Unit 1

Introduction and Classical Ciphers

(7 Hours)

1.4. Security: Computer Security, Information Security, Network Security, CIA Triad, Cryptography, Cryptosystem, Cryptanalysis, Security Threats and Attacks, Security Services, Security Mechanisms

1.5. Classical Cryptosystems: Substitution Techniques: Ceasar, Monoalphabetic, Playfair, Hill, Polyalphabetic ciphers, One-time pad Transposition Techniques: Rail Fence Cipher

1.6. Modern Ciphers: Block vs. Stream Ciphers, Symmetric vs. Asymmetric Ciphers

Sanjeev Thapa, Er. DevOps, SRE, CKA, RHCSA, RHCE, RHCSA-Openstack, MTCNA, MTCTCE, UBSRS, HEv6, Research Evangelist

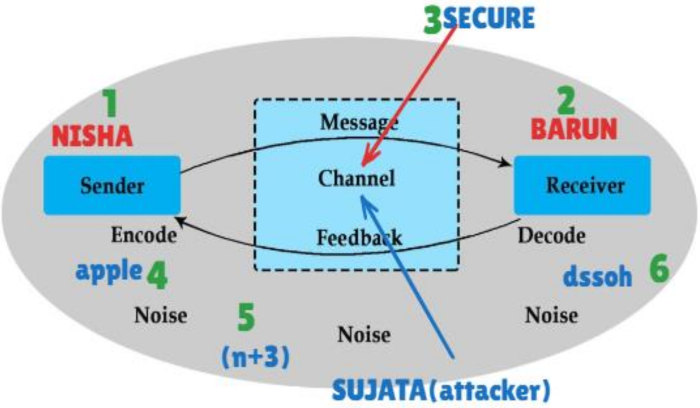
Security

🔐 What is Security?

Security refers to the protection of systems, data, networks, and resources from unauthorized access, misuse, modification, or destruction.

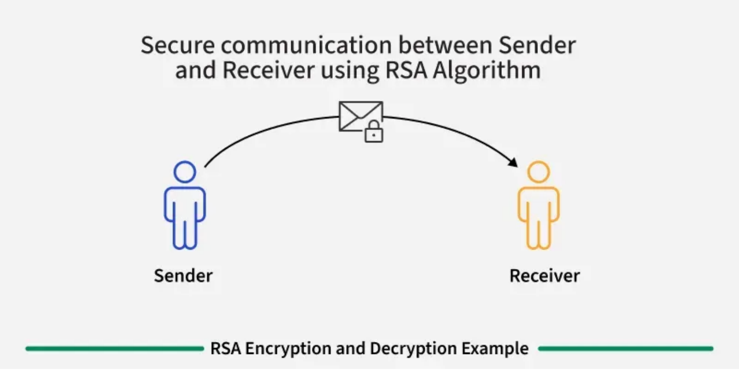
In computing, **security ensures that information and technology resources remain:**

- **Confidential** (only authorized people can access)
- **Accurate & Unchanged** (integrity)
- **Available** when needed (availability)



Security applies to:

- Computer systems
- Information/data
- Networks
- Users and processes


Secure communication between Sender and Receiver using RSA Algorithm
Sender
Receiver
RSA Encryption and Decryption Example

Formal definition:

Security is the practice of defending information and systems from threats and attacks to ensure confidentiality, integrity, and availability.

🔒 Why is Security Needed?

Security is essential for multiple reasons:

1 To Protect Sensitive Information

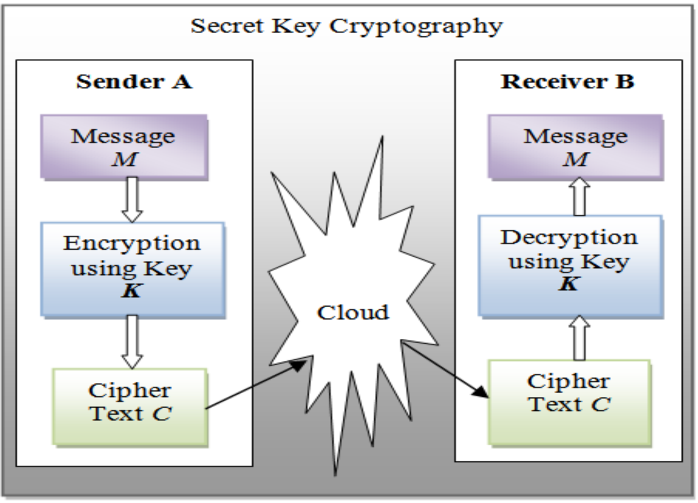
Prevent unauthorized people from seeing private or confidential data.
Example:
Bank account details, passwords, exam results, personal identity data.

2 To Maintain Data Integrity

Ensure data is not intentionally or accidentally changed.
Example:
Medical records must remain accurate; financial transactions must not be altered.

3 To Ensure System and Service Availability

Security protects systems from failures, attacks, or downtime.
Example:
Servers must resist DoS attacks so websites remain online.



4 To Prevent Unauthorized Access

Only authorized users should access systems and data.
Example:
Login authentication, role-based access control.

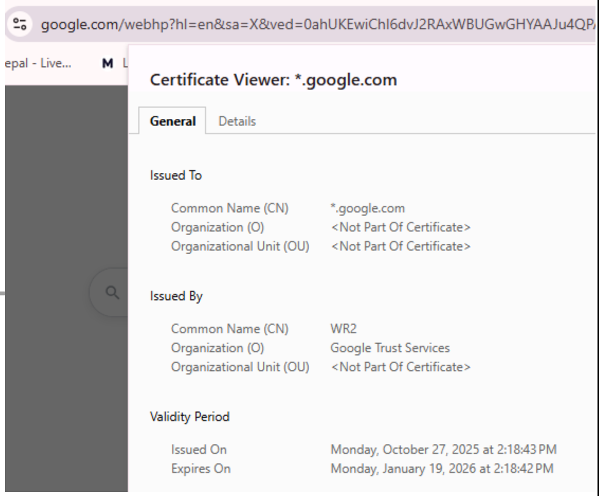
5 To Protect Against Cyber Attacks

Security guards against:

- Viruses
- Worms
- Trojans
- Ransomware
- Hacking attempts
- Man-in-the-middle attacks

6 To Build Trust in Digital Systems

Users must trust the system for secure online banking, e-commerce, cloud storage, etc.



google.com/webhp?hl=en&sa=X&ved=0ahUKEwiChl6dvJ2RAxWBUGwGHYAAJu4QP

Certificate Viewer: *.google.com

Issued To

Common Name (CN)	*.google.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	WR2
Organization (O)	Google Trust Services
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, October 27, 2025 at 2:18:43 PM
Expires On	Monday, January 19, 2026 at 2:18:42 PM

7 To Comply with Legal and Ethical Requirements

Many sectors (banking, healthcare, government) are legally required to secure their systems and data.

8 To Prevent Financial Loss

Security breaches can lead to:

- Theft of money
- Loss of business
- Repair costs
- Legal penalties

Step / Action	Terminal Command / Example	Security Concept Involved	What Happens / Why Needed
https://killercoda.com/killer-shell-cka/scenario/playground			
1. Create a file	*cat > file.txt* *hello this text*	File Creation	User creates a plaintext file using basic Linux command.
2. Default file permissions	*ls -l file.txt → -* *rw-r--r--*	**Confidentiality (risk)**	Others can read the file; data is not private.

Step / Action	**Terminal Command / Example**	**Security Concept Involved**	**What Happens / Why Needed**
https://killercoda.com/killer-shell-cka/scenario/playground			
3. Restrict access	*chmod 600 file.txt*	**Confidentiality (protection)**	Only the owner can read/write the file. Prevents unauthorized access.
4. Make file read-only	*chmod 400 file.txt*	**Integrity (protection)**	No one can modify the file (including owner unless permissions changed).
5. Detect changes using checksum	*sha256sum file.txt*	**Integrity (verification)**	Hash value ensures file hasn't been altered. If hash changes → file tampered.
6. Example of modification	*Another user runs:* *echo "hacked" >> file.txt*	**Threat: Integrity Attack**	File content changes → unauthorized modification.
7. Availability risk (accidental deletion)	*rm file.txt*	**Availability Issue**	File can be lost due to mistakes or attacks.
8. Create backup	*cp file.txt ~/Backup/file.txt*	**Availability (protection)**	Ensures file is still accessible even if primary file is lost.
9. Check who accessed system	*last*	**Authentication Monitoring**	Helps monitor who logged in; detects suspicious activity.
10. Verify file authenticity after download	*sha256sum downloaded_file.deb*	**Integrity & Trust**	Ensures downloaded file is not corrupted or infected.
11. Protect system on public WiFi	*sudo ufw enable*	**Network Security / Confidentiality**	Firewall blocks unwanted connections.

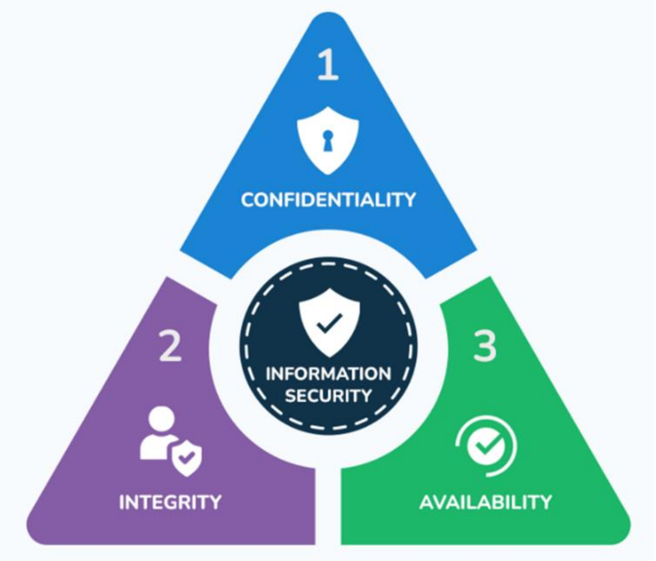
Step / Action	Terminal Command / Example	Security Concept Involved	What Happens / Why Needed
https://killercoda.com/killer-shell-cka/scenario/playground			
12. Encrypt sensitive file	*openssl enc -aes-256-cbc -salt -in file.txt -out file.enc*	**Confidentiality via Cryptography**	Even if someone copies the file, they cannot read it.
13. Decrypt encrypted file	*openssl enc -aes-256-cbc -d -in file.enc -out file_new.txt*	**Restoring Availability**	Authorized user reads file safely.

Computer Security vs Information Security vs Network Security

Criteria	Computer Security	Information Security	Network Security
Definition	Protects computer systems (hardware, OS, software) from unauthorized access or damage.	Protects *information/data* in any form (digital, physical, printed) from unauthorized access, alteration, or destruction.	Protects data *during transmission* across networks and safeguards network devices.
Focus Area	Individual computers, devices, endpoints.	Data confidentiality, integrity, and availability.	Communication channels, network traffic, routers, switches, Wi-Fi, etc.
Main Goal	Ensure system is secure and functions correctly.	Keep data secure, accurate, private, and accessible.	Protect network infrastructure and secure data in motion.
What is Protected?	Operating system, hard disks, applications, local files.	Sensitive data, records, documents, credentials.	Packets, network connections, network devices, communication pathways.

Criteria	Computer Security	Information Security	Network Security
Threat Examples	Malware, unauthorized logins, OS vulnerabilities.	Data breach, data tampering, insider misuse, data theft.	Sniffing, spoofing, MITM attack, DoS attack, ARP poisoning.
Techniques Used	Antivirus, OS hardening, user authentication, access control, disk encryption.	Encryption, hashing, access control, data classification, backups.	Firewalls, IDS/IPS, VPN, SSL/TLS, IPSec, packet filtering.
Scope	Narrow (device-level protection).	Broad (data-level protection).	Network-level protection across multiple devices.
Example	Protecting a laptop from viruses and unauthorized users.	Encrypting exam marks database or protecting students' personal details.	Securing data while submitting an online form via HTTPS or preventing Wi-Fi attacks.
Responsible Team	System administrators, desktop security team.	Information security team, compliance team.	Network administrators, cybersecurity engineers.
Relation	Component of overall system security.	Superset that includes computer & network security.	Overlaps with both but focuses only on network communication.

CIA Triad



The **CIA Triad** is the foundational model of information security. It consists of **three core principles**:

- **C – Confidentiality**
- **I – Integrity**
- **A – Availability**

These three ensure that information remains protected from unauthorized use, modification, and disruption.

1 Confidentiality

Definition:

Ensures that **only authorized users** can access information.
Prevents disclosure of data to unauthorized persons.

Examples:

- Passwords protect files from unauthorized access
- Encryption (AES, RSA) makes data unreadable to attackers
- Access control (file permissions: chmod 600)
- Secure communication (HTTPS, SSL/TLS)

Threats to Confidentiality:

- Unauthorized access
- Eavesdropping/sniffing
- Data leakage
- Shoulder surfing

2 Integrity

Definition:

Ensures that information remains **accurate, original, complete, and unaltered**.

Examples:

- Hash functions (SHA-256) verify file integrity
- Digital signatures ensure authenticity + no modification
- Checksums used when downloading software
- Version control to detect unauthorized changes

Threats to Integrity:

- Data tampering
- Unauthorized modification
- Malware altering files
- Accidental edits or deletion

3️⃣ Availability

Definition:

Ensures that information and systems are **accessible whenever required** by authorized users.

Examples:

- Backups to recover lost data
- Redundant systems (RAID, load balancers)
- Up-to-date antivirus & patches
- DoS attack protection
- Power backups & stable network

Threats to Availability:

- Hardware failure
- DoS/DDoS attacks
- System crashes
- Natural disasters
- Ransomware locking files

📌 CIA Triad Table Summary

Component	Meaning	Goal	Example
Confidentiality	Only authorized users access data	Privacy	Passwords, encryption
Integrity	Data remains accurate & unchanged	Trust	Hashing, digital signatures
Availability	Data/services available when needed	Access	Backups, DoS protection

CIA Triad lab scenarios.

🧪 TABLE 1: Confidentiality Lab Scenario

Step	Command / Action	Output / Observation	Security Concept
1. Create a file	echo "This is a secret message" > secret.txt	File created	Start of confidentiality scenario
2. Check default permissions	ls -l secret.txt → -rw-r--r--	File readable by others	Confidentiality is **not** ensured
3. Restrict permissions	chmod 600 secret.txt	-rw-------	Only owner can read/write → Confidentiality ensured
4. Optional encryption	openssl enc -aes-256-cbc -salt -in secret.txt -out secret.enc	Encrypted file created	Extra confidentiality layer

📜 TABLE 2: Integrity Lab Scenario

Step	Command / Action	Output / Observation	What It Proves
1. Create a file	echo "Student Marks: 86" > marks.txt	File created	Base file for integrity test
2. Generate hash	sha256sum marks.txt > marks.hash	Hash stored in marks.hash	Integrity baseline created
3. Modify file	echo "Student Marks: 56" > marks.txt	File changed	File integrity compromised
4. Verify integrity	sha256sum marks.txt vs cat marks.hash	Hash mismatch	Unauthorized modification detected

🗂️ TABLE 3: Availability Lab Scenario

Step	Command / Action	Output / Result	Security Concept
1. Create important file	echo "Project work: Cryptography lab" > project.txt	Project file created	Base for availability test
2. Create backup	cp project.txt project_backup.txt	Backup created	Ensures availability
3. Simulate deletion	rm project.txt	File deleted	Data unavailable
4. Restore backup	cp project_backup.txt project.txt	File restored	Availability maintained

🔐 TABLE 4: Combined CIA Triad Demonstration

Concept	**Command / Action**	**Observation**	**What It Shows**
Confidentiality	chmod 600 cia_demo.txt	Only owner can read/write	Data privacy ensured
Integrity	sha256sum cia_demo.txt > cia_demo.hash	Hash saved	File integrity baseline created
Integrity Test	Modify file: echo "hacked!" >> cia_demo.txt	File changed	Integrity broken
Integrity Verification	sha256sum cia_demo.txt	Hash mismatch	Modification detected
Availability	Backup: cp cia_demo.txt cia_demo_backup.txt	Backup exists	Data available even if lost
Availability Restore	Restore: cp cia_demo_backup.txt cia_demo.txt	File recovered	Availability preserved

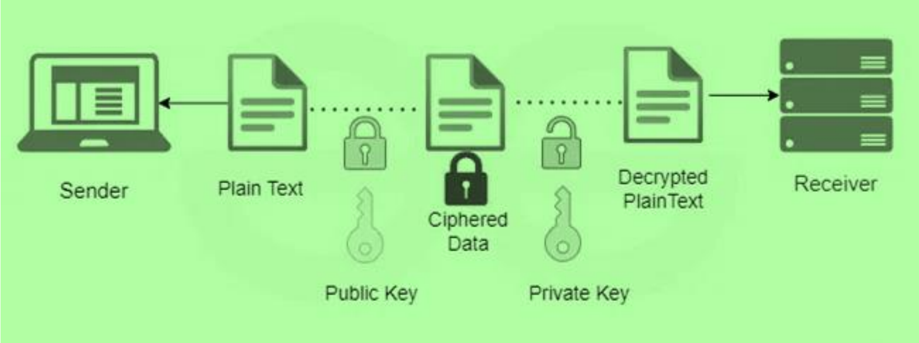
🏁 Summary Table: CIA Triad Concepts

CIA Component	**Meaning**	**Example in Lab**	**Purpose**
Confidentiality	Prevent unauthorized access	chmod 600, encryption	Protects privacy of data
Integrity	Ensure data is accurate & unchanged	Hash check (sha256sum)	Detects tampering or corruption
Availability	Ensure data is accessible when needed	Backup & restore	Prevents data loss and downtime

🔐 Cryptography

Sanjeev Thapa, Er. DevOps, SRE, CKA, RHCSA, RHCE, RHCSA-Openstack, MTCNA, MTCTCE, UBSRS, HEv6, Research Evangelist

- The **science of secret writing**.
- Converts **plaintext → ciphertext** (encryption) and **ciphertext → plaintext** (decryption).
- Uses mathematical algorithms and keys.
- Ensures:
  ✓ Confidentiality
  ✓ Integrity
  ✓ Authentication
  ✓ Non-repudiation



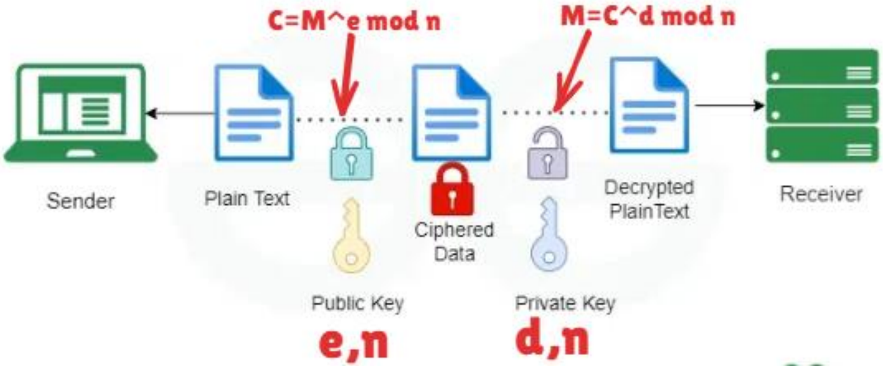
Example:
AES encrypts data so only authorized users can read it.

🧩 Cryptosystem

- A **complete framework** that supports secure communication.
- Includes:
  1. Plaintext
  2. Ciphertext
  3. Encryption algorithm
  4. Decryption algorithm
  5. Key(s)
  6. Key generation

Example: *RSA Cryptosystem* uses:

- Public key (e, n)
- Private key (d, n)
- Encryption: $C = M^e \bmod n$
- Decryption: $M = C^d \bmod n$

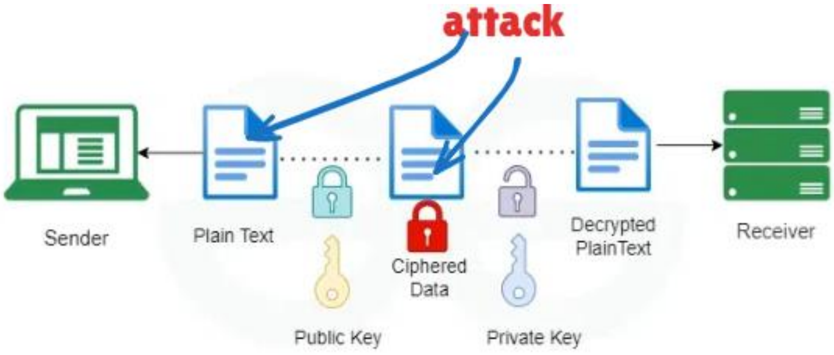


🕵️ Cryptanalysis

- The art/science of **breaking ciphers**.
- Goal: recover plaintext or key *without authorization*.
- Used by attackers *and* security professionals (ethical).

Types of Cryptanalysis Attacks:

- Ciphertext-only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Brute force attack

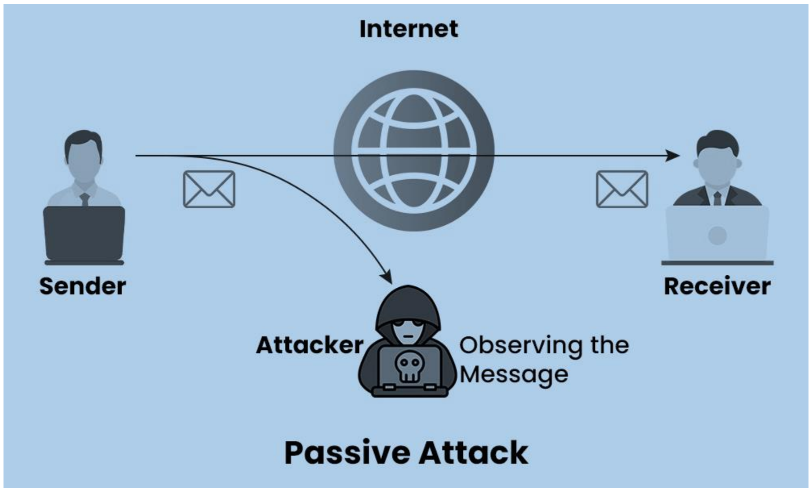


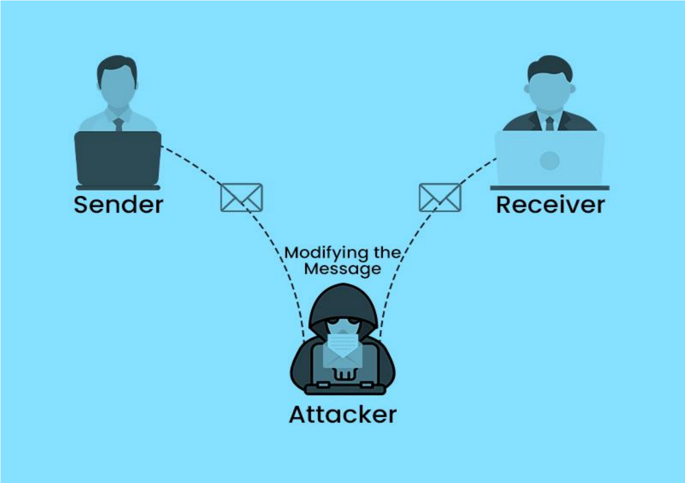
Example:
Trying all 25 keys in Caesar cipher to break encryption.

✅ 3. Summary Table (For Quick Revision)

Feature	Cryptography	Cryptosystem	Cryptanalysis
Focus	Protect data	Provide structure for encryption	Break or attack crypto
Users	Designers / security engineers	System architects	Attackers & analysts
Goal	Secure information	Establish secure communication	Find weaknesses
Output	Ciphertext, signatures	Full system (keys + algorithms)	Plaintext/key recovery
Nature	Constructive	Structural	Destructive / analytical

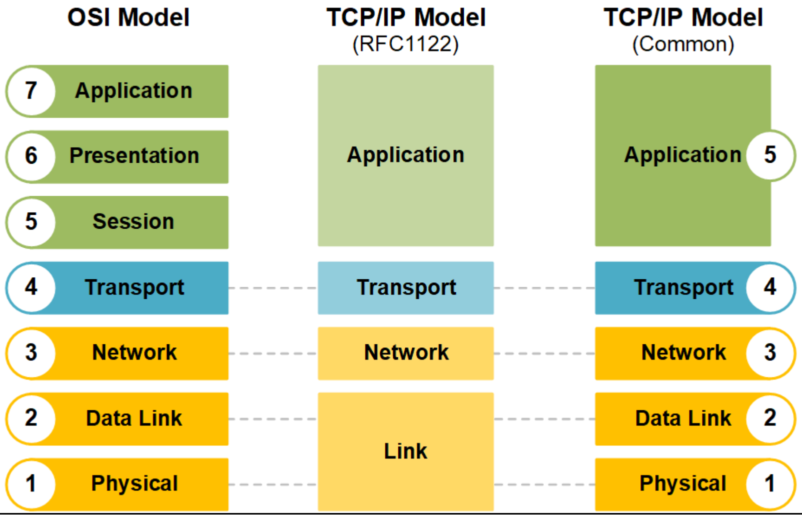
🧨 1. SECURITY THREATS & ATTACKS





Category	**Definition**	**Examples**	**Impact**
Passive Attacks	Attacker only *observes* data but does not modify it.	Eavesdropping, traffic analysis.	Loss of confidentiality.
Active Attacks	Attacker *modifies* data or disrupts the system.	Masquerading, DoS, replay attack.	Loss of integrity + availability.
Malware	Malicious software designed to damage or exploit systems.	Virus, worm, trojan, ransomware.	Data loss, corruption, system slowdown.
Social Engineering	Manipulating people to reveal confidential info.	Phishing, fake login pages, phone scams.	Credential leakage, identity theft.
Network Attacks	Attacks on communication channels or networks.	MITM, ARP spoofing, sniffing, session hijacking.	Data theft, impersonation.
Web Attacks	Target web apps/services.	SQL Injection, XSS, CSRF.	Unauthorized access, data breach.
Physical Threats	Damage to hardware.	Theft, fire, power failure.	Total data/system loss.

2. SECURITY SERVICES



Security Services are *what security SHOULD achieve* (OSI model).

Security Service	**Goal**	**Description**	**Example**
Confidentiality	Privacy	Prevent unauthorized access to data.	Encryption (AES), file permissions.
Integrity	Accuracy	Protect data from unauthorized modification.	Hashing (SHA-256), digital signatures.
Authentication	Identity verification	Check if user/system is genuine.	Password login, certificates.
Authorization / Access Control	Permission control	Decide what actions user can perform.	RBAC, ACL.
Non-Repudiation	Accountability	Sender cannot deny sending data.	Digital signatures.
Availability	Access	Ensure system/services are available when needed.	Backups, DoS protection.
Auditing / Accountability	Tracking	Record user and system activities.	System logs, audit trails.

⚙️ 3. SECURITY MECHANISMS

Security Mechanisms are *how security is implemented* (tools, techniques).

Security Mechanism	**Purpose**	**Real Example / Tool**
Encryption	Protect confidentiality	AES, RSA, TLS, SSH
Hash Functions	Ensure integrity	SHA-256, MD5 (deprecated)
Digital Signatures	Integrity + non-repudiation + authentication	RSA Signatures, DSA
Authentication Mechanisms	Verify identity	Passwords, OTP, biometrics, OAuth
Access Control	Allow/deny permissions	RBAC, ACL, file permissions (chmod)
Firewalls	Filter network traffic	UFW, iptables, hardware firewalls
Intrusion Detection/Prevention (IDS/IPS)	Detect attacks	Snort, OSSEC
Security Policies	Rules that define how systems must be used	Password policy, access rules
Cryptographic Protocols	Secure communication	SSL/TLS, IPSec, Kerberos
Physical Security	Protect hardware	Locks, CCTV, security guards
Backup & Recovery	Maintain availability	Rsync, cloud backup

✅ MCQs

1. Which of the following best describes *Confidentiality* in the CIA Triad?

A. Ensuring data is accurate
B. Ensuring data is available
C. Ensuring only authorized users can access data
D. Ensuring faster data processing

2. Which type of attack involves only monitoring or listening to network traffic?

A. DoS attack
B. Replay attack
C. Passive attack
D. Masquerading attack

3. Which of the following is an example of *Information Security*?

A. Protecting routers from attacks
B. Encrypting a student's mark-sheet
C. Restricting CPU access
D. Disabling unused network ports

4. A complete set of encryption/decryption processes, keys, and algorithms is called:

A. Cryptography
B. Cryptanalysis
C. Cryptosystem
D. Ciphertext

5. Which one is a symmetric key algorithm?

A. RSA
B. AES
C. Diffie-Hellman
D. ElGamal

6. Which service ensures that a sender cannot deny sending a message?

A. Authentication
B. Integrity

C. Non-repudiation
D. Authorization

7. Altering data during transmission is an example of which attack?

A. Replay attack
B. Traffic analysis
C. Data modification attack
D. Shoulder surfing

8. The primary purpose of *cryptanalysis* is to:

A. Design encryption algorithms
B. Break or analyze encryption without the key
C. Store secret keys
D. Manage digital certificates

9. Which of the following ensures the accuracy and consistency of data?

A. Integrity
B. Confidentiality
C. Availability
D. Redundancy

10. Which of the following is a *security mechanism*?

A. Confidentiality
B. Hashing
C. Availability
D. Non-repudiation

11. Which attack floods a system with traffic to make it unavailable?

A. MITM attack
B. DDoS attack
C. Phishing attack
D. Social engineering

12. A firewall primarily helps in ensuring:

A. Confidentiality only
B. Integrity only

C. Network security
D. Data recovery

13. The process of converting plaintext into ciphertext is known as:

A. Cryptanalysis
B. Decryption
C. Encryption
D. Key distribution

14. Which one is an example of *security service*?

A. Digital signature
B. Encryption algorithm
C. Authentication
D. Firewall installation

15. Which threat involves pretending to be another legitimate user or device?

A. Eavesdropping
B. Masquerading attack
C. Brute force attack
D. Virus infection

✅ **Answers**

1. C
2. C
3. B
4. C
5. B
6. C
7. C
8. B
9. A
10. B
11. B

12. C

13. C

14. C

15. B

🏛️ HISTORY OF CRYPTOGRAPHY

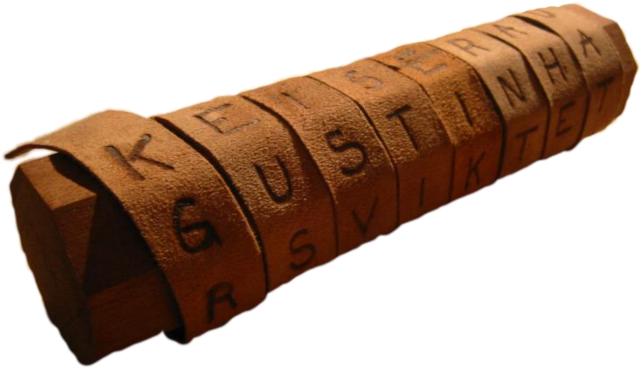
Cryptography is thousands of years old. Humans have always tried to **protect messages**, especially during **wars, diplomacy, politics, and military strategy**.
The evolution of cryptography can be divided into major time periods:

1️⃣ Ancient Civilizations (2000 BCE – 500 CE)

a) Egypt (2000 BCE)

- Oldest known cryptography found in **Egyptian hieroglyphs**.
- Used simple **symbol substitutions**.
- Purpose: **to hide religious or royal messages**.

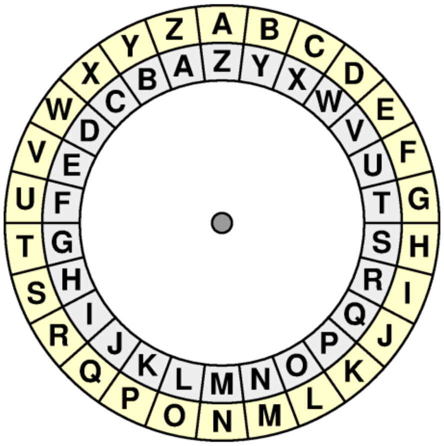
b) Spartan Scytale (600 BCE)



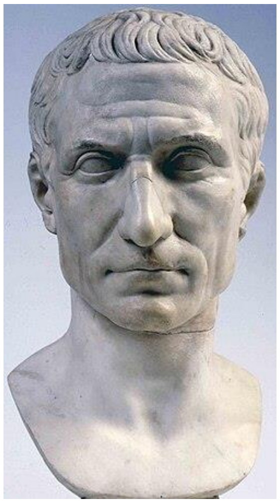
- Used by Spartan warriors.
- A **wooden rod with a strip of leather**.
- Message written across rod → unreadable when unwrapped → readable only on a rod of same size.
- One of the earliest **transposition ciphers**.

c) Ancient Hebrew Atbash Cipher (500 BCE)

- Simple substitution:
  A ↔ Z, B ↔ Y, C ↔ X, etc.
- Used in Biblical writings.


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

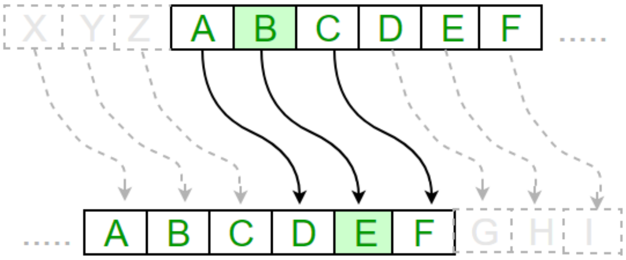
2 Roman Empire (100 BCE – 400 CE)



This is the most famous era in early cryptography, mainly because of **Julius Caesar**.

⭐ Caesar Cipher (Shift Cipher)

- Introduced by **Julius Caesar**, a Roman general and statesman.
- Used to send **military commands** secretly.
- Each letter shifted by **3 positions**:
  A→D, B→E, C→F
- Example:
  "ATTACK" → "DWWDFN"



Why it was effective at the time?

- Enemies were mostly illiterate.
- Writing systems were limited.
- Attackers lacked frequency analysis.

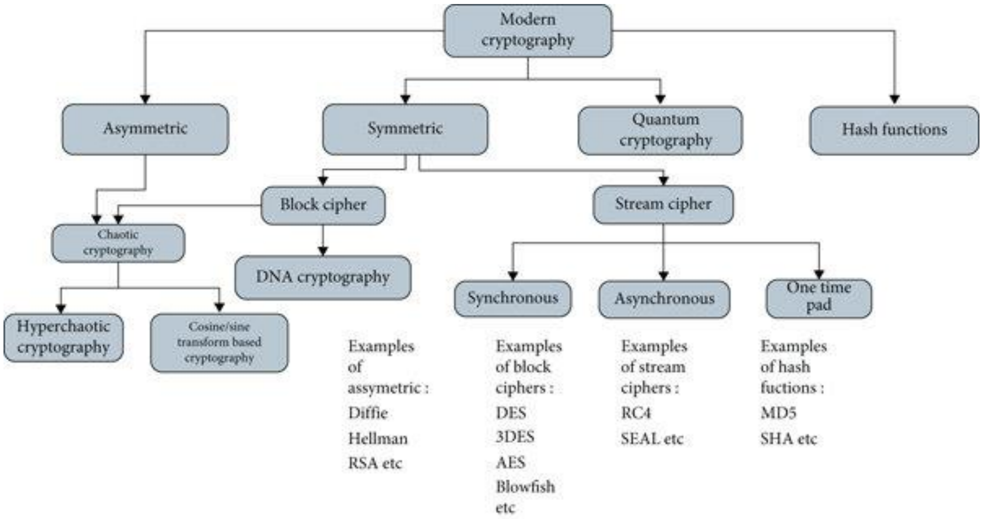
But today, it is easily broken by brute force.

3 Medieval Period (500 – 1500 CE)

a) Monoalphabetic Substitution (Arab Cryptographers)

- Arabs during the Islamic Golden Age studied **frequency analysis** .
- Scholar **Al-Kindi** (9th century) wrote the **first book on cryptanalysis**.
- This made simple substitution ciphers vulnerable.

4 Renaissance & Early Modern Cryptography (1500 – 1900)


Modern cryptography
Asymmetric
Symmetric
Quantum cryptography
Hash functions
Block cipher
Stream cipher
Chaotic cryptography
DNA cryptography
Synchronous
Asynchronous
One time pad
Hyperchaotic cryptography
Cosine/sine transform based cryptography
Examples of assymetric : Diffie Hellman RSA etc
Examples of block ciphers : DES 3DES AES Blowfish etc
Examples of stream ciphers : RC4 SEAL etc
Examples of hash fuctions : MD5 SHA etc

a) Vigenère Cipher (Polyalphabetic Cipher)

- Introduced in 1500s by **Giovan Battista Bellaso**, improved by **Blaise de Vigenère**.
- Used a **keyword** to change alphabets repeatedly.
- Much stronger than Caesar/monoalphabetic ciphers.
- Called the **"unbreakable cipher" for 300 years."**

b) Playfair Cipher (1854)

- Created by Charles Wheatstone; promoted by Lord Playfair.
- First **digraph substitution cipher**.
- Used in **World War I**.

c) Hill Cipher (1929)

- Developed by Lester S. Hill.
- First cipher based on **linear algebra** and matrix multiplication.

---

5 World War Era (1900 – 1945)

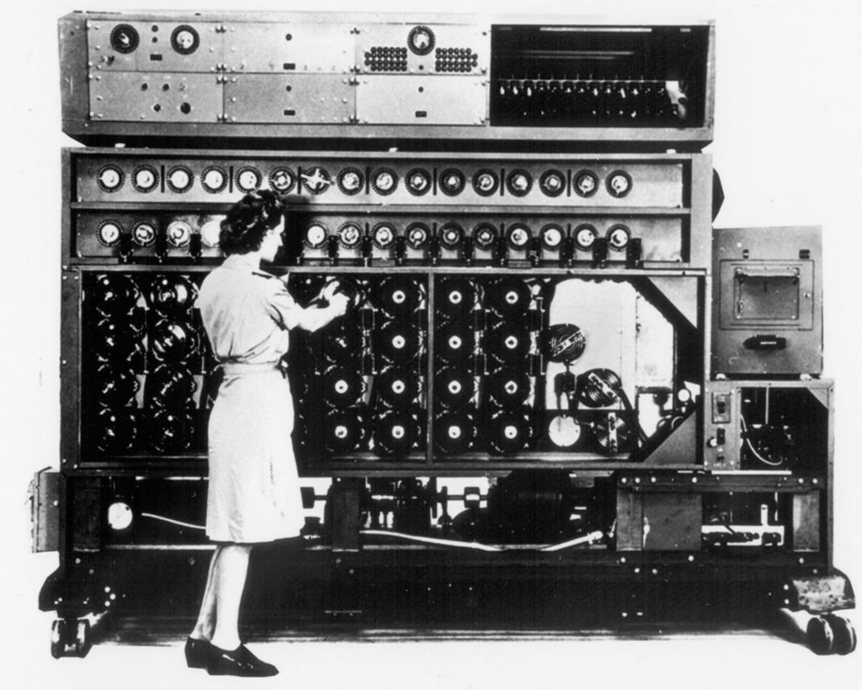
a) One-Time Pad (OTP)

- Invented in 1917.
- If used correctly → **perfect secrecy**.
- Still unbreakable today.

b) Mechanical Ciphers (WWII)

German Enigma Machine

- Most famous machine cipher.
- Used rotating wheels (rotors).
- Broken by **Alan Turing** and team at Bletchley Park.
- Marked the beginning of **modern cryptanalysis**.



Japanese Purple Cipher

- Broken by American cryptanalysts during WWII.

---

6 Birth of Modern Cryptography (1945 – present)

After WWII, cryptography shifted from mechanical devices to **mathematics and computers**.

a) Claude Shannon (1949)

- Father of modern information theory.
- Defined **confusion**, **diffusion**, **entropy**, “perfect secrecy”.
- Inspired modern block ciphers.

b) Symmetric Key Algorithms (1970s–1980s)

- **DES (1977) – Data Encryption Standard**
- Later improved to **Triple DES**
- Eventually replaced by **AES (2001)**

c) Public-Key Cryptography (1976)

- Revolutionized cryptography.

- Invented by **Whitfield Diffie**, **Martin Hellman**, later formalized by **Rivest–Shamir–Adleman (RSA)**.
- Introduced:
  - Public key
  - Private key
  - Digital signatures
  - Key exchange

d) Internet Age (1990s – present)

Modern cryptography includes:

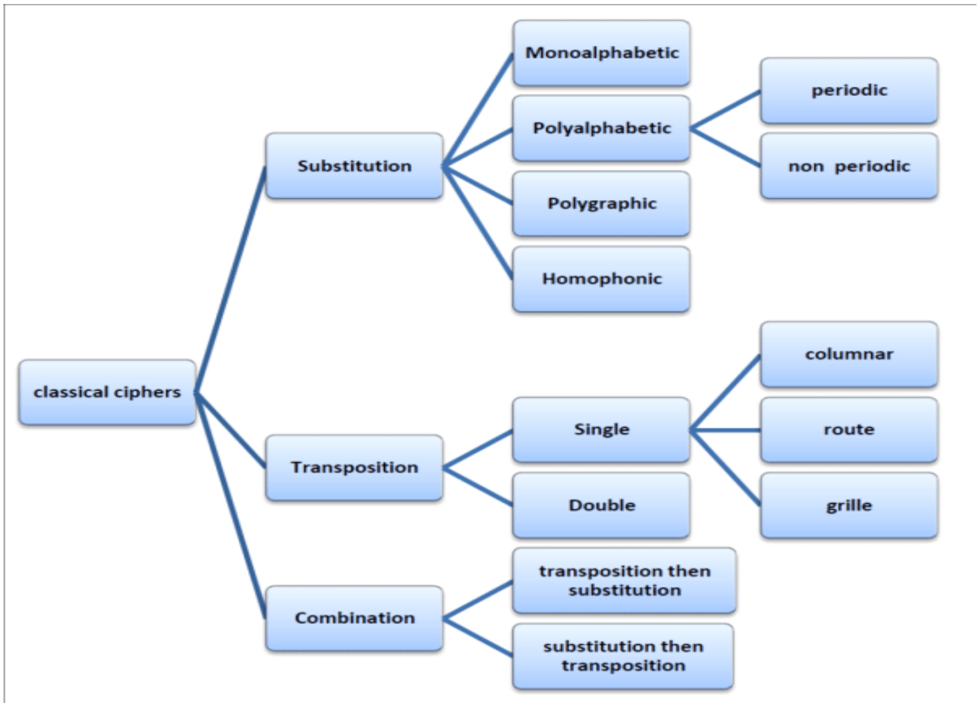
- AES
- RSA
- ECC (Elliptic Curve Cryptography)
- Digital Signatures
- TLS/SSL
- Blockchain cryptography
- Quantum-resistant cryptography

Classical Cryptosystems

Classical cryptosystems are the **oldest methods of encryption**, used before modern computer-based cryptography. They mainly rely on:

- Simple letter substitution
- Rearranging (transposing) characters
- Manual or mechanical techniques

Although simple, they form the **foundation** of modern cryptography.



The diagram divides **Classical Ciphers** into:

1. **Substitution Ciphers**
2. **Transposition Ciphers**
3. **Combination Ciphers**

1️⃣ SUBSTITUTION CIPHERS

A substitution cipher **replaces** each letter/group of letters with another letter/group.

📌 Types of Substitution Ciphers (from diagram):

A. Monoalphabetic Cipher

- Uses **one single alphabet substitution** for the whole message.
- Each plaintext letter always maps to the same ciphertext letter.

✔ Example:

Mapping:
A→Q, B→W, C→E …

Plaintext: **HELLO**
Ciphertext: **EQQMT**

📝 Questions (2):

1. Define monoalphabetic cipher with an example.
2. Why is monoalphabetic substitution vulnerable to frequency analysis?

B. Polyalphabetic Cipher

- Uses **multiple substitution alphabets**.
- Shifting changes based on a key (e.g., Vigenère cipher).

There are two types:

✔ 1. Periodic Polyalphabetic

Keyword repeats periodically.

Example (Vigenère):
Key: **LIME**
Plain: **HELLO**
Cipher: **SQQXQ**

✓ 2. Non-Periodic Polyalphabetic

Key does **not repeat**; could be a long, random key.

Example:
One-time pad (non-periodic) shifting for each letter.

📝 **Exam Questions (2):**

1. Differentiate between periodic and non-periodic polyalphabetic ciphers.
2. Encrypt the text "CAT" using Vigenère cipher with key "DOG".

C. Polygraphic Cipher

- Substitutes **multiple letters at once** (digraph or blocks).
- Playfair & Hill are common examples.

✓ Example: Playfair Cipher

Key: **SECURITY**
Plain: **MEET** → Split as: ME ET
Cipher (after matrix rules): **CL ZB**

📝 **Exam Questions (2):**

1. What is a polygraphic cipher? Give two examples.
2. Explain how Playfair cipher encrypts a pair of letters.

D. Homophonic Cipher

- Maps **one plaintext letter to multiple ciphertext symbols**.
- Used to defeat frequency analysis.

✓ Example:

Plain A → {F, 12, 9}
Plain E → {Q, %, 17}

Message: **MEET**
Cipher could be: **9 % 12 17**

📝 **Exam Questions (2):**

1. Define homophonic substitution with an example.
2. Why are homophonic ciphers more secure than Caesar ciphers?

---

2 TRANSPOSITION CIPHERS

These ciphers **rearrange the positions** of letters but keep them unchanged.

📌 **Types of Transposition (from diagram):**

A. Single Transposition

Only **one round of rearrangement**.

Types:

✓ 1. Columnar Transposition

Write by rows, read by columns.

Plain: **HELLOWORLD**
3 columns:

H E L

L O W

O R L

D

Cipher: **HL O L E R W L D**

✓ 2. Route Cipher

Write the message in a block and read in a particular path (spiral, zigzag).

Example:
HELLOWORLD arranged in 3×4 matrix, read in spiral order.

✔ 3. Grille Cipher

Use a **stencil (grille)** with holes to place characters, then rotate.

📝 Exam Questions (2):

1. Explain columnar transposition with an example.
2. What is a route cipher? How does it work?

B. Double Transposition

Two rounds of transposition, often two columnar transpositions.

✔ Example:

Plain: **ATTACKATDAWN**

Key1 = 3 1 4 2
Key2 = 2 4 1 3

Apply columnar transposition twice.

📝 Exam Questions (2):

1. Why is double transposition more secure than single transposition?
2. Encrypt "CRYPTO" using double transposition with given keys.

3️⃣ COMBINATION CIPHERS

Uses **both substitution and transposition**.

📌 Two types (from diagram):

A. Transposition then Substitution

1. First shuffle positions
2. Then substitute characters

✔ Example:

Plain: **HELLO**
Step 1 (Transposition): HLOEL
Step 2 (Substitution Caesar+3): KORHO

B. Substitution then Transposition

1. First replace letters
2. Then rearrange them

✓ Example:

Plain: HELLO
Step 1 Substitute (A→D): H→K, E→H → KHOOR
Step 2 Transpose: KOORH

📝 **Exam Questions (2):**

1. Explain “substitution then transposition” with an example.
2. Why are combination ciphers stronger than using a single method?

📜 **SUMMARY TABLE (Quick Revision)**

Category	**Types**	**Key Idea**	**Example**
Substitution	Monoalphabetic, Polyalphabetic, Polygraphic, Homophonic	Replace letters	Caesar, Vigenère, Playfair
Transposition	Single (columnar, route, grille), Double	Rearrange letters	Rail Fence, Columnar
Combination	Sub→Trans, Trans→Sub	Mix types	Modern block ciphers follow similar idea

sa

Classical Cryptosystems

Sa

sa

Classical Cryptosystems

Sa

sa

Classical Cryptosystems

Sa

sa

Classical Cryptosystems

Sa

sa

Classical Cryptosystems

Sa

sa

Classical Cryptosystems

Sa

sa

Classical Cryptosystems

Sa

sa

Classical Cryptosystems

Sa