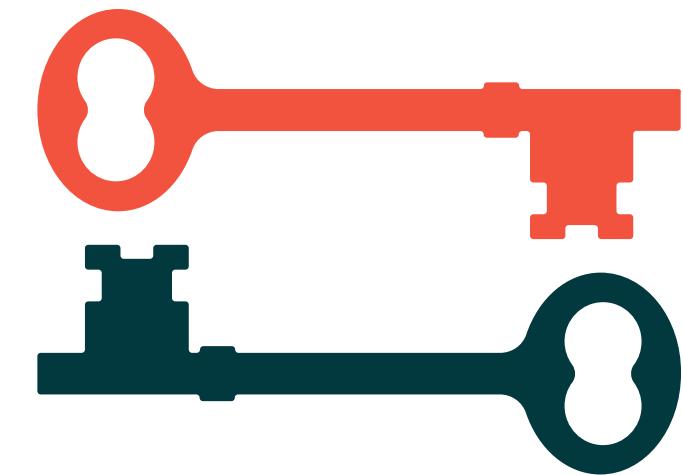
Other Types of Asymmetric Cryptography: Diffie-Hellman Key Exchange

- A key distribution asymmetric algorithm
 - A protocol whereby two or more parties can agree on a key in such a way that both influence the outcome
- Allows two users to exchange a secret key
- Requires no prior secrets
- Does not provide for encryption or digital signature functions



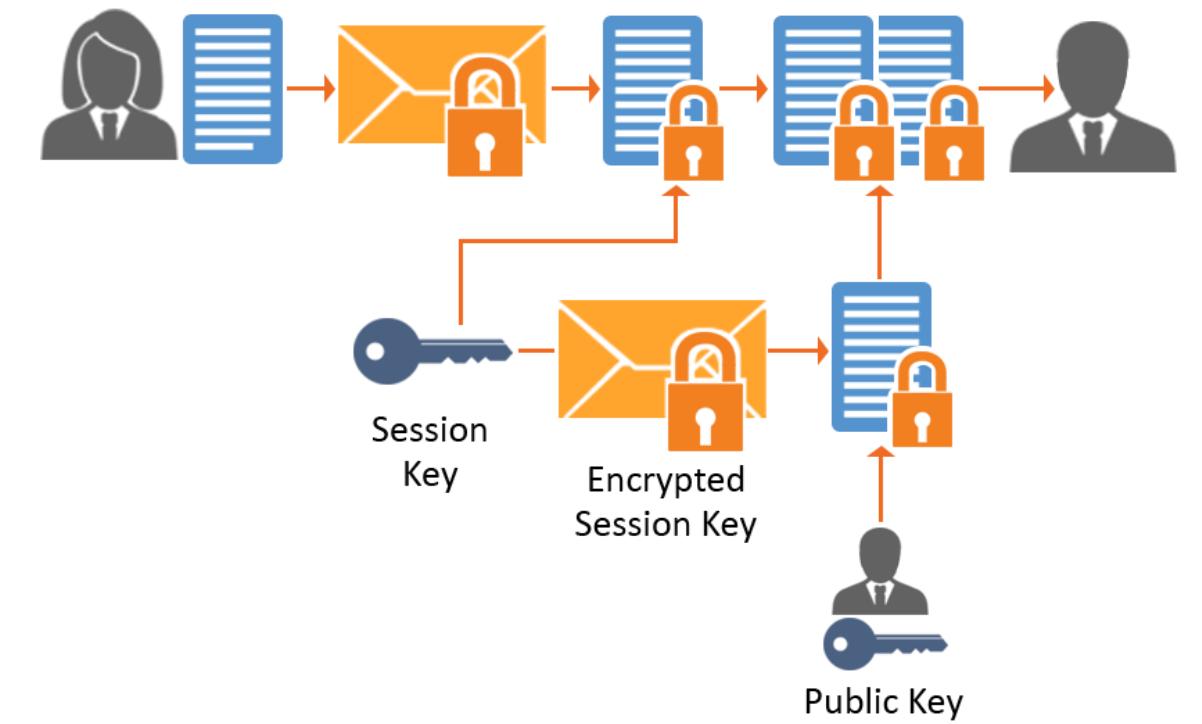
Other Types of Asymmetric Cryptography: Diffie-Hellman Key Exchange

- Vulnerable to man-in-the-middle attack
- Based on the difficulty of calculating discrete logarithms in a finite field
- Currently used in many protocols, namely:
 - Secure Sockets Layer (SSL) or Transport Layer Security (TLS)
 - Secure Shell (SSH)
 - Internet Protocol Security (IPSec)
 - Public Key Infrastructure (PKI)



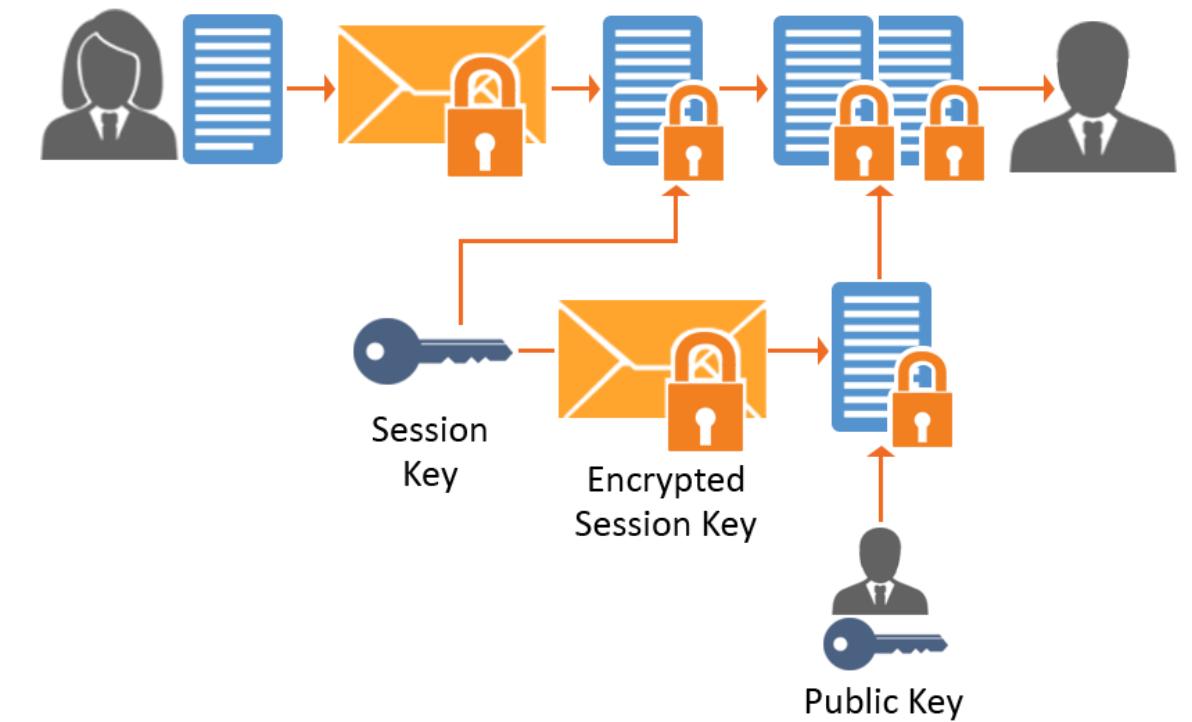
Hybrid Cryptography

- A hybrid system that combines the symmetric and asymmetric methods
- The more efficient symmetric algorithm encrypts a message using a secret key
- The symmetric secret key is encrypted using recipient's public key with an asymmetric algorithm
- The message encrypted with that secret key and the encrypted symmetric secret key are sent to the recipient



Hybrid Cryptography

- The recipient uses their private key to decrypt the secret key.
- The secret key is then used to decrypt the message.
- A symmetric algorithm is used for bulk encryption.
- The asymmetric algorithm is used to distribute the symmetric key.

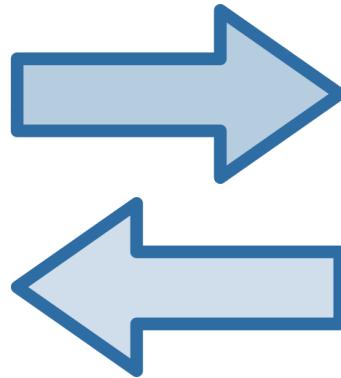


Hybrid Cryptography



Charles

Charles wants to send bulk data to Alice and ensure that only she can read it.



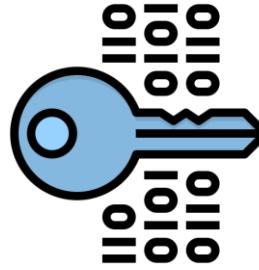
Alice

Hybrid Key Cryptography

Charles generates a private and public key pair and exchanges his public key with Alice's public key.

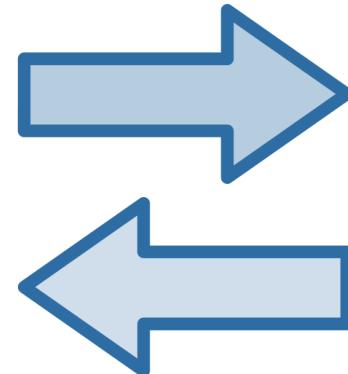
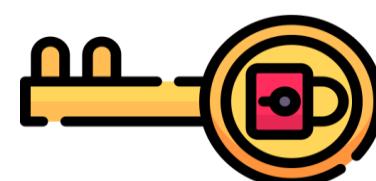


Charles

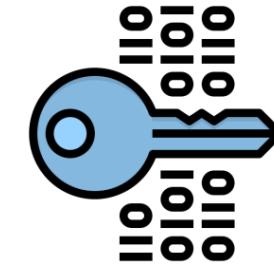


Alice public key

Charles private key



Charles public key



Alice private key

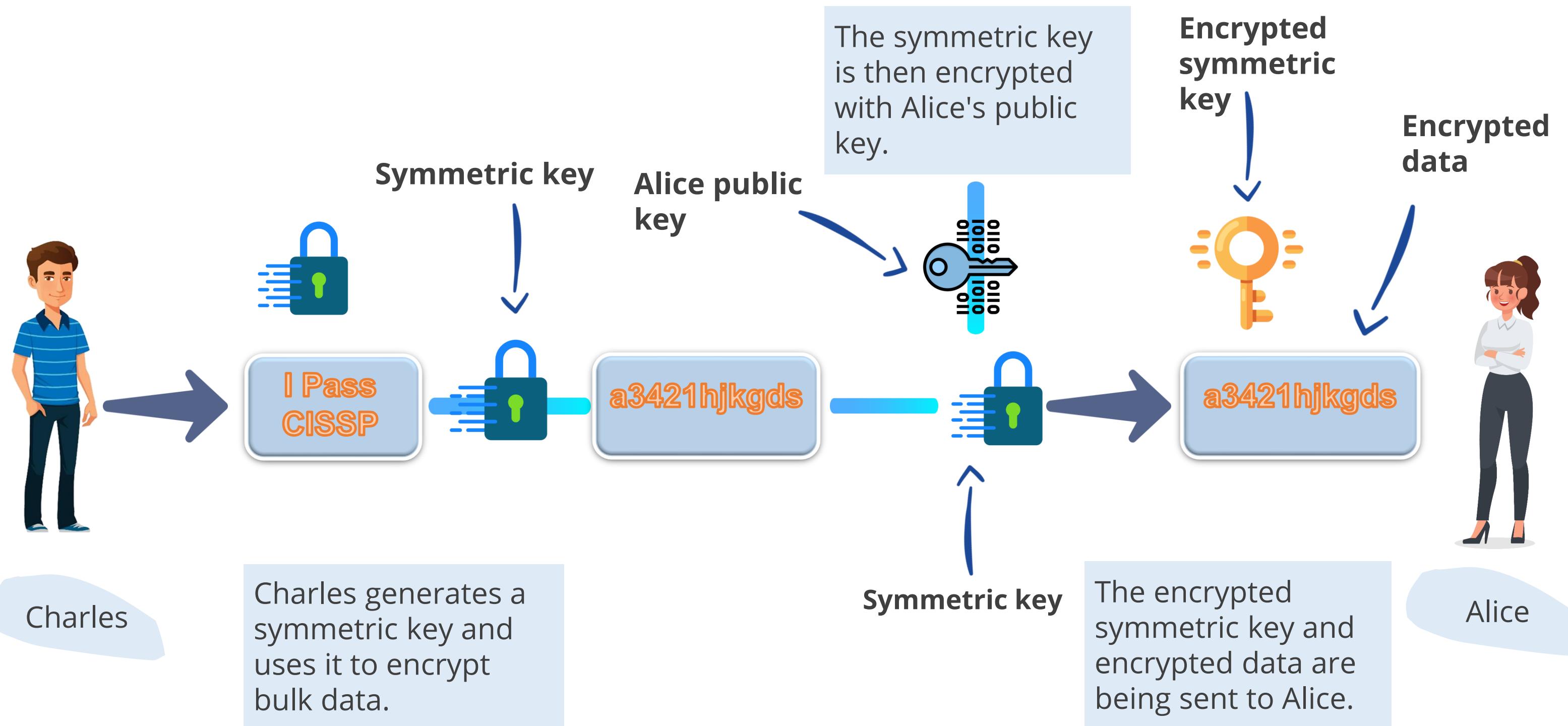


Similarly, Alice will also generate a private and public key pair and exchange her public key with Charles's public key.

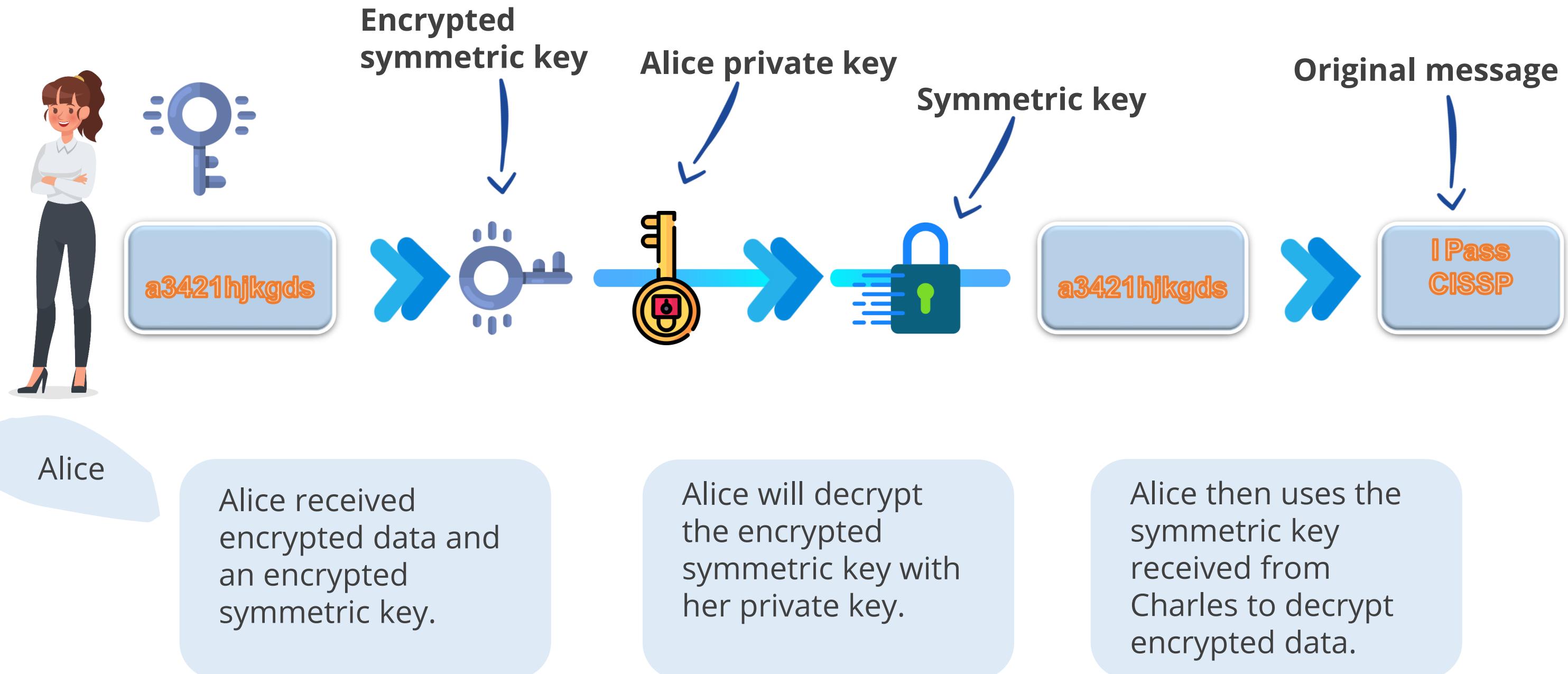


Alice

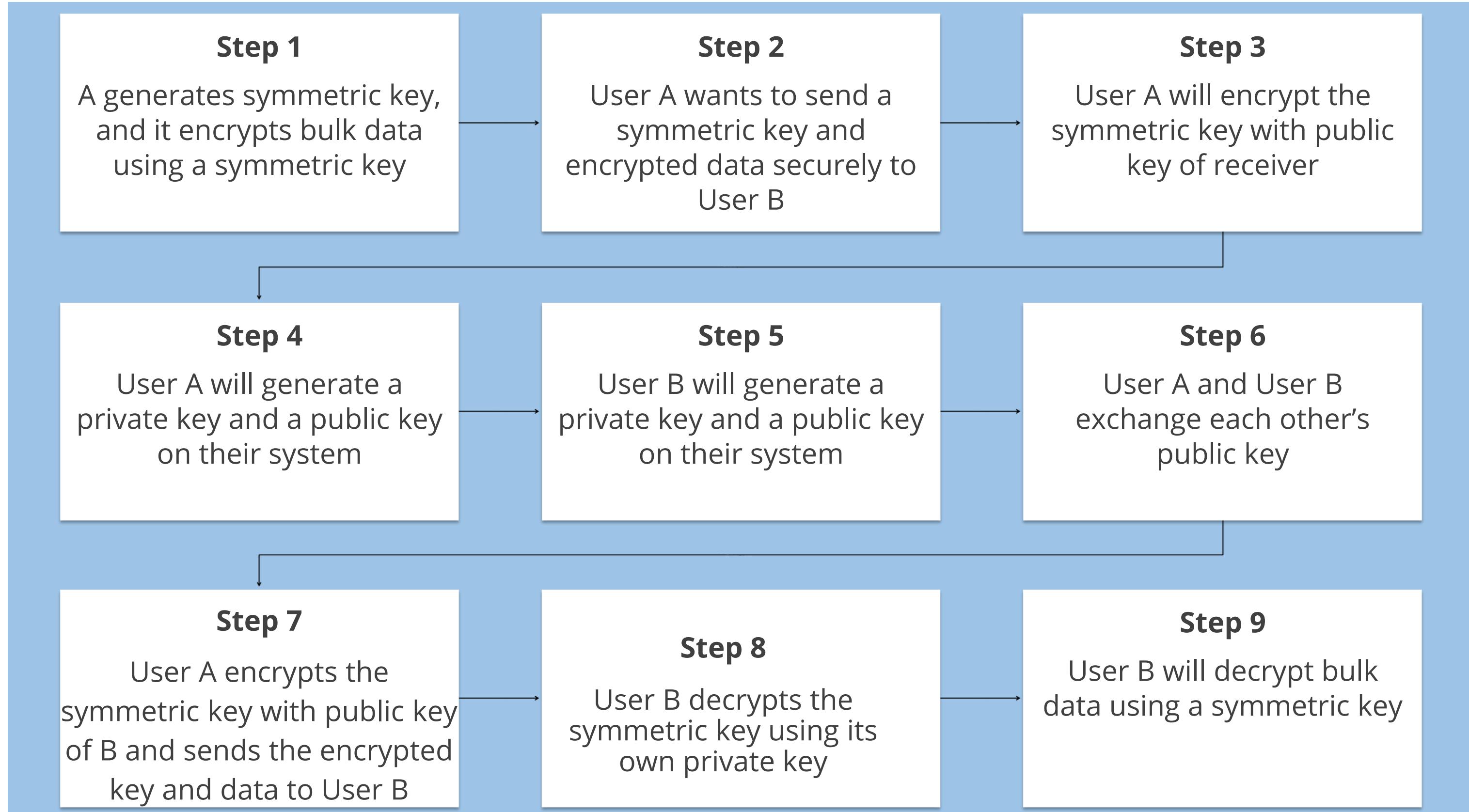
Communication Process at Sender's End



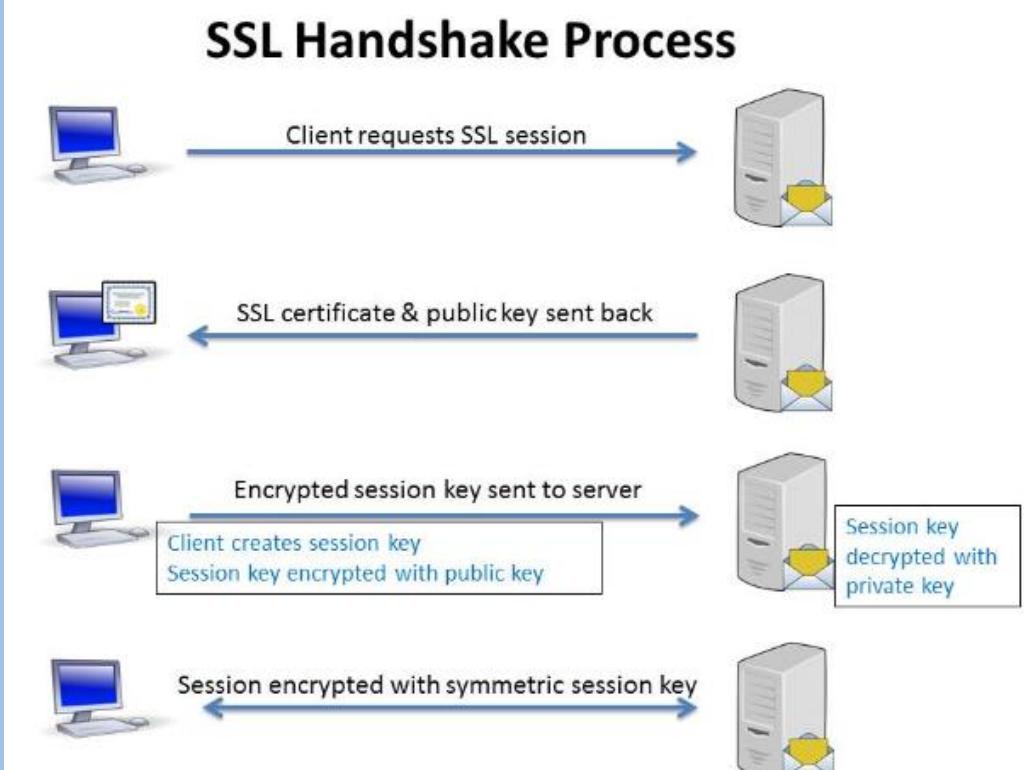
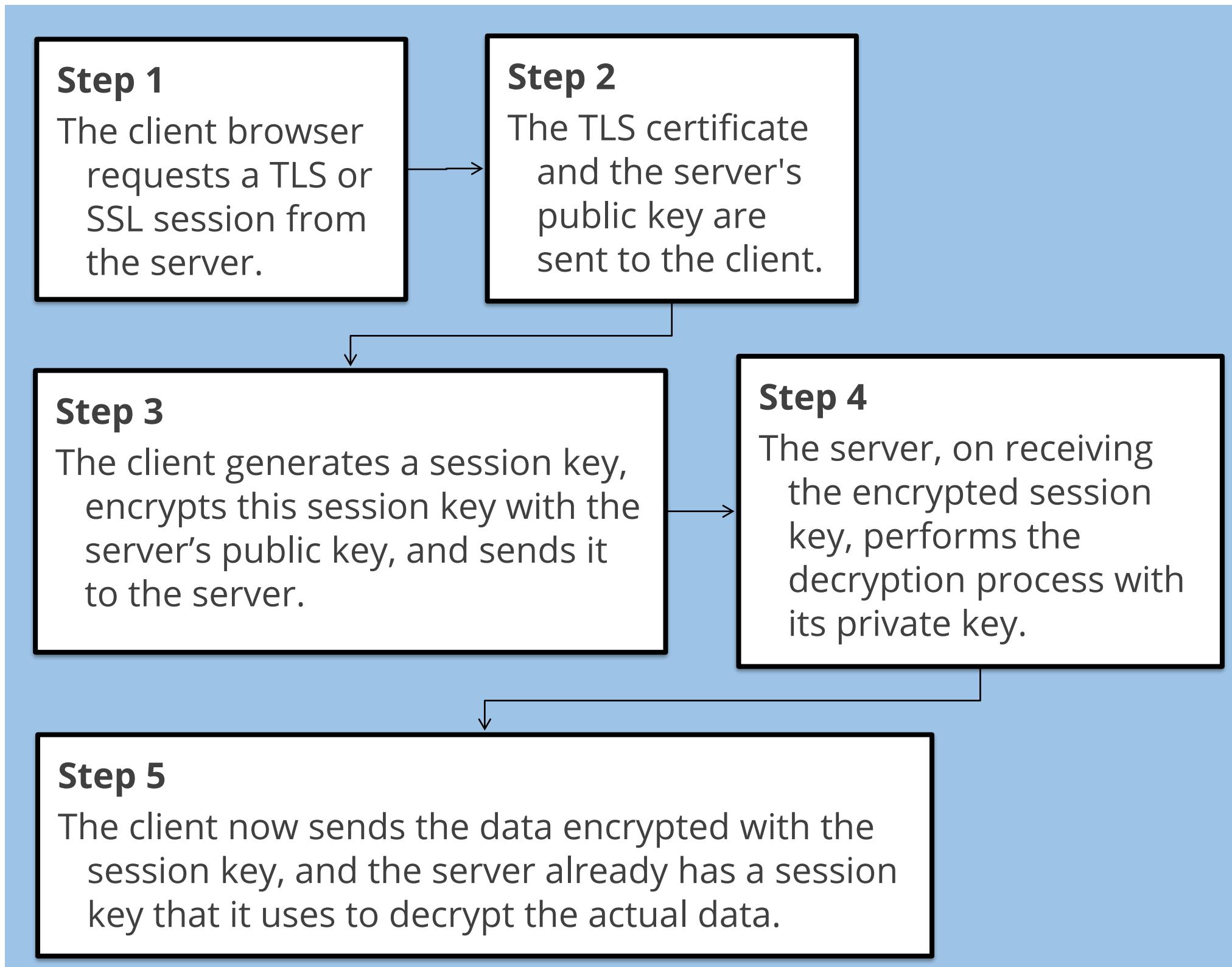
Communication Process at Receiver's End



Hybrid Cryptography-Digital Envelope



SSL or TLS



Session Key

- A single-use symmetric key is used to encrypt or decrypt communication between two users for a single session.
- It's more secure than static symmetric keys.
- Peers decide on the session key and continue to use it until the session is over.
- Eavesdropping is difficult here, and attempting to break the keys is futile.



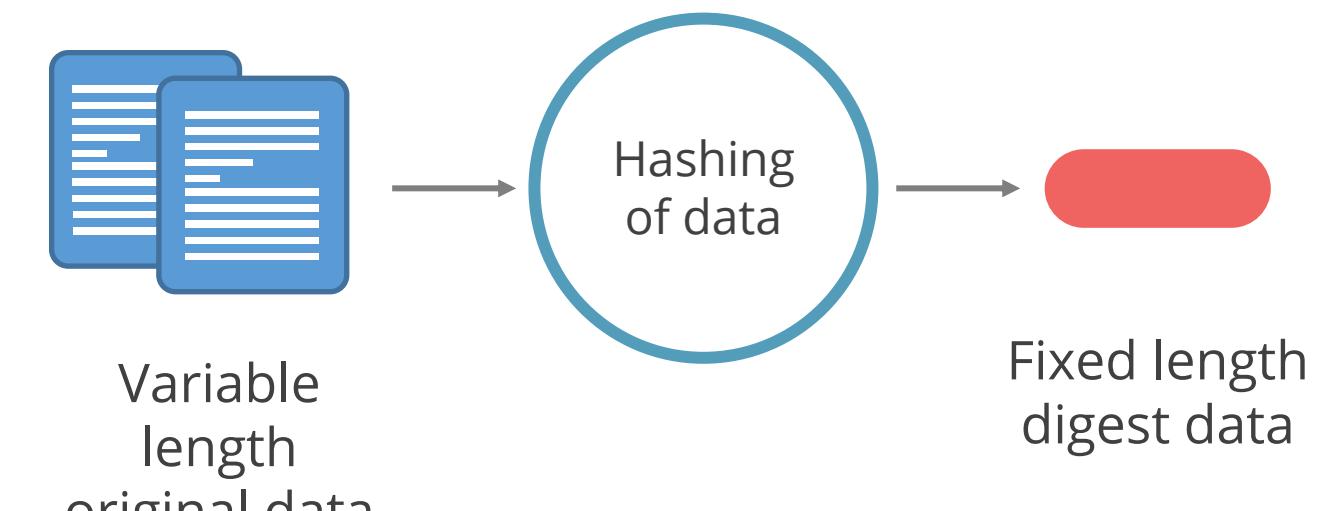
TECHNOLOGY

Hashing Process

One-Way Hash

A hash function uses an algorithm without any key for encryption. This encryption cannot be reversed and hence is called one-way.

- A fixed-length hash value (message digest or hash) is created or hashed from variable-length plaintext.
- When the plaintext changes, its hash value also changes. Thus, hash functions are used to provide integrity.
- It guarantees the integrity of data.
- It can be applied to data blocks of any size.
- It produces a fixed-length output.



One-Way Hash

Characteristics:

- The Hash should be computed over the entire message.
- The Hash should be a one-way function.
- Given a message and hash value, computing another message with the same value should be impossible.
- It should be resistant to birthday attacks.



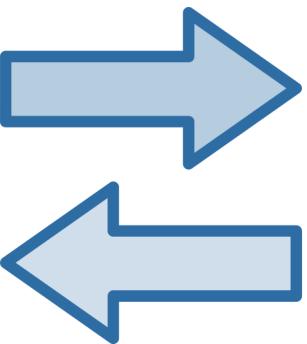
Hashing Process

1

Charles wants to send an email to Alice and ensure that it is not tampered with during transit.

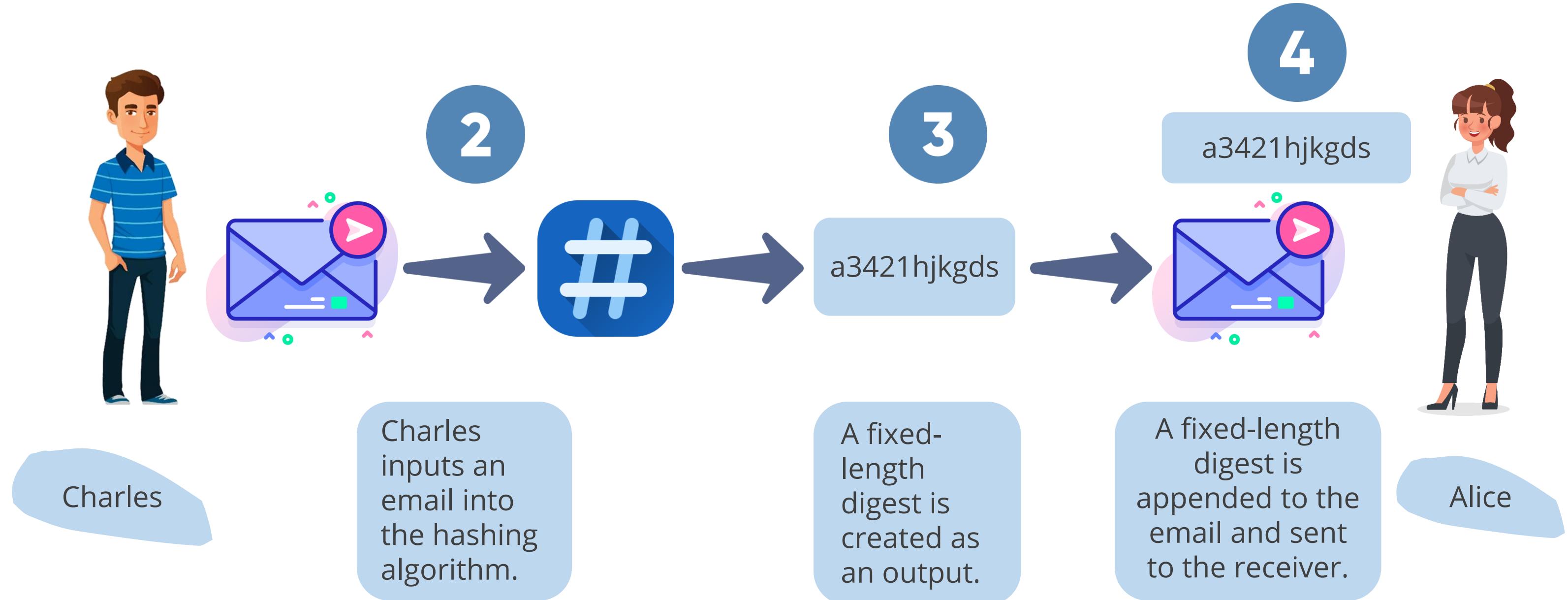


Charles



Alice

Hashing Communication Process at Sender's End



Hashing Communication Process at Receiver's End



5

a3421hjkgsd



Alice

Alice, on receiving the email appended with hash, will separate email and hash digest.

6



7

a3421hjkgsd

a3421hjkgsd



a3421hjkgsd

Alice will input the email received from Charles into the hashing algorithm, and a fixed-length digest will be created again.

Fixed length digest created at the receiver end and that is received from the sender will be compared.

If they are the same, no tampering happens in transit.

Hashing Process Summarized - Integrity

Step 1

User A wants to send an email to User B and ensure that the email is not tampered with in transit.

Step 2

User A feeds the email into an MD5 or SHA hashing algorithm.

Step 3

A hashing algorithm processes an email and produces a fixed-length digest as output (**MD5 128 B, SHA 160**).

Step 6

User B removes the digest and feeds the email back into the hashing algorithm.

Step 5

User B receives an email along with the digest.

Step 4

User A appends this digest to the email and sends it to User B.

Step 7

The email received from User A will be fed into a hashing algorithm at the receiving end, which will produce a message digest as output.

Step 8

Both message digests will be compared; if they are the same, then the data has not been tampered with.

Hashing Algorithms

A hash function is any algorithm or subroutine that maps large data sets of variable length to smaller data sets of a fixed length.

MD5:

- The most widely used hash algorithm in the MD (Message-Digest Algorithm) family.
- It is harder to break; for any input length, it creates a 128-bit hash value.

SHA-1:

- Belongs to the Secure Hash Algorithm (SHA) family
- Generates a 160-bit hash value
- SHA-2 includes SHA-224, SHA-256, SHA-384, and SHA-512, termed after the length of the hash value each creates

Application of Hashing

Password verification

Storing passwords in normal text files is dangerous, which is why almost all sites store passwords as hashes.

Signature verification

Generating and verifying signatures is a mathematical process used to verify the authenticity of digital documents or messages.

Data integrity checks

Data integrity checks are a crucial application of hashing. They involve generating checksums for data files, which provide users with assurance about the correctness of the data.

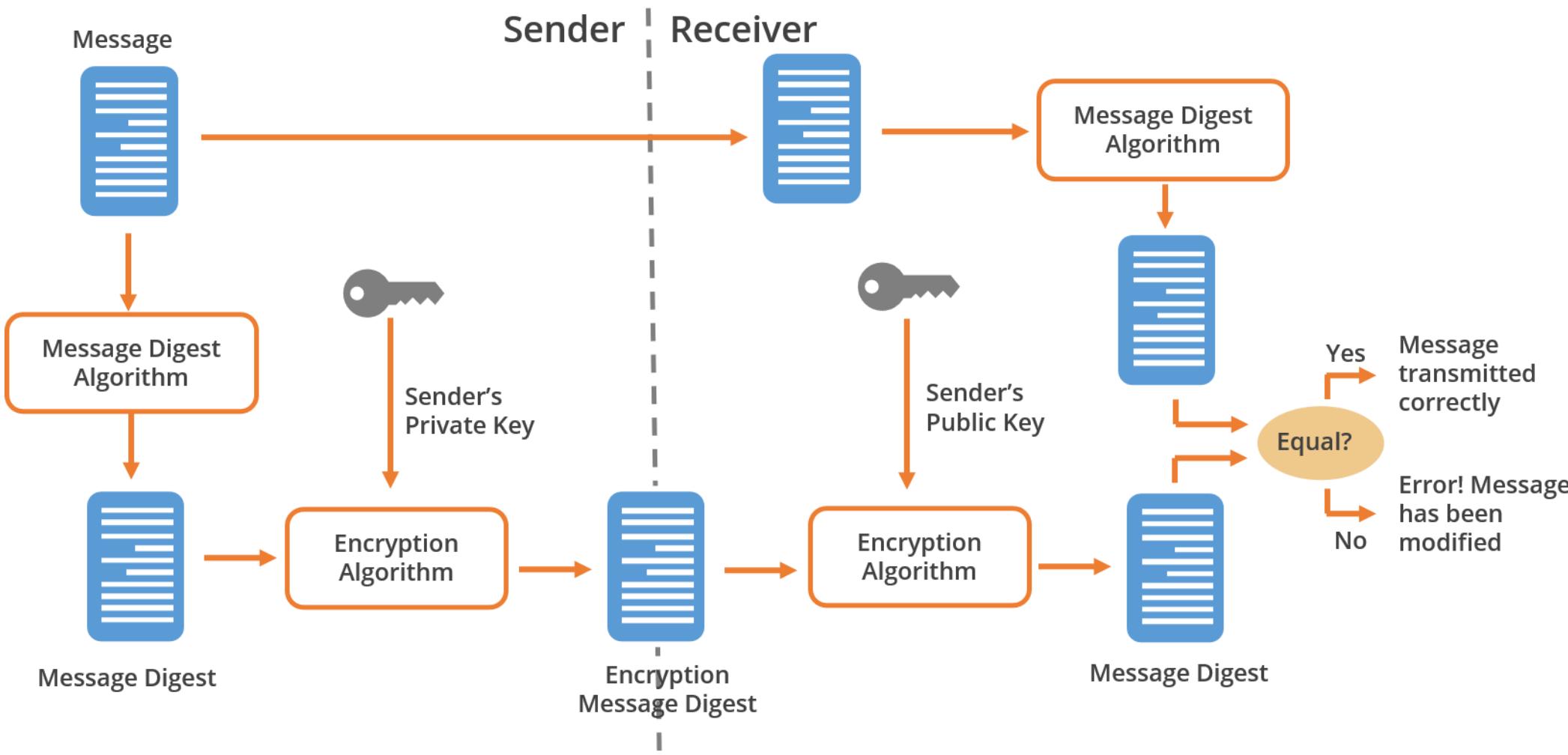
Digital Signatures

Digital signatures:

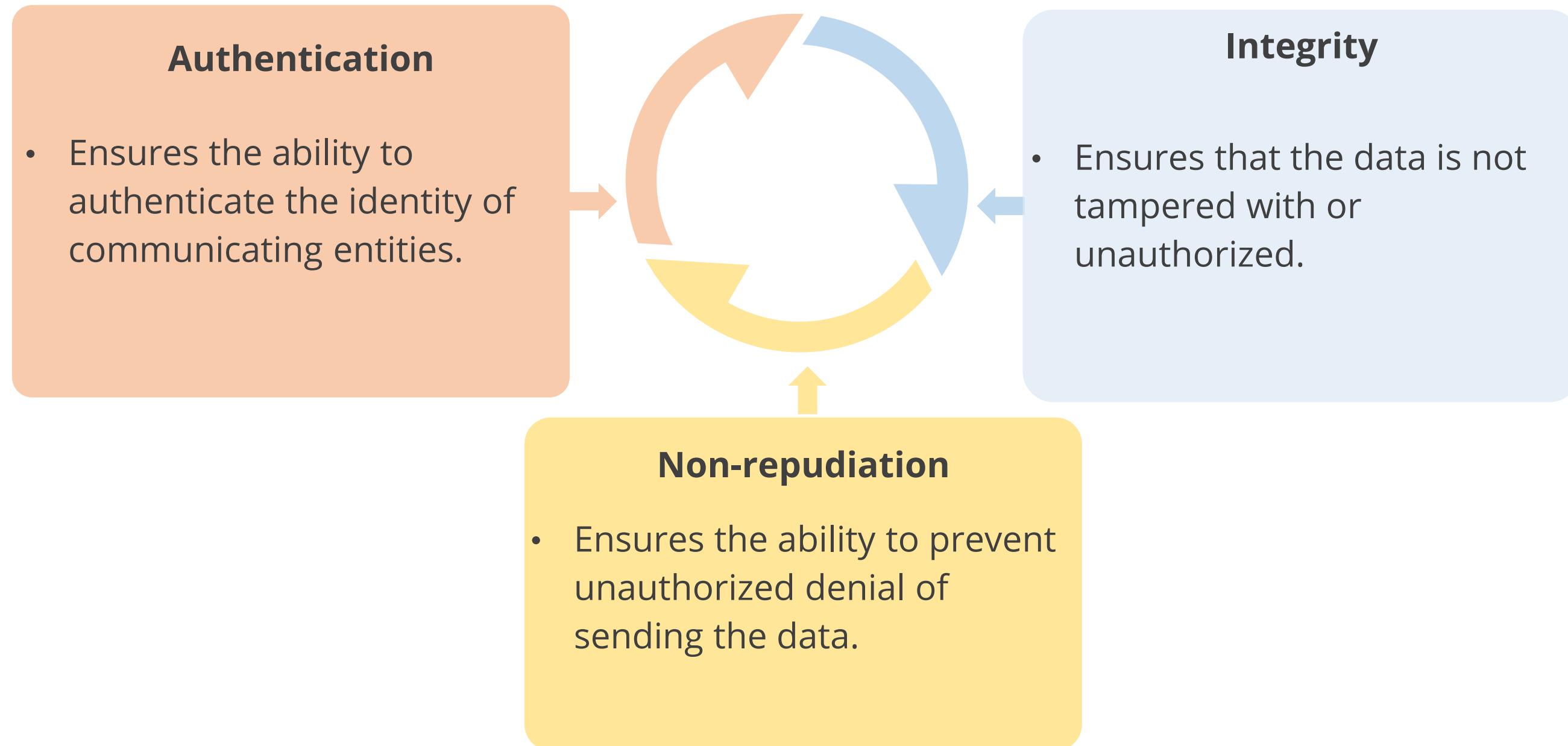
- Are used for signing the document cryptographically
- To digitally sign the data:
 - Create a hash of the data
 - Encrypt that hash with the sender's private key
- To verify the digital signature:
 - Hash the data
 - Find the sender's public key
 - Decrypt the signature with the sender's public key
 - Check whether the hash you have created matches the hash you received
- Hashing provides message integrity; signing of hash provides authentication and non-repudiation
- Involve encrypting the hash value of a message with a private key

Digital Signatures

The working of digital signatures is illustrated below:



Goal of Digital Signature



TECHNOLOGY

Digital Signature Process

Digital Signature

Charles wants to send an email to Alice and wants that email not to be tampered with in transit.



Charles



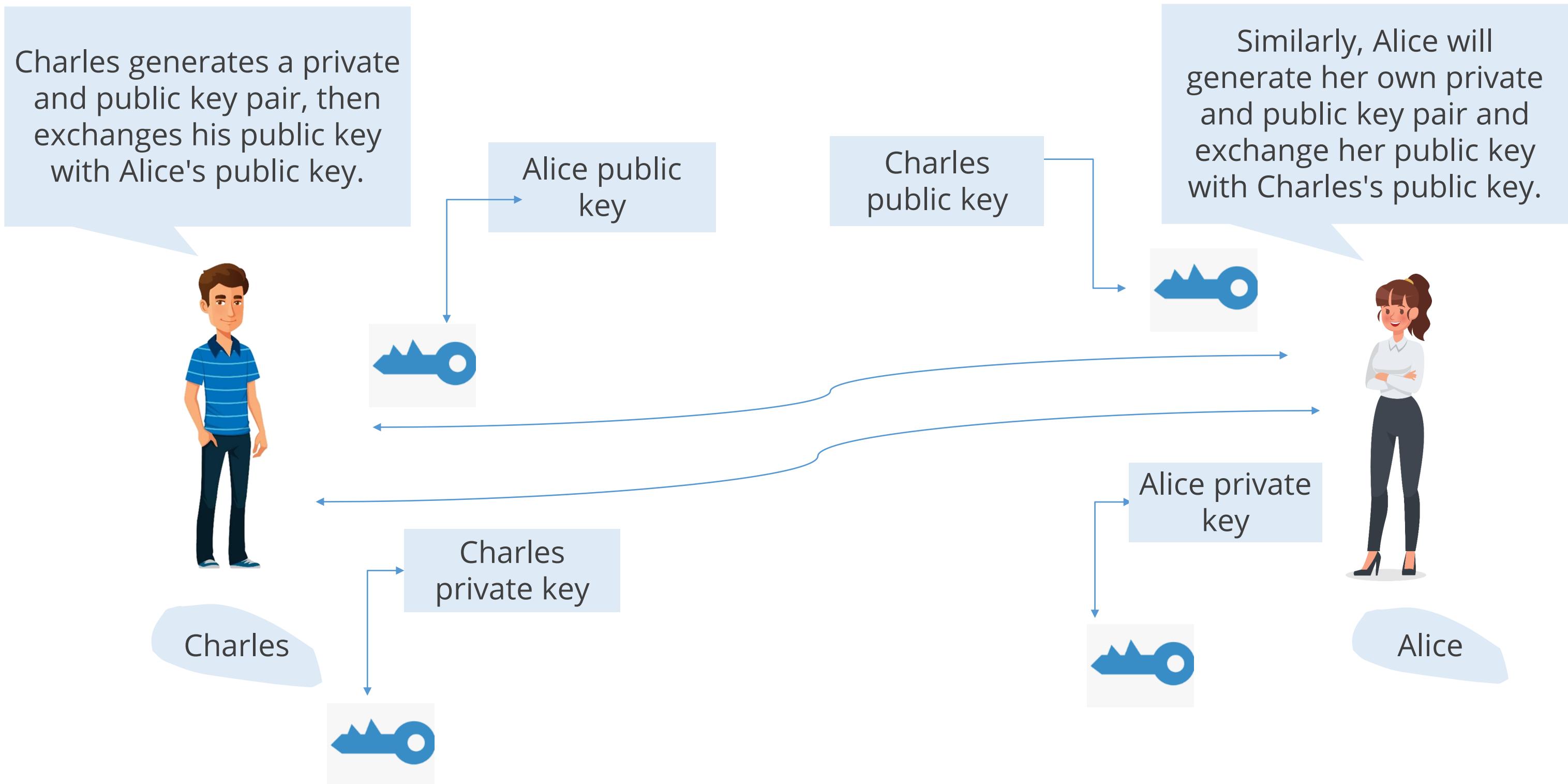
Alice wants to ensure not only integrity but also authentication and non-repudiation.



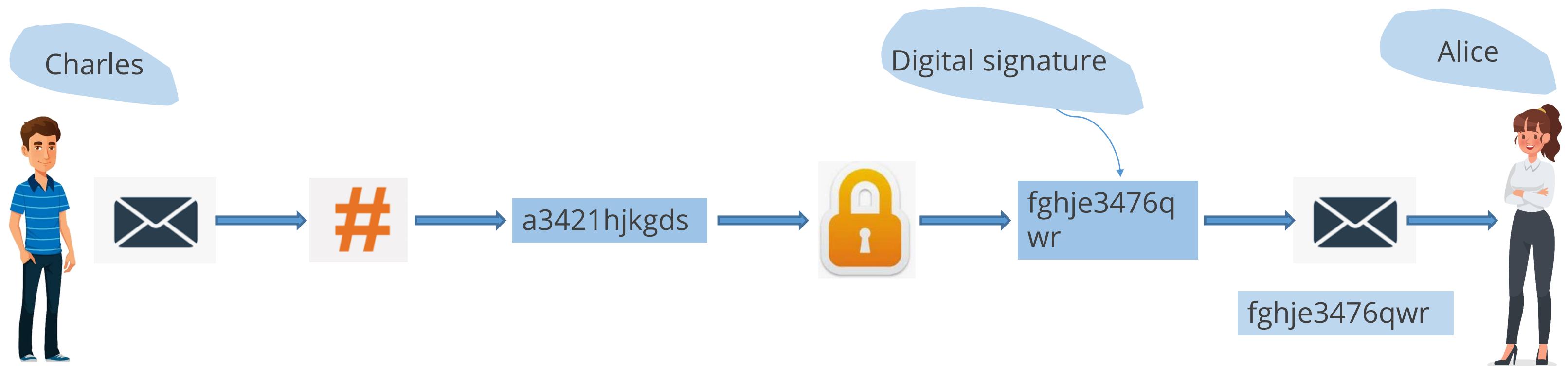
Alice



Digital Signature



Digital Signature Communication at Sender's End



Charles inputs an email into a hashing algorithm.

A fixed-length digest is created as the output.

The message digest is encrypted using the private key of the sender, Charles, in this communication.

The encrypted message digest is called a digital signature.

This digital signature will be appended to the email and sent to the receiver.

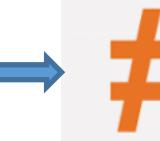
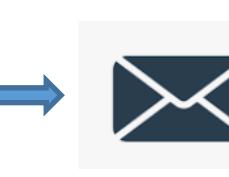
Digital Signature Communication at Receiver's End



fghje3476



a3421hjk



a3421hjk



fghje3476qwr

Alice, upon receiving the email appended with the digital signature, will separate the digital signature from the email.

The digital signature will be decrypted with the sender's public key. Correct decryption ensures authentication and non-repudiation.

After decrypting with the sender's public key, the hash digest received from the sender will be visible.

Now, the email will be fed into a hashing algorithm to generate a hash digest.

Both hash digests will be compared. If they are the same, it means the email has not been tampered with, ensuring integrity.

a3421hjk

a3421hjk

Application of Digital Signatures

Communication security

You can encrypt the mail with the recipient's public key and sign it on your side. This way the sender knows for sure that there was no tampering and that the message comes from you.

Code security

Authors or coders can protect their code against tampering by digitally signing it.

Software updates

Vendors digitally sign the updates to protect against tampering and ensure that it is released by them by digitally signing and providing users with their public key to verify their digital signature.

Financial sectors

It is used by a company to protect against tampering with financial documents and ensuring that it has been issued by them. For e.g., when a company issues Form 16, it is digitally signed to protect against tampering and prove authenticity.

Advantages of Digital Signature

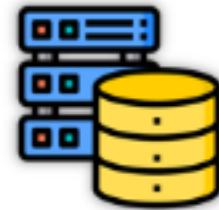
Highly robust:

- DSA is highly robust in the security and stability aspect compared to alternative signature verification algorithms.



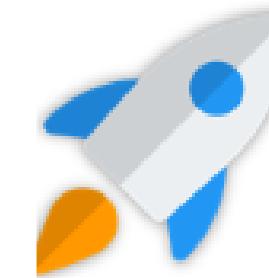
Less storage:

- DSA requires less storage space to work its entire cycle.



Better speed:

- The key generation is much faster compared to the RSA algorithm and such.



Patent free:

- When NIST releases it, it is patent-free to enable its global use free of cost.



Birthday Attack

Birthday attack

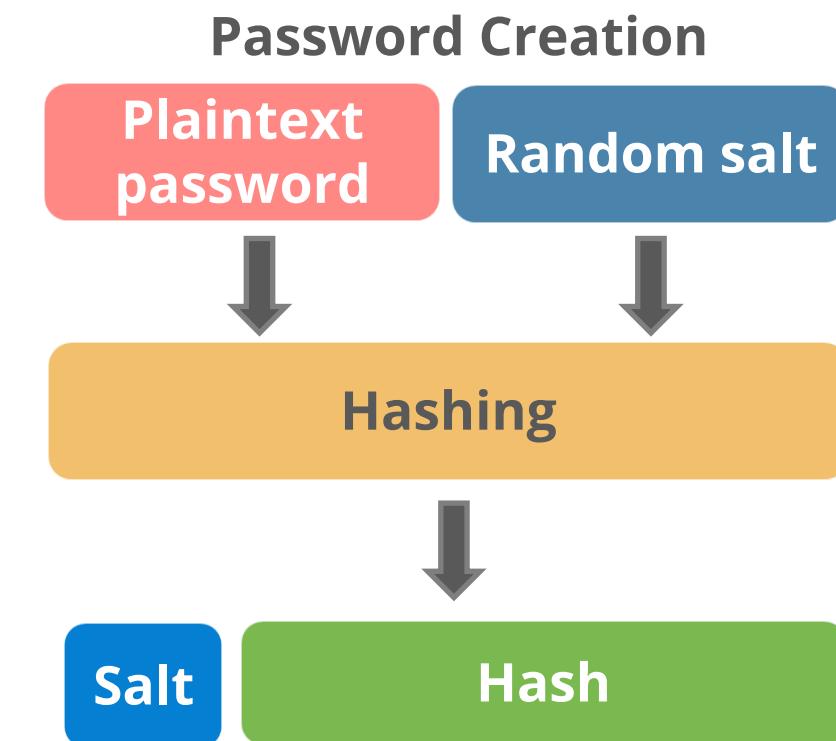
- If an algorithm produces the same value for two distinctly different messages, it is called a hash collision.
- The birthday attack attempts to exploit the probability of two messages producing the same message digest by using the same hash function.
- It is based on the statistical probability that with 23 people in a room, there is more than a 50% probability that two people have the same birthday.
- SHA-1 (160 bits) may require approximately 280 computations to find a hash collision.
- A hashing algorithm that has a larger bit output, such as a birthday attack, is less vulnerable to brute force attacks.

Salting

Salt is a random value added to password hash to prevent dictionary attacks and hash collisions.

Salting

- It makes it difficult for the attacker to break into a system by using the strategy of password hash-matching.
- For each password, a new salt is randomly generated.
- Instead of the original password, the output of the cryptographic hash function processed is stored in the database.
- It is used in Unix systems and for internet security.

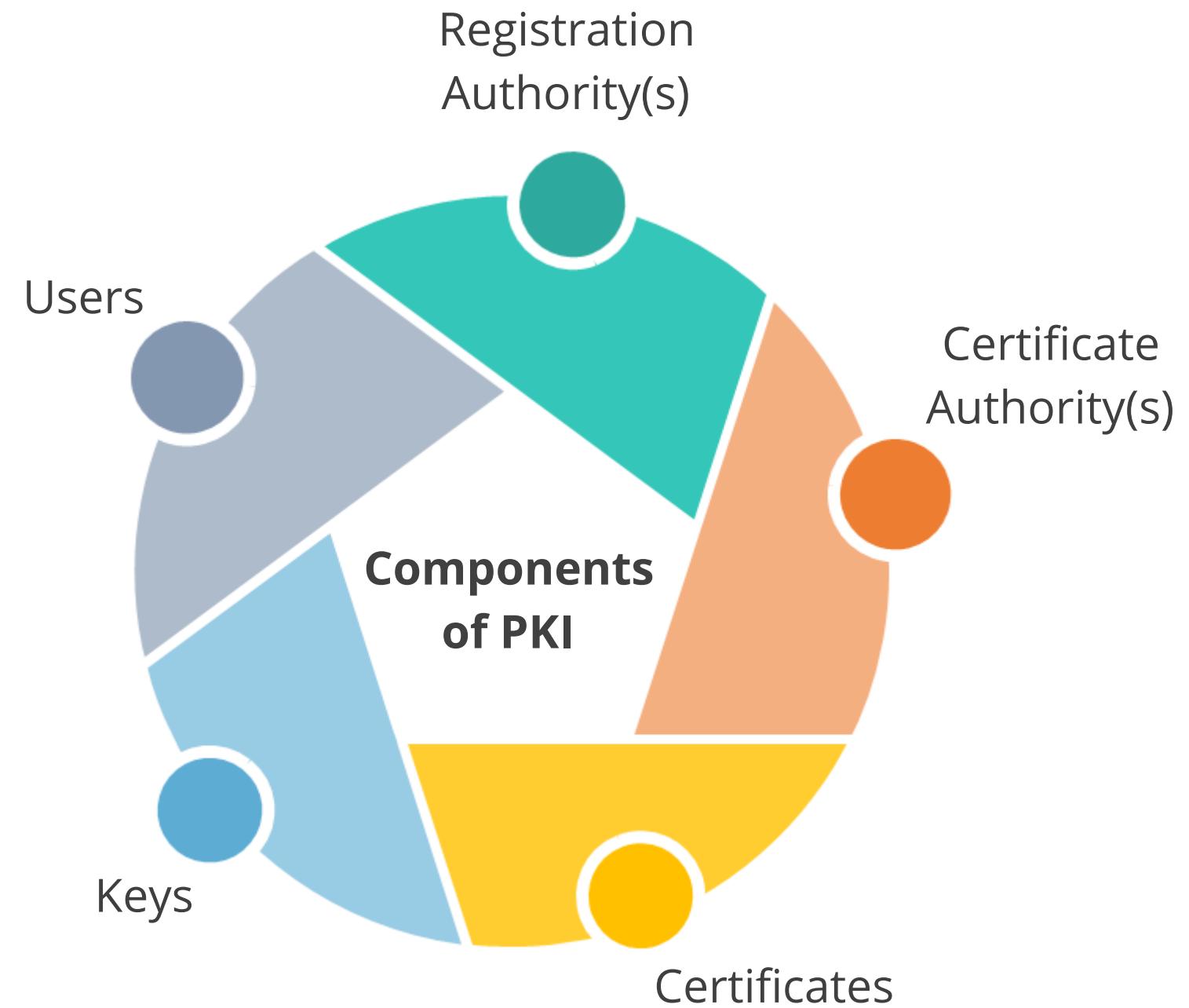


TECHNOLOGY

Public Key Infrastructure

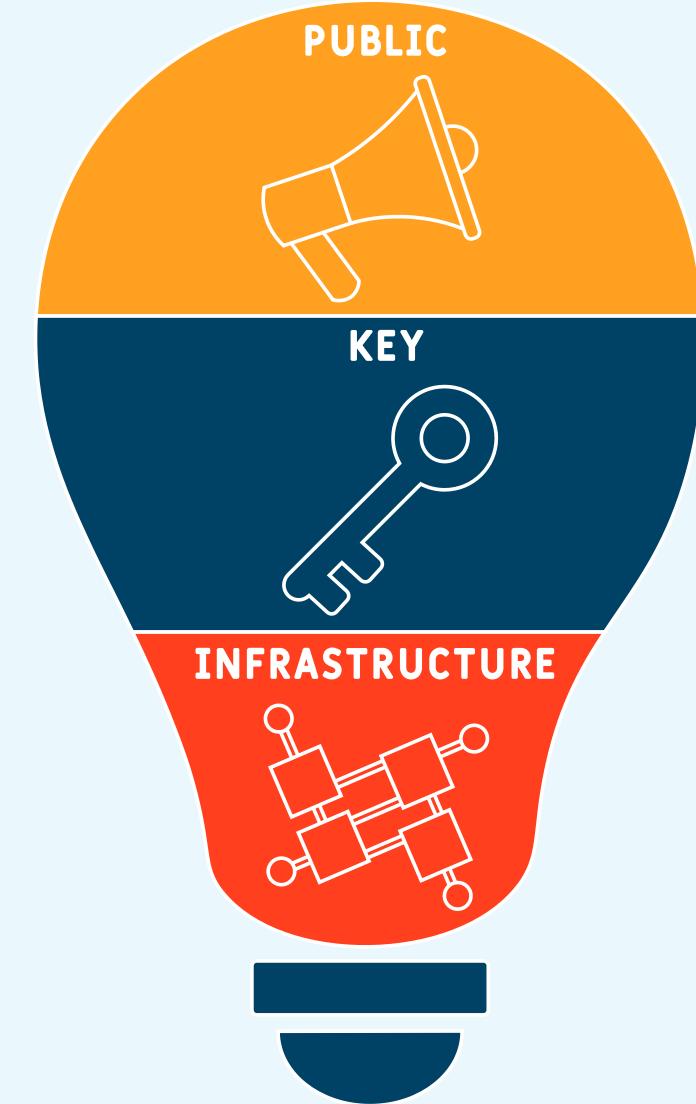
Introduction to Public Key Infrastructure

“ A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.”



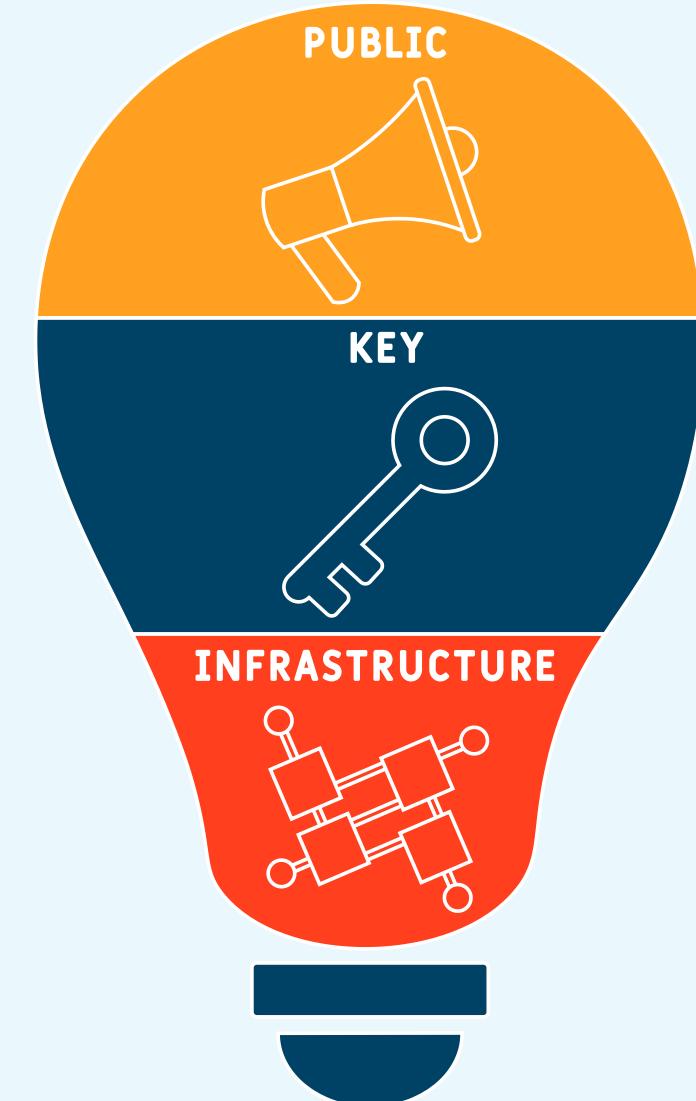
Introduction to Public Key Infrastructure

- The public key infrastructure provides confidentiality, integrity, authentication, and non-repudiation.
- PKI includes:
 - Certificate Authority (CA)
 - Digital certificates
 - Registration Authorities (RA)
 - Policies and procedures
 - Certificate revocation
 - Time-stamping
 - Nonrepudiation support
 - Security-enabled applications



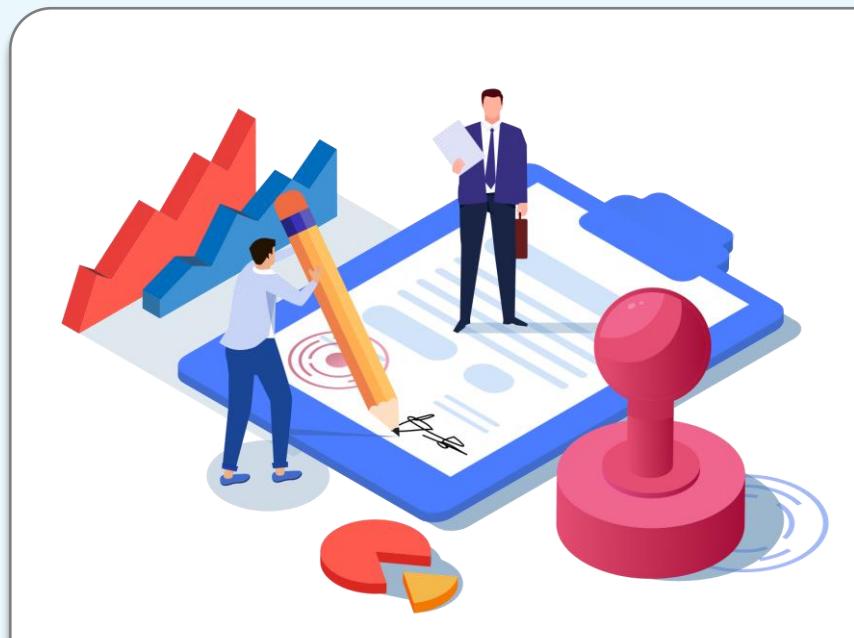
Introduction to Public Key Infrastructure

- A digital certificate is required by each participant in a PKI, which contains a particular participant's public key and other identifying information.
- This is signed by a trusted CA, and the authenticity of the public key is the liability of the CA.
- PKI is used in online banking and e-commerce.



Certificate Authority

- CA is a trusted third party responsible for the issuance and maintenance of digital certificates.
- It can also be internal to an organization.
- CA also handles the revocation of certificates.
- The revoked certificates are stored in the Certificate Revocation List (CRL), which is updated and maintained by the CA.



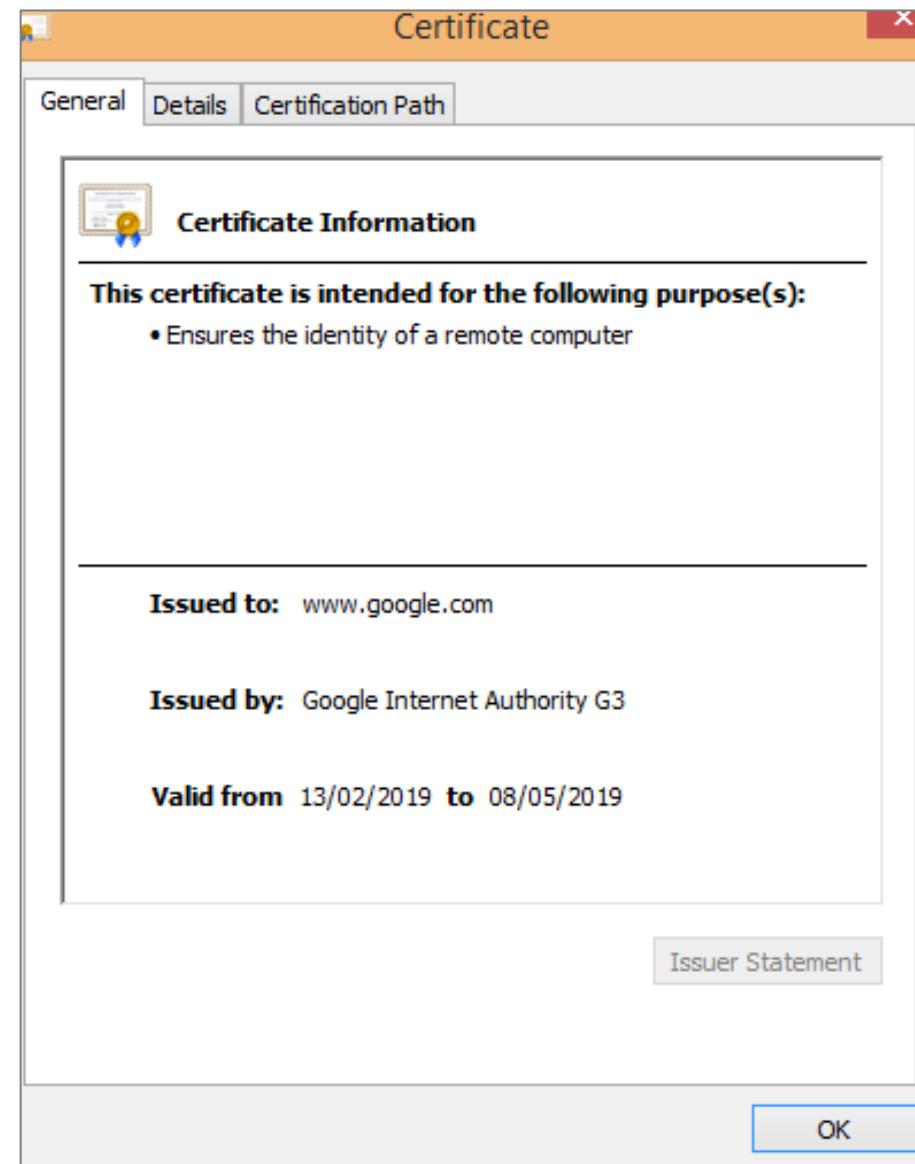
Registration Authority

- The RA performs the registration duties.
- It establishes and confirms the identity of the individual, initiates the registration process with CA, and performs certificate lifecycle management.
- The RA verifies all the necessary information before allowing a request to go to CA.
- The RA cannot issue certificates.



PKI Certificate

A digital certificate, also known as a public key infrastructure certificate, is used to cryptographically link the ownership of a public key with the entity that owns it.



Digital certificates are used for sharing public keys for encryption and authentication.

PKI Certificate

Digital certificates include:

- The public key being certified
- Identifying information about the entity that owns the public key
- Metadata relating to the digital certificate
- A digital signature of the public key created by the issuer of the certificate



X.509 is the standard that dictates the fields used in the certificate and the valid values that can be populated in those fields.

Root of Trust

The root certificate is a self-signed certificate that serves as the foundation for the entire certificate chain. The root key is utilized to generate the root certificate.

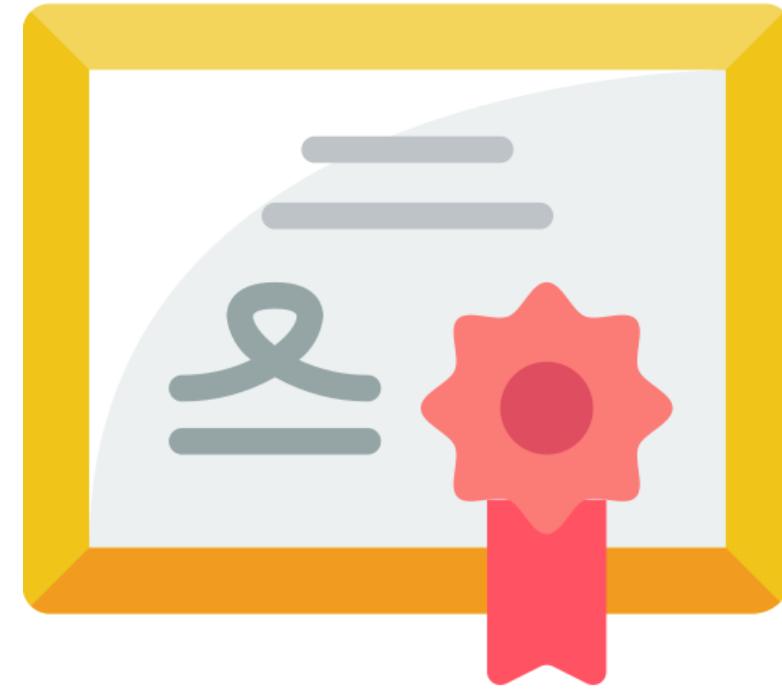
- When a device encounters a digital certificate, it can verify its authenticity by checking the certificate's chain of trust.
- The communication is secure and genuine if the certificate can be traced back to a trusted root certificate.
- In certificate management, the root CA is the highest authority in the certificate chain and is trusted to validate and sign certificates.
- Trust is extended downstream to all issued certificates, establishing the certificate hierarchy.



Self-Signed Certificate

A self-signed certificate is created and signed by the same entity to which it is issued.

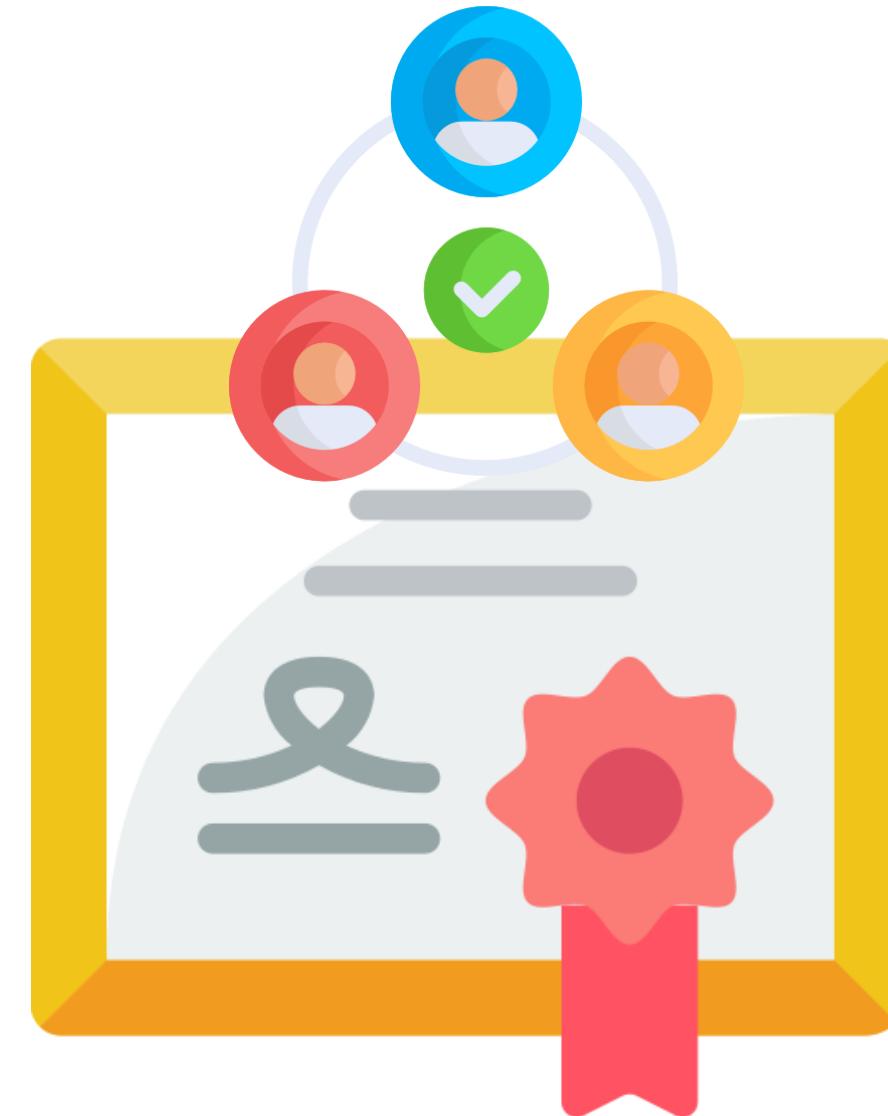
- Unlike certificates issued by trusted third-party CAs, self-signed certificates are not verified by an external authority.
- This means the entity creating the certificate asserts its identity without external validation.



These certificates can be installed on multiple internal servers.

Third-Party Certificates

- A third-party CA is responsible for verifying entities' identities and issuing digital certificates, which serve as digital ID cards to prove an entity's authenticity on the Internet.
- For online trading, the website needs globally recognized third-party certificates.
- Examples of third-party certificate authorities: DigiCert, GlobalSign, GeoTrust, and Thawte.



Certificate Signing Request (CSR)

A CSR is a digital identity certificate application.

- It is what an entity sends to a CA to secure its online communications.
- The CSR includes the public key and identifying information.
- The CA then verifies the credentials and issues a trusted certificate, confirming the entity's authenticity.



Wildcard Certificate

It is an SSL/TLS certificate that secures an entire domain and its subdomains with a single certificate.

- It employs a wildcard character, typically an asterisk (*), to represent any subdomain within the main domain.
- A single wildcard certificate, *.example.com, can secure all current and future subdomains, such as mail.example.com and shop.example.com.

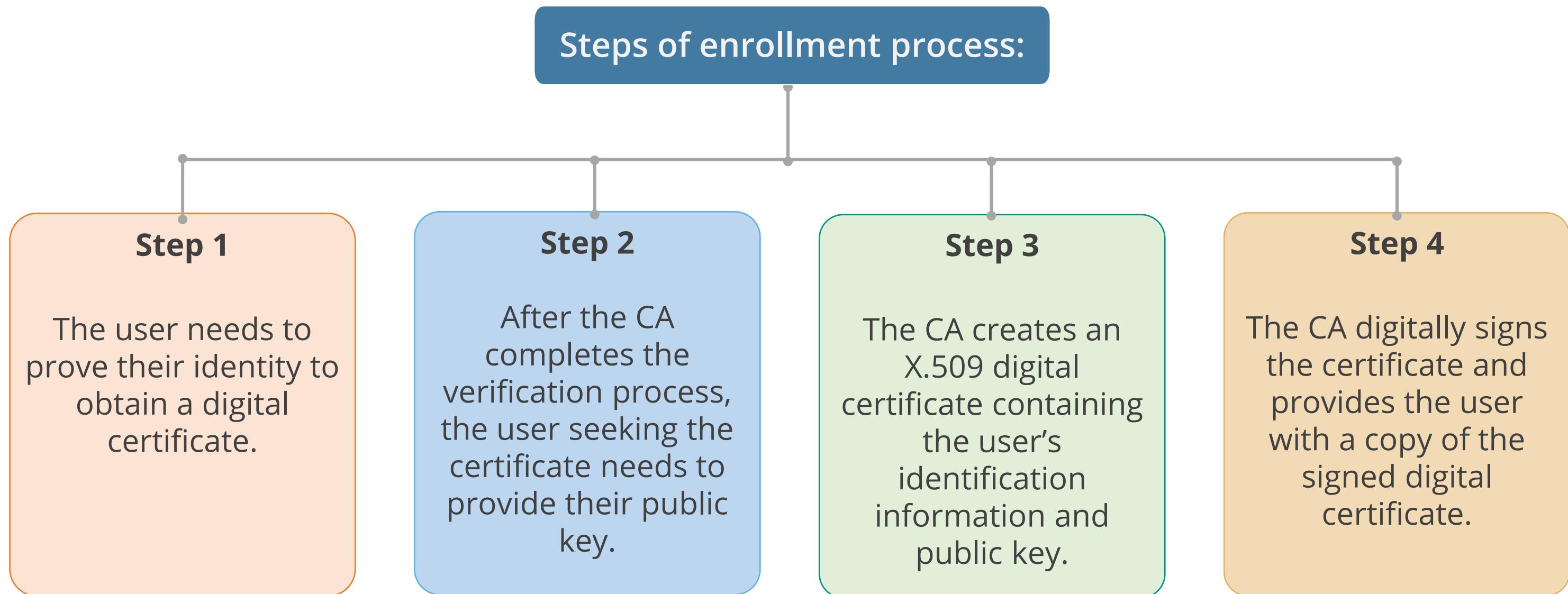


Enrollment Process

When a user wants to obtain a digital certificate, the user must first prove their identity to the CA in some manner. This process is called enrollment.



Enrollment Process



Verification Process

When a user receives a digital certificate from a person with whom they wish to communicate, they must verify if:

The digital signature of
the CA is authentic

The certificate contains
the trusted data

The CA is trusted
by the user

The certificate is not
listed on a certificate
revocation list (CRL)



Revocation Process

Occasionally, a certificate authority needs to revoke a certificate. This might occur because:



Certificate Revocation Lists (CRLs)

- CRLs are published lists of certificates revoked by their issuing CA before their expiration date.
- They contain the serial numbers of certificates issued by a CA that have been revoked, along with the date and time the revocation took effect.

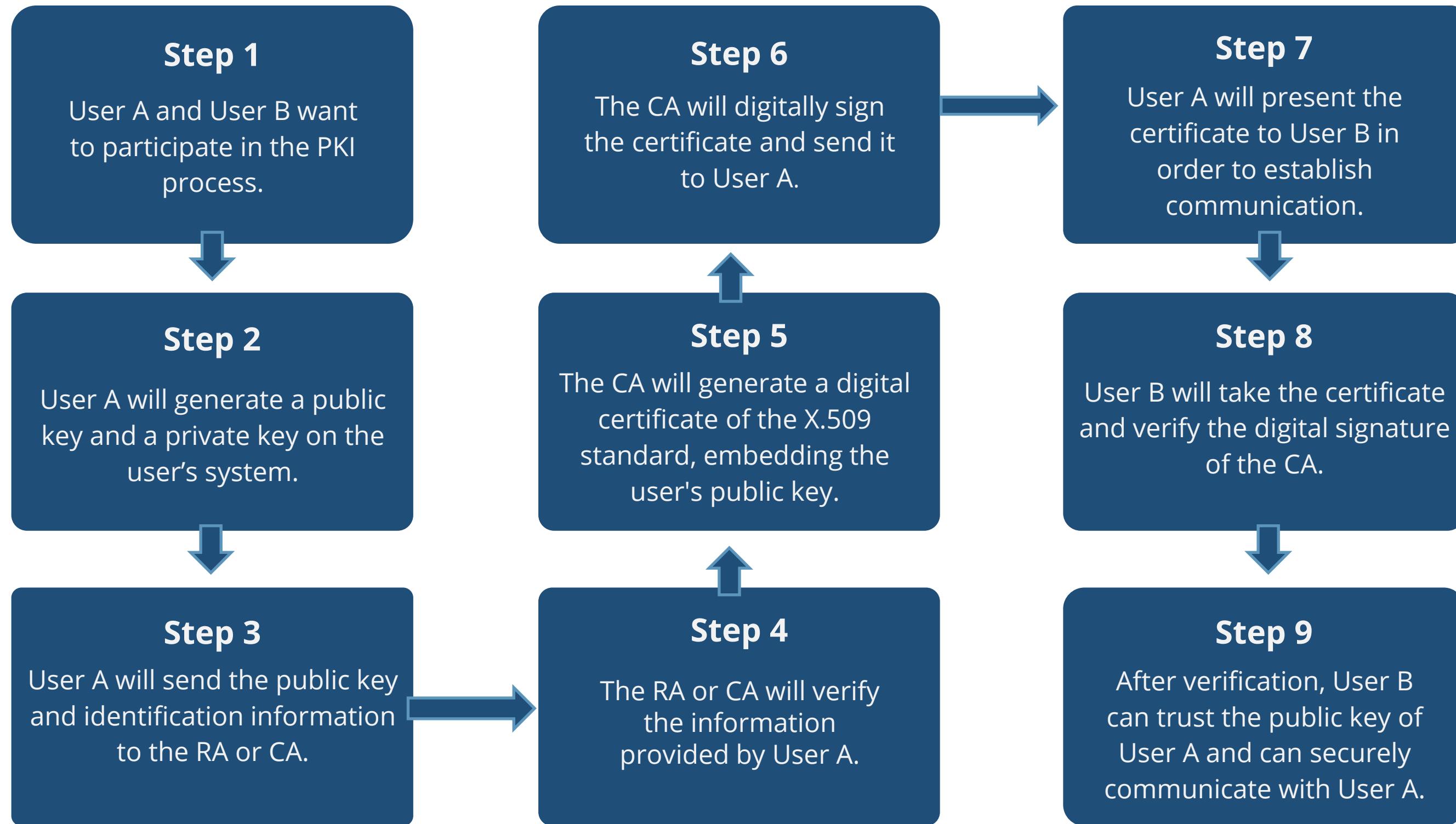


Online Certificate Status Protocol (OCSP)

- It carries out real-time validation of certificates and reports it back to the user.
- It checks the CRL that is maintained by the CA.



PKI Process

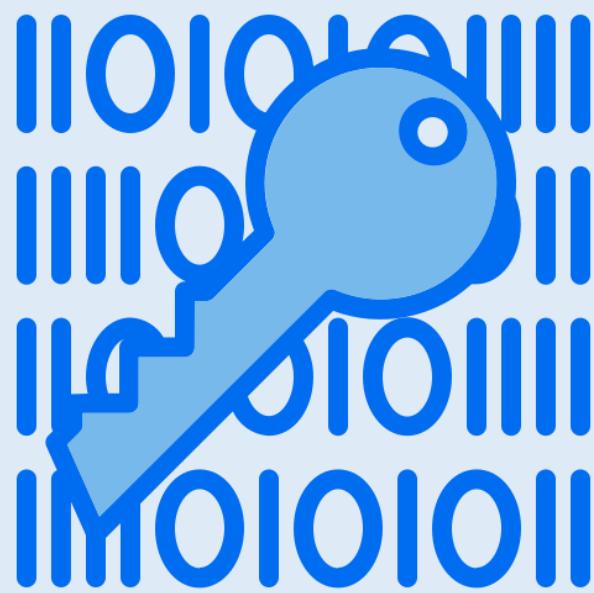


TECHNOLOGY

Key Management

Key Management

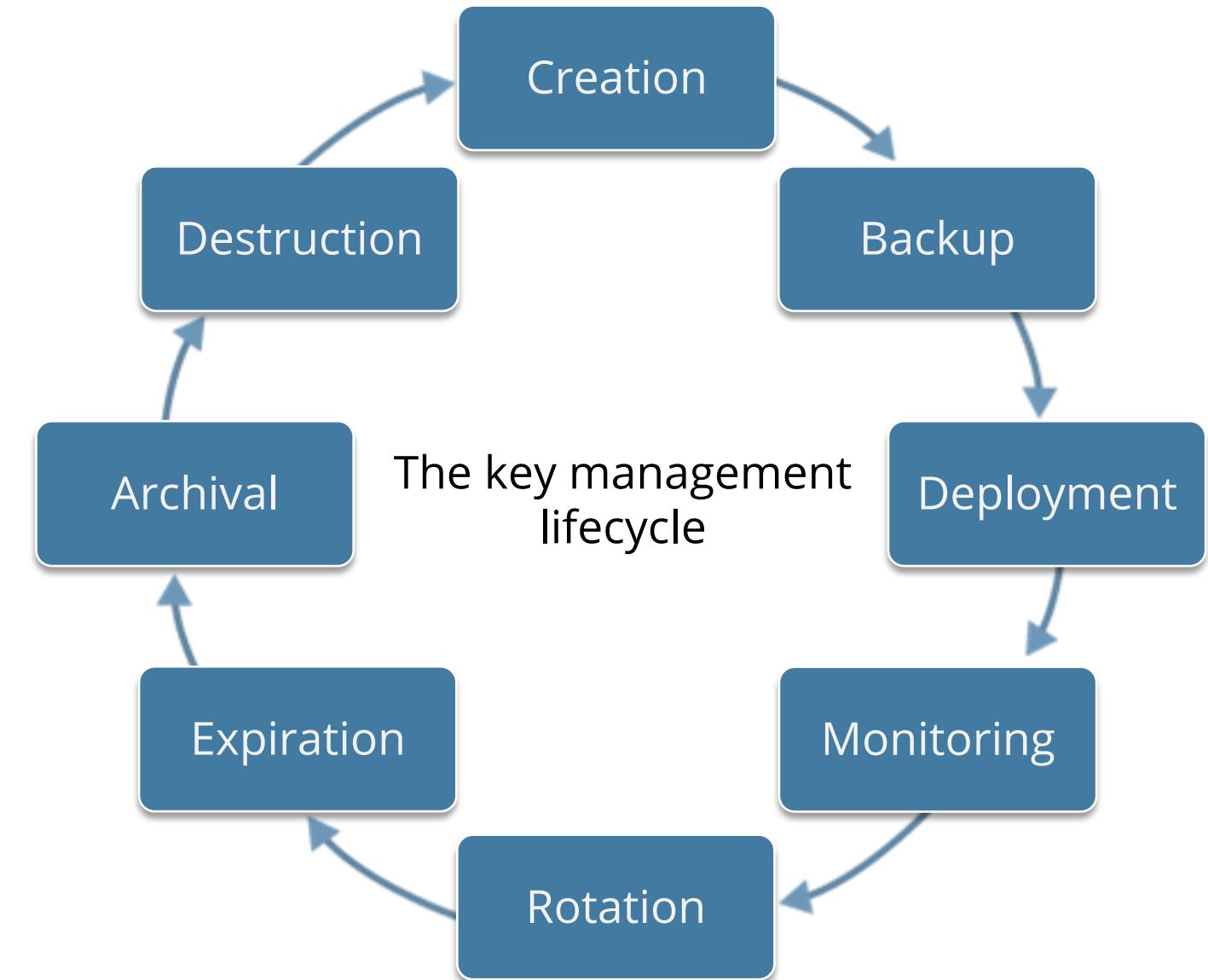
This is the most challenging part of cryptography and can be handled manually or automatically.



- Key management includes:
 - Generating, destroying, and recovering keys
 - Protecting keys against capturing, modification, corruption, or disclosure to unauthorized individuals
 - Regularly updating keys and distributing the right entities
 - Taking backup copies and adopting multi-party key recovery.
- Key distribution protocols (asymmetric) include:
 - RSA
 - Diffie-Hellman
- The Kerberos Key Distribution Center (KDC) is an example of automated key management.

Key Management Principles and Lifecycle

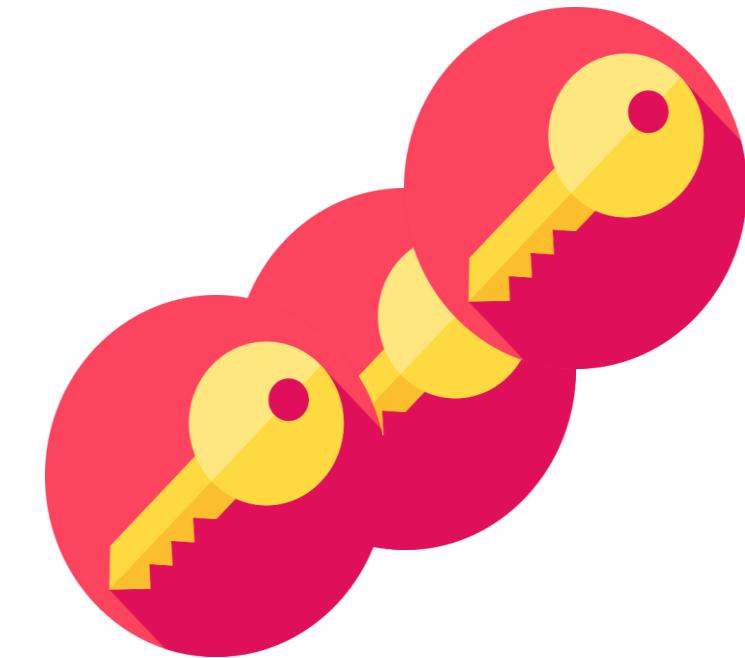
- The keys should be:
 - Stored and transmitted by secure means
 - Random
 - Properly destroyed at the end of their lifetime
 - Long enough to provide the necessary level of protection
- The key's lifetime should correspond with the sensitivity of the data it is protecting.



Key Stretching

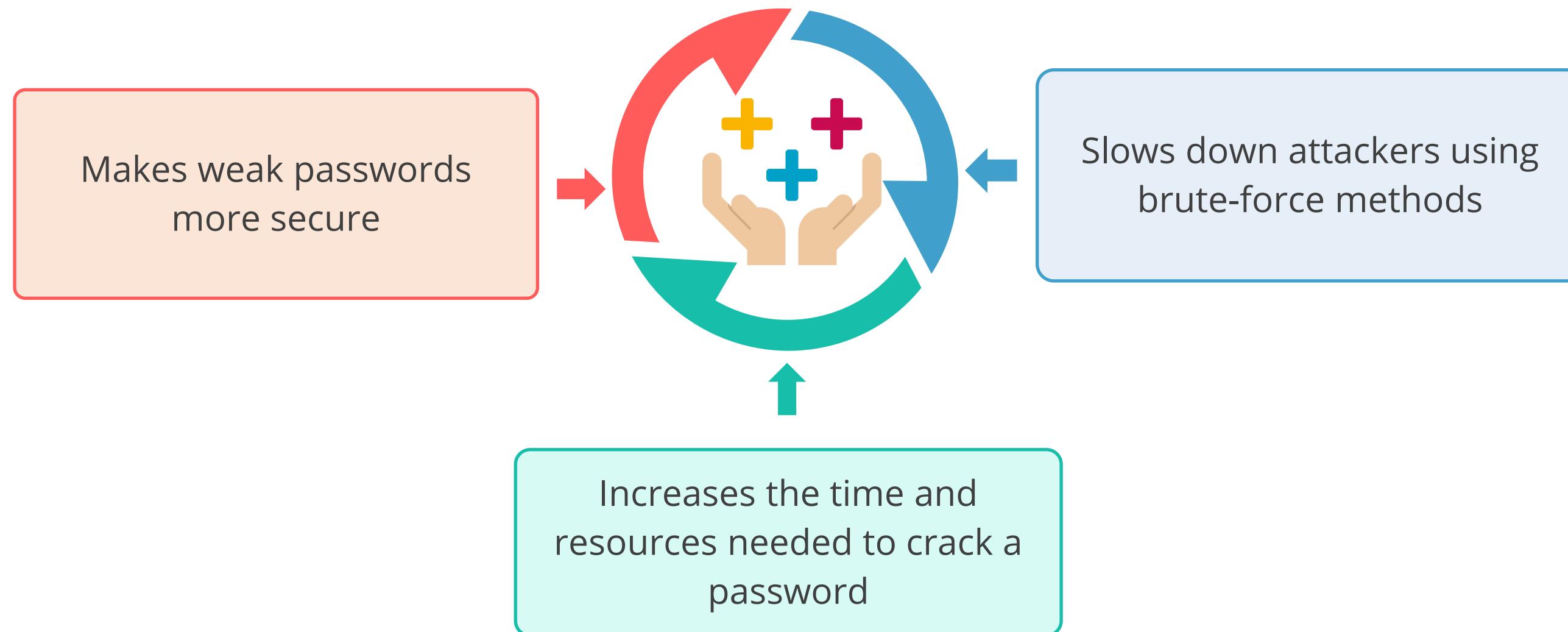
Key stretching, also known as key strengthening, is a cryptography technique that makes weak keys, particularly passwords, more secure.

- This involves running the weak key through a special function multiple times, transforming it into a longer and more complex key.
- This makes it significantly harder for attackers to crack using brute-force methods.
- Key stretching is like stretching taffy: you start with a small piece (a weak key) and pull it repeatedly (apply the function), making it longer and harder to break (resulting in a stronger key).

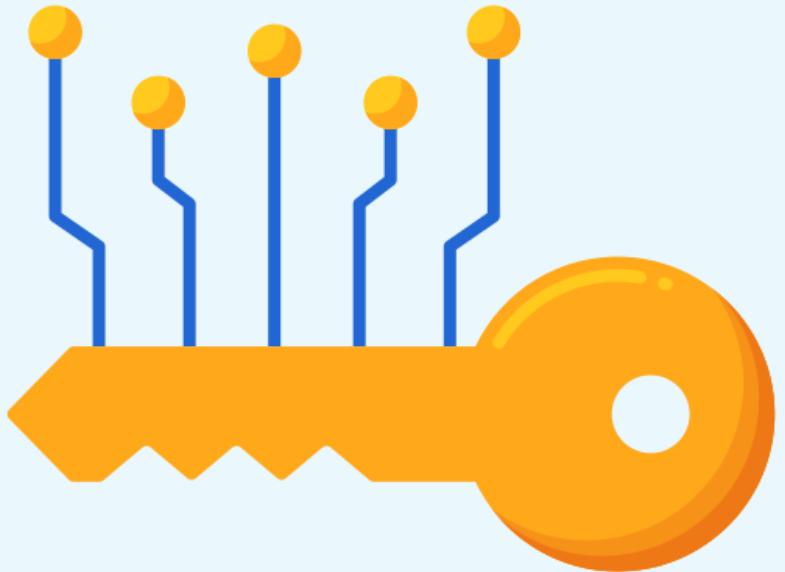


Adding random data to a password before inputting it into the key stretching function is called *salting*.

Benefits of Key Stretching



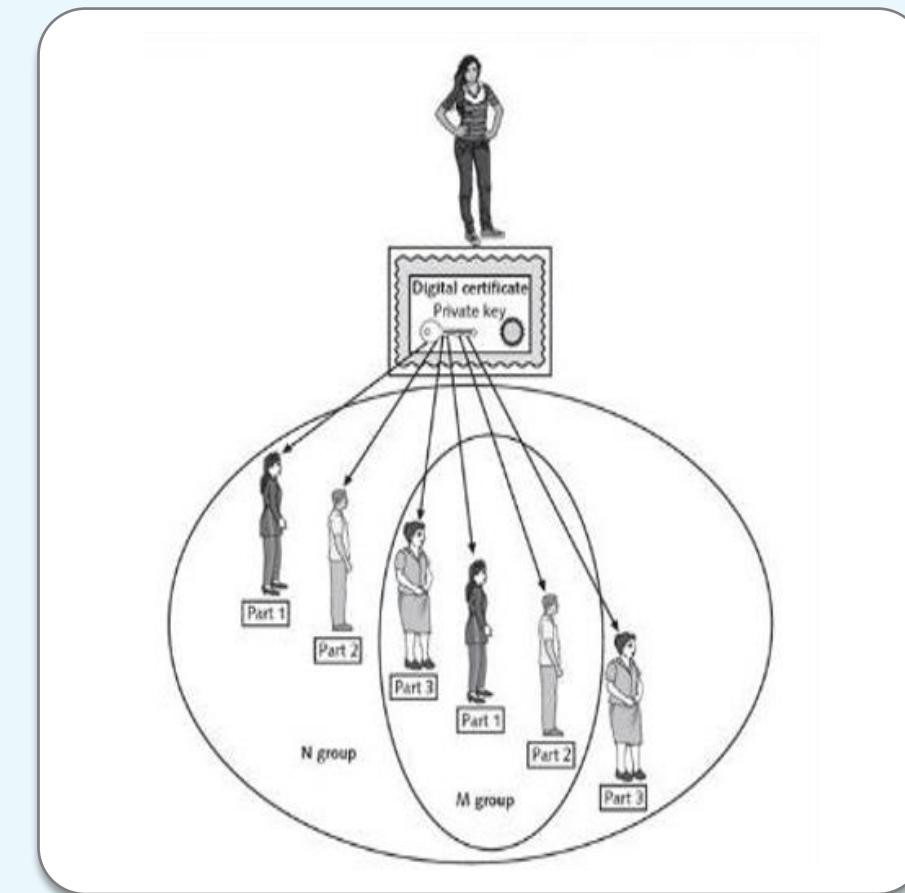
M of N Control



- It is a tool that helps recreate private and public key material from a backup.
- The key material is backed up and mathematically distributed across several systems or devices.
- Implementing three out of eight controls would require three people out of the eight assigned as key escrow recovery agents to work together to retrieve a single key from the key escrow database.
 - This illustrates that M is always less than or equal to N .

M of N Control

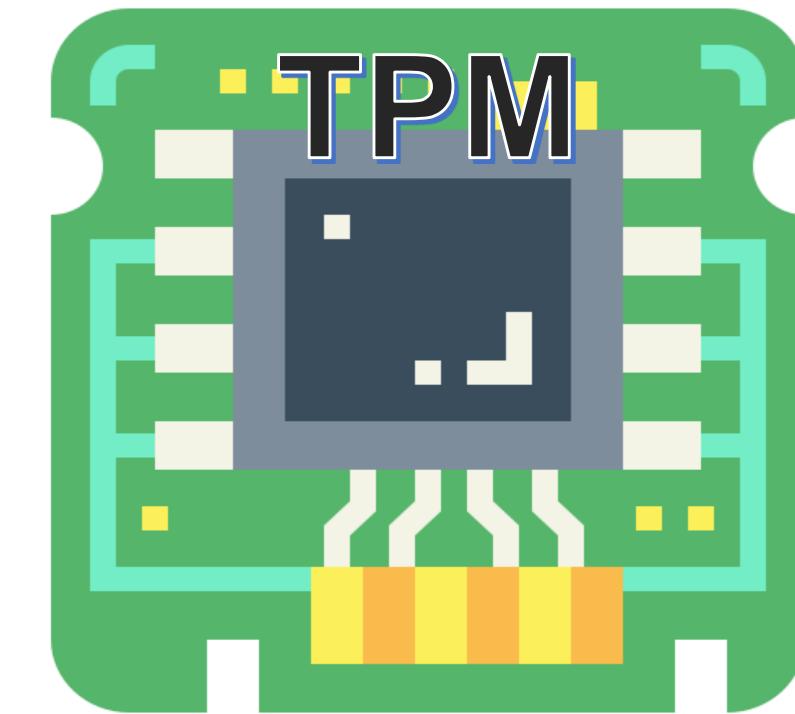
- M of N control requires a minimum number of agents (M) out of the total number of agents (N) to work together to perform high-security tasks.
- This is a backup process for public and private key material across multiple systems or devices.



Trusted Platform Module (TPM)

TPM is a hardware chip on the computer's motherboard that stores cryptographic keys used for encryption.

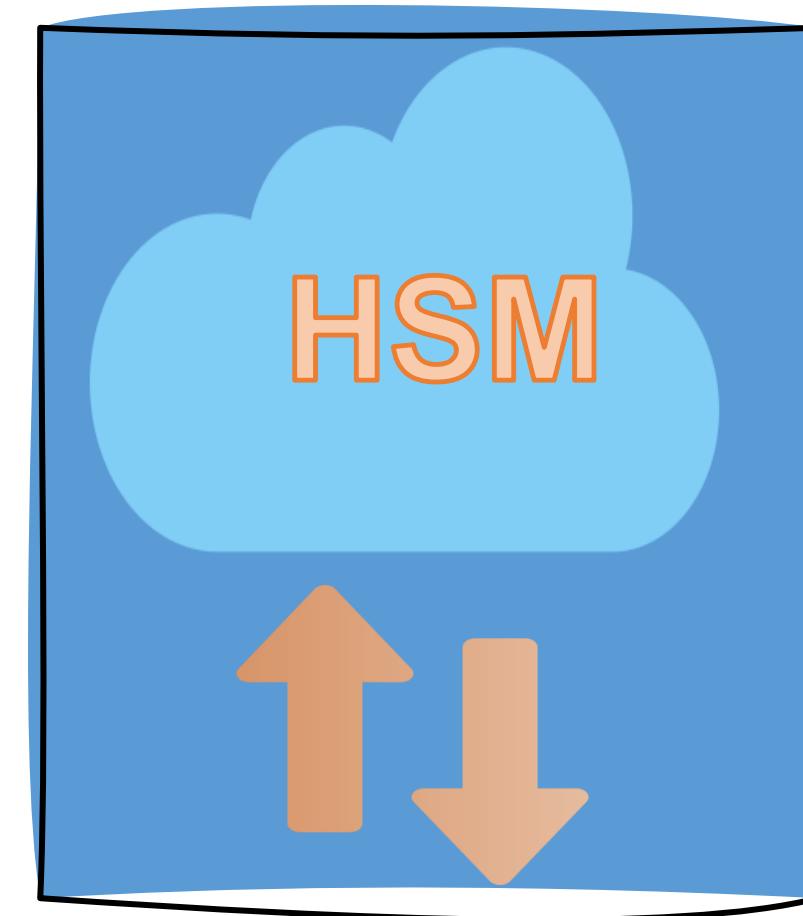
- Once enabled, TPM provides full disk encryption capabilities, keeping hard drives locked or sealed until the system completes a verification or authentication process.
- The TPM includes a unique RSA key burned into it, which is used for asymmetric encryption.
- Additionally, it can generate, store, and protect other keys used in the encryption and decryption process.



Hardware Security Model (HSM)

An HSM is a security device added to a system to manage, generate, and securely store cryptographic keys.

- High-performance HSMs are external devices connected to a network using TCP/IP.
- Smaller HSMs come as expansion cards installed within a server or as devices plugged into computer ports.



HSM vs. TPM

Sl. No	Parameter	HSM	TPM
1	Focus	Focuses on securely storing and managing cryptographic keys	Focuses on protecting the overall security and integrity of a computing platform
2	Hardware vs. Software	Is a dedicated hardware device built with tamper-resistant features, ensuring the physical security of keys	Is an integrated chip on a computer motherboard, offering hardware-based security but less physical isolation
3	Key management	Offers advanced key management features like secure key generation, secure storage, and access control mechanisms	Stores limited keys and performs key operations but primarily relies on software for key management

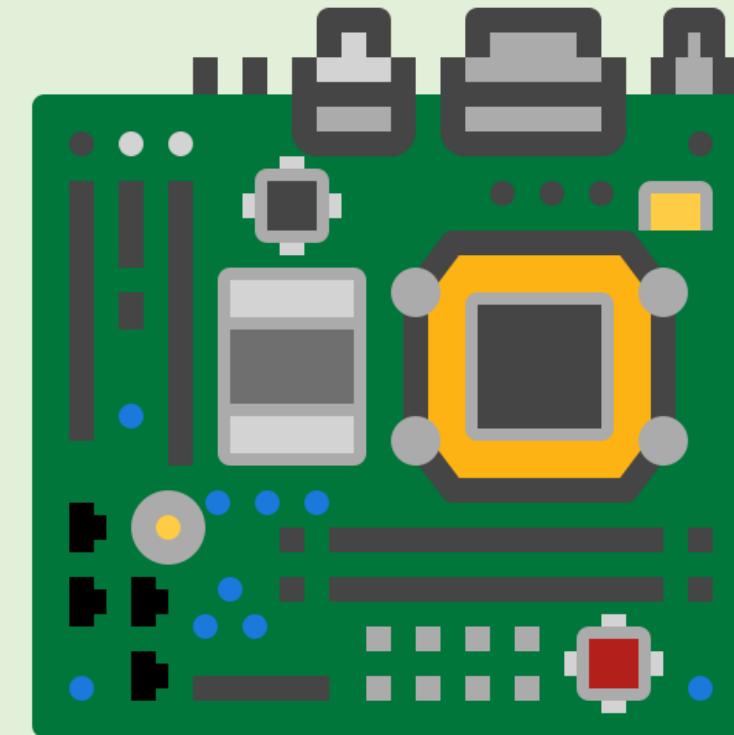
HSM vs. TPM

Sl. No	Parameter	HSM	TPM
4	Performance	Offers higher performance for cryptographic operations due to dedicated hardware	Performance varies depending on the platform and TPM version but may not be as high as dedicated HSMs
5	Cost	More expensive due to the dedicated hardware and advanced features	Is included in modern computers at little or no additional cost
6	Usage	<ul style="list-style-type: none">Environments requiring high security, such as banking, healthcare, and governmentProtection for sensitive data, such as payment card information, medical records, and classified informationOperations involving large-scale cryptography and demanding high performance	<ul style="list-style-type: none">Enhancing platform security for personal computers and serversEnabling features like secure boot, disk encryption, and multi-factor authenticationMeeting regulatory compliance requirements related to data security

Secure Enclave

This is a dedicated hardware component built into modern processors in many smartphones, tablets, and computers.

- It acts like a mini-fortress within the central processor, designed to protect the most sensitive data and cryptographic operations.
- This microprocessor has its own boot process and runs a separate operating system from the primary device, effectively segregating it.
- It resists tampering and prevents its data from being accessed through any means other than strict protocol.
- Its unique hardware and firmware are inextricably tied together, ensuring that a breach in one does not lead to a vulnerability in the other.



Functioning of Secure Enclave

Physical isolation

- It is physically separated from the main processor, creating a secure environment for sensitive tasks.
 - This isolation makes it much harder for attackers to access or tamper with the data stored or processed within the enclave.

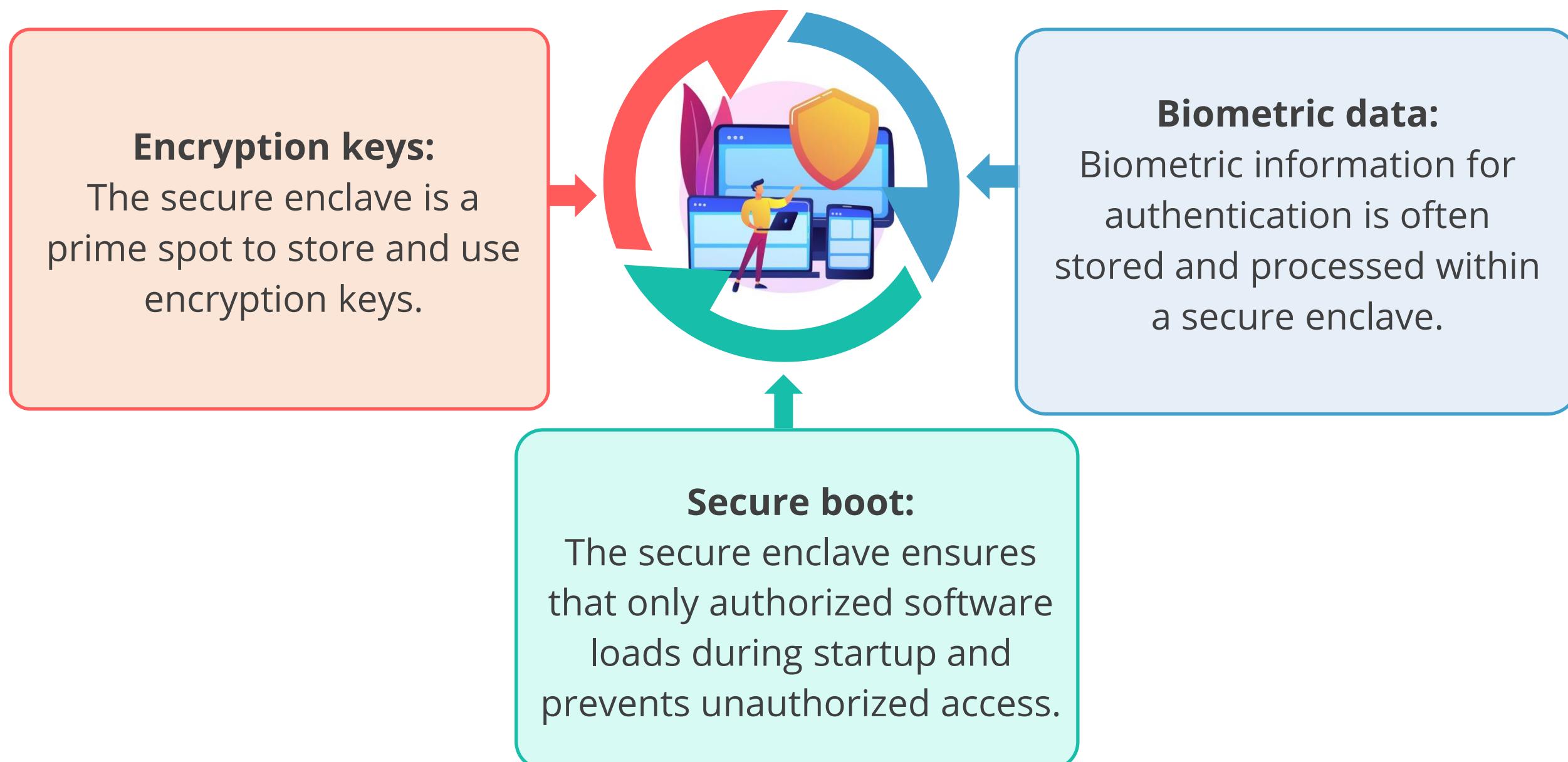
Protected memory

- It has its own dedicated memory space, preventing unauthorized access to sensitive information from the main system memory where malware or other threats might reside.

Secure execution environment

- The secure enclave operates with its own operating system or firmware for security, restricting code execution to authorized processes and minimizing vulnerability risks.

What Does Secure Enclave Protect?



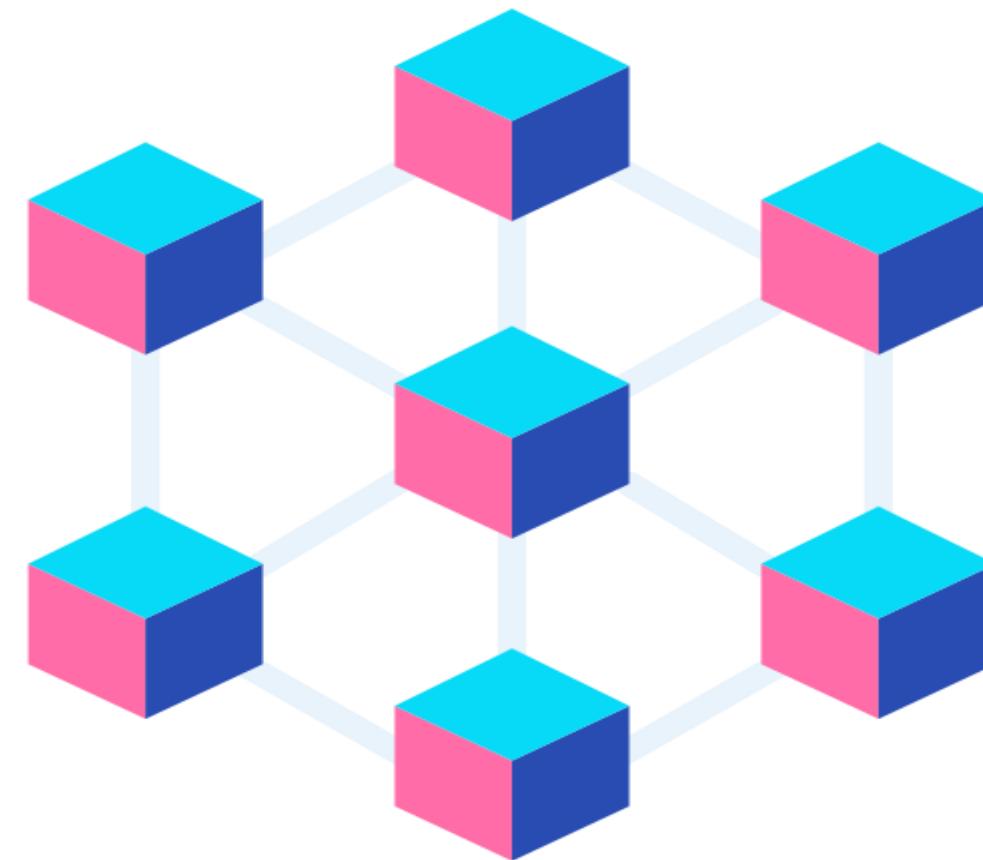
TECHNOLOGY

Blockchain and Open Ledger

Blockchain

Blockchain technology offers a secure, decentralized method for recording transactions on a digital ledger distributed across multiple computers.

- Blockchain operates as a decentralized database to enhance security and minimize failures.
- Each block links securely to its predecessor, validated and approved by network consensus, while unique cryptographic keys protect each entry, ensuring data integrity and immutability on the network.



Blockchain

Components

- Blocks: Each block stores critical information, such as transaction details.
- Chain: Blocks are linked chronologically to form a chain.
- Security: Cryptography secures the blocks, making it extremely difficult to tamper with the information.

Key features

- Decentralized: No single individual or group controls the information; every user has access to their own copy.
- Immutable: Once information is added, it cannot be changed.
- Transparent: All information on the blockchain is accessible to any viewer.

Applications of Blockchain



Payment processing and money transfer

Enables fast transactions and reduces banking fees



Healthcare

Manages clinical trial data and electronic records while ensuring regulatory compliance



Monitoring of supply chains

Improves supply chain efficiency by tracking goods and identifying real-time inefficiencies



Digital ID

Enhances security and privacy in identity management, ensuring user control over data access



IOT network management

Regulates IoT networks, identifies connected devices, and monitors their activities



Data sharing

Secures and facilitates the movement of data across industries

Blockchains Concerns

Malware and phishing attacks

Loss of private keys through attacks can block access to blockchain assets

Privacy concerns

Public blockchains risk exposing transaction details and account balances

Centralization

Despite its decentralized ideal, blockchain often ends up being controlled by a small number of entities

Governance

Unclear governance can complicate decision-making and maintenance of the network

Quantum computing

Blockchain encryption may be vulnerable to future quantum computing technologies

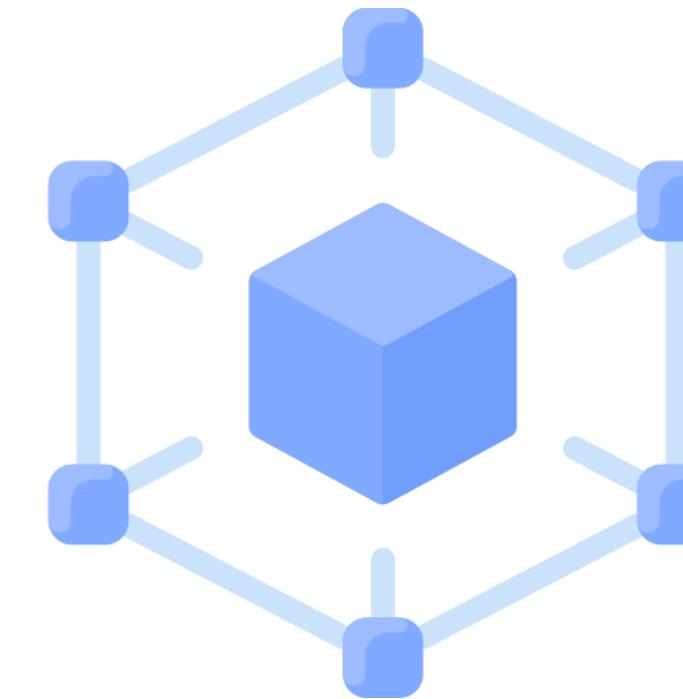
Scalability

As more users join, the blockchain can suffer from slow transaction times and network congestion

Open Ledger

An open ledger in blockchain functions as a public notebook, making it possible for everyone to view crucial transactions such as money transfers and contracts.

The open public ledger is fundamental to the blockchain, recording every transaction and allowing real-time access and verification by all network participants.



The openness of the blockchain ledger not only fosters transparency but also enhances security and trust among users by allowing real-time verification and auditing of transactions.

Benefits of Open Ledger

Decentralization

The ledger is decentralized, with copies distributed across multiple network nodes, enhancing reliability and accessibility

Security

Due to its decentralized and cryptographic structure, tampering with the ledger is significantly challenging

Transaction processing

Transactions are broadcasted to the network, verified by participants, and recorded following predefined blockchain rules

Consensus mechanisms

Consensus mechanisms like Proof of Work or Proof of Stake ensure the ledger's accuracy and integrity

Immutable and chronological

Transactions, once validated and recorded, are permanently embedded in the ledger in chronological order

Transparency

The ledger's openness permits anyone to verify transactions independently, promoting trust and accountability

Key Takeaways

- Information security is crucial within an organization for protecting data and ensuring business continuity.
- Deploying various security controls based on organizational risk helps tailor defenses to specific threats.
- Gap analysis plays a significant role in achieving business goals by identifying and addressing security weaknesses.
- Change management is essential for maintaining the confidentiality, integrity, and availability of organizational information, ensuring robust security practices.
- The concept of zero trust is important in today's security landscape, forming the foundation for modern cybersecurity strategies.

