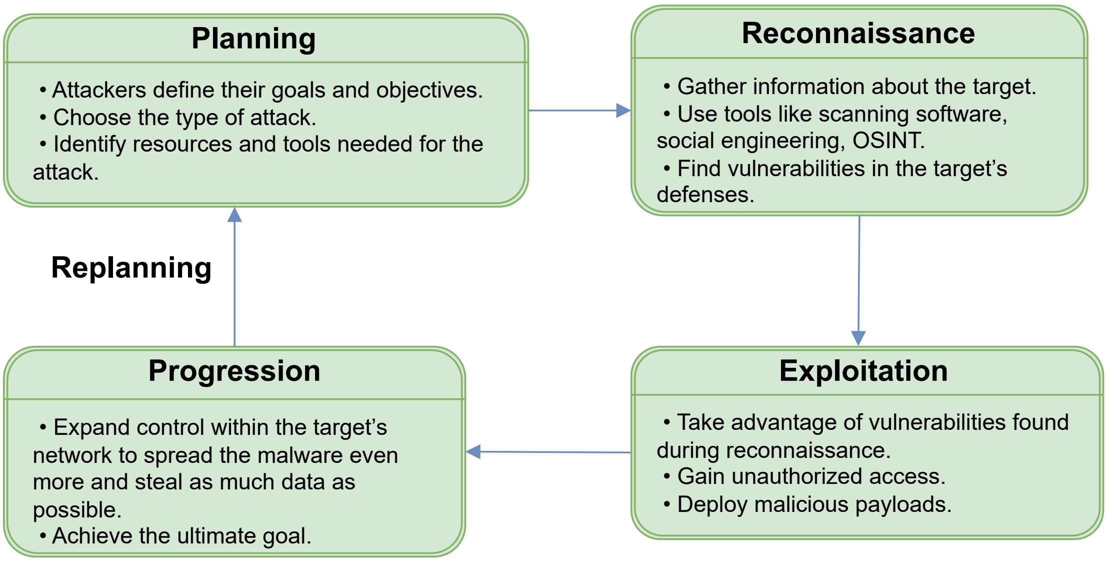
Chapter 0: Ancient Introduction

1 Steps Of An Attack



Planning

- Attackers define their goals and objectives.
- Choose the type of attack.
- Identify resources and tools needed for the attack.

Reconnaissance

- Gather information about the target.
- Use tools like scanning software, social engineering, OSINT.
- Find vulnerabilities in the target's defenses.

Exploitation

- Take advantage of vulnerabilities found during reconnaissance.
- Gain unauthorized access.
- Deploy malicious payloads.

Progression

- Expand control within the target's network to spread the malware even more and steal as much data as possible.
- Achieve the ultimate goal.

2 Reasons for Poor Security

Reasons

- **Insufficient Budget**: Approximately $\frac{1}{4}$ of issues arise due to inadequate funding for cybersecurity initiatives and personnel.
- **Unqualified Personnel**: A lack of skilled and properly trained cybersecurity professionals.
- **Poor Administration**: Inefficient management and lack of synchronization in security policies and practices.

3 Impacts of a Cyberattack

Impacts

- **Data Breach**: Unauthorized access to sensitive client or organizational data. This may include encrypting data for ransom (ransomware), sharing confidential information, or selling it on the dark web.
- **Denial of Service (DoS)**: Disrupting or halting the services of an organization, making them inaccessible to users.
- **Financial Loss**: Hacking into bank accounts, demanding ransom (ransomware attacks), or causing service interruptions that result in revenue loss.
- **Damage to Reputation**: Eroding client trust or tarnishing someone's reputation by exposing compromised or sensitive data.
- **Loss of Clients**: Organizations may lose clients due to the exposure of sensitive information, compromised systems, server outages, and interruptions in services.

4 Information System

Definition

A set of active applications, services, and other components that allow for the management of informations. Vulnerabilities can affect all components of the information system (IS).

5 Responses to Cyberattacks

Responses

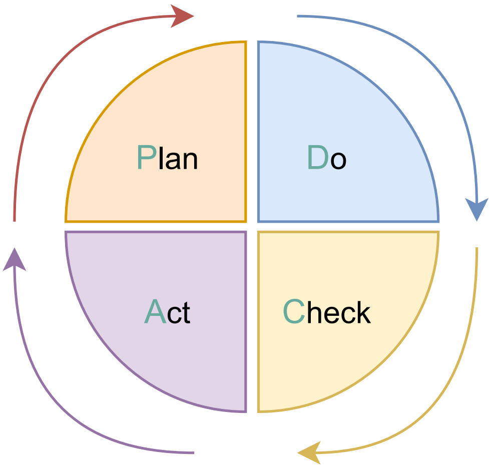
- **Reduce the Impact**: Taking measures to minimize the damage caused by the cyberattack, such as isolating affected systems, restoring backups, or limiting access.
- **Accept the Risk**: The least effective response, where no action is taken to counter the attack. This could include surrendering to attackers' demands, such as paying a ransom.
- **Refuse or Resolve the Risk**: Actively countering the attack by refusing to comply with attackers and taking corrective actions to fix vulnerabilities or breaches.
- **Transfer the Responsibility**: Shifting the burden of dealing with the cyberattack to a third party, such as an insurance provider or a managed cybersecurity service.

6 Steps For Protection (Deming's Wheel)

PDCA

The PDCA (Plan-Do-Check-Act) cycle is a continuous improvement process widely used in cybersecurity to ensure effective protection and adapt to evolving threats. Below are the four key steps:

- **Plan**: Identify goals, assess risks, and develop strategies to strengthen cybersecurity.
- **Do**: Implement the cybersecurity measures, like deploying firewalls and training staff.
- **Check**: Monitor and evaluate the effectiveness of security measures through audits and testing.
- **Act**: Address weaknesses and refine security measures to adapt to new threats.



7 Objectives Of Cybersecurity

Objectives

- **Confidentiality:** Ensuring that information is accessible only to authorized individuals or systems.
- **Integrity:** Protecting information from being altered or tampered with by unauthorized parties.
- **Availability:** Ensuring that information and resources are accessible when needed by authorized users.
- **Accountability:** Tracking and attributing actions to specific individuals or systems to ensure responsibility.
- **Non-Repudiation:** Preventing individuals or systems from denying their actions or commitments.

8 Domain Of Cybersecurity

Domain

- **Physical Security:** Protecting physical assets (e.g., servers, devices, and facilities) from unauthorized access, theft, or damage.
- **OS Security:** Securing operating systems by implementing measures like access controls, patches, and malware protection.
- **Logical Security:** Safeguarding data and systems through software-based controls like encryption, firewalls, and authentication.
- **Application Security:** Ensuring that applications are secure by identifying and fixing vulnerabilities during development and deployment.
- **Telecommunication Security:** Protecting communication systems (e.g., networks, phones, and internet) from interception, eavesdropping, or attacks.

9 Transmission Security

Transmission Security

- Only the intended recipient can access the message.
- Verify the identity of both the sender and the receiver.
- Ensure that the message sent and the message received are identical.
- Provide proof that the message was successfully sent and received.

10 Identification & Authentication

Identification & Authentication

- **Identification:** The process of claiming an identity (e.g., providing a username or email address).
- **Authentication:** The process of verifying the claimed identity (e.g., using a password, biometrics, or a one-time code).
- **Example - Two-Factor Authentication (2FA):**
  - **Step 1 - Identification:** Provide a username or email.
  - **Step 2 - Authentication:**
    - **First Factor:** Provide a password.
    - **Second Factor:** Input the code that was sent to your email or phone number

11 The Risks of Network Security

The Risks

- Theft of passwords and personal data.
- Insertion of malware and viruses.
- Spoofing of source addresses.
- Violation of data integrity.
- Denial of Service (DoS) attacks.

12 Objectives of Attacks

Objectives

- Misinforming.
- Denying access to a resource.
- Taking control of a resource.
- Stealing data present in the system.
- Using the system as a relay.
- Creating a botnet network (zombies).

13 Attacks

Attacks

- **DOS (Denial of Service):** An attack that overwhelms a system, making it unavailable to users by flooding it with excessive requests.
- **DDOS (Distributed Denial of Service):** A more advanced form of DOS where multiple systems (often compromised) are used to flood a target, making it harder to mitigate.
- **MITM (Man-in-the-Middle):** An attack where an attacker intercepts and potentially alters communication between two parties without their knowledge.
- **IP Spoofing:** An attack where an attacker disguises their IP address to impersonate another system, often to gain unauthorized access or launch further attacks.
- **DNS Spoofing/Poisoning:** An attack where an attacker corrupts DNS records to redirect users to malicious websites instead of legitimate ones.
- **Smurf Attack:** A type of DOS attack where the attacker sends spoofed ICMP packets to broadcast addresses, causing multiple systems to respond and overwhelm the target.
- **Port Scan:** An attack where an attacker scans a system for open ports to identify potential vulnerabilities or services to exploit.
- **Phishing:** A social engineering attack where attackers trick users into revealing sensitive information (e.g., passwords) by pretending to be a trusted entity.
- **Hoax:** A false message or warning designed to deceive users, often causing unnecessary panic or spreading misinformation.
- **Bot or Zombie:** A compromised computer controlled by an attacker, often used to carry out malicious activities like DDOS attacks or spam distribution.
- **Backdoor:** A hidden method of bypassing normal authentication or security mechanisms, often left by attackers to regain access to a system.

14 Types of Malware

Types

- **Worm:** A self-replicating malware that spreads across networks without user action. It consumes system resources and can deliver malicious payloads.
- **Spyware:** Software that secretly monitors user activity, collecting personal data such as passwords, browsing habits, or financial information.
- **Rootkit:** A hidden malware that provides hackers deep access to a system while avoiding detection, often modifying system files.
- **Logic Bomb:** Malicious code hidden inside a program that activates under specific conditions, such as a certain date or user action.

15 Types Of Hackers

Types

- **Anonymous:** Hackers who act without revealing their identity, often working individually or in loosely connected groups.
- **Cyber-Indigned:** Activist hackers (hacktivists) who attack systems to protest or promote a political, social, or ideological cause.
- **Cyber-Armed:** Hackers who possess advanced skills and tools, often working for governments or military operations to conduct cyber warfare.
- **Cyber-Criminal:** Hackers who engage in illegal activities for financial gain, such as stealing data, fraud, or ransomware attacks.

16 How To Protect Ourselves

Protection

- **Antivirus:** Software that detects, prevents, and removes malware by scanning files and monitoring system behavior.
- **IDS/IPS (Intrusion Detection/Prevention System):** Security tools that monitor network traffic to detect (IDS) or block (IPS) suspicious activity.
- **OS Firewall:** A built-in security feature in operating systems that filters incoming and outgoing network traffic to prevent unauthorized access.
- **Anti-spam:** Software that filters unwanted emails, blocking phishing attempts, scams, and malware hidden in messages.

Chapter 1: Cryptography

1 Cryptography

Definition

The word **cryptography** is derived from two Greek words:

- **Crypt**: means "hidden".
- **Graphy**: means "writing".

2 Why We Need Cryptography

Need

Cryptography is essential for securing data and communications. It provides:

- **Confidentiality**: Ensures that only authorized users can access sensitive information.
- **Data Integrity**: Guarantees that data has not been altered or tampered with during transmission or storage.
- **Availability**: Ensures that authorized users can access data and services when needed.

3 Some Terminology

3.1 Cryptology

Cryptology

Sub filed of math it's the study of secure communication techniques, including both cryptography (creating secure systems) and cryptanalysis (breaking them).

3.2 Cryptography

Cryptography

The practice of designing secure communication methods to protect information from unauthorized access.

3.3 Cryptanalysis

Cryptanalysis

The study of breaking cryptographic systems to decode encrypted messages without knowing the secret key by finding the key or part of it , the plain-text or part of it.

3.4 Encryption

Encryption

The process of converting plain text into cipher text using an encryption algorithm and a key.

3.5 Decryption

Decryption

The process of converting cipher text back into plain text using the correct decryption key.

3.6 Cryptographic Algorithm

Cryptographic Algorithm

A mathematical procedure used for encryption and decryption to secure data.

3.7 Crypto System

Crypto System

A system that implements cryptographic techniques to secure communications, including encryption algorithms, keys, and protocols.

3.8 Plain Text

Plain Text

The original, readable text before encryption.

3.9 Cipher Text

Cipher Text

The unreadable, encrypted version of plain text.

3.10 Key

Key

A secret value used in cryptographic algorithms to encrypt or decrypt data.

3.11 Steganography

Steganography

The practice of hiding information within other non-secret data, such as images, audio files, or text.

4 Categories of Cryptography

Categories

Cryptography can be broadly classified into two major categories:

- **Substitution:** Each letter or group of letters in the plaintext is replaced with a different letter, number, or symbol.
- **Transposition:** The positions of characters in the plaintext are rearranged according to a fixed pattern.

Additionally, substitution ciphers can be divided into three subcategories:

- **Monoalphabetic:** Maps each plaintext character to one ciphertext character. Examples include the Caesar cipher, Shifting cipher, Affine cipher, and Random substitution.
- **Polyalphabetic:** Maps each plaintext character to multiple ciphertext characters using different substitution alphabets, making frequency analysis more difficult. An example is the Vigenère cipher.
- **Polygraphic:** Encrypts groups of letters (digraphs, trigraphs, etc.) rather than individual letters. Examples include the Playfair cipher and Hill cipher.

Reminder

Modulo Arithmetic

In all the upcoming ciphers, modular arithmetic will play a crucial role. We will frequently use the modulo operation (**mod**) to keep the index in bound. Here's how to compute $a \bmod b$:

- If $a = b$, then $a \bmod b = 0$.
- If $0 \leq a < b$, then $a \bmod b = a$.
- If $a > b$ then $a \bmod b = a - b \cdot \left\lfloor \frac{a}{b} \right\rfloor$
- If $a < 0$, then $a \bmod b = (-a \bmod b) + b$.

5 Classical Cryptography & Cryptanalysis

5.1 Caesar Cipher

Caesar Cipher

The Caesar cipher is a mono-alphabetic substitution cipher used by Julius Caesar, where each letter of the alphabet is shifted by a fixed amount (commonly 3) to the right. The alphabet is labeled from 0 to 25.

- **Encryption:**

$$\boxed{C = E(p,k) = (p+k) \mod 26}$$

- **Decryption:**

$$\boxed{p = D(C,k) = (C-k) \mod 26}$$

Where:

- C is the ciphered character.
- p is the plain character.
- E is the encryption function.
- D is the decryption function.
- k is the key (shift value).

Example

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Encryption Of RABAH

$$C_1 = E(17,3) \mod 26 = 20 \mod 26 = \boxed{20}$$

$$C_2 = E(0,3) \mod 26 = 3 \mod 26 = \boxed{3}$$

$$C_3 = E(1,3) \mod 26 = 4 \mod 26 = \boxed{4}$$

$$C_4 = E(0,3) \mod 26 = 3 \mod 26 = \boxed{3}$$

$$C_5 = E(7,3) \mod 26 = 10 \mod 26 = \boxed{10}$$

$$\text{RABAH} \implies \text{UDEDK}$$

Decryption Of ODWHA

$p_1 = D(14, 3) \mod 26 = 11 \mod 26 = \boxed{11}$

$p_2 = D(3, 3) \mod 26 = 0 \mod 26 = \boxed{0}$

$p_3 = D(22, 3) \mod 26 = 19 \mod 26 = \boxed{19}$

$p_4 = D(7, 3) \mod 26 = 4 \mod 26 = \boxed{4}$

$p_5 = D(0, 3) \mod 26 = -3 \mod 26 = \boxed{23}$

$$\text{ODWHA} \implies \text{LATEX}$$

5.2 Shifting Cipher

Shifting Cipher

The shifting cipher is a mono-alphabetic substitution cipher that shifts each letter of the alphabet left or right by k positions. If $k = 3$ and the shift is to the right, it becomes the Caesar cipher.

- **Encryption:**

$$\boxed{C = E(p, k) = (p + k) \mod 26} \quad \text{(Right shift)}$$

$$\boxed{C = E(p, k) = (p - k) \mod 26} \quad \text{(Left shift)}$$

- **Decryption:**

$$\boxed{p = D(C, k) = (C - k) \mod 26} \quad \text{(Right shift decryption)}$$

$$\boxed{p = D(C, k) = (C + k) \mod 26} \quad \text{(Left shift decryption)}$$

5.3 Random Substitution

Random Substitution

Random substitution is a type of **mono-alphabetic substitution cipher** where each letter in the plaintext is randomly mapped to a unique ciphertext letter. The key for this cipher is the mapping table itself, which defines the substitution for each letter.

Example

Plain Text	A	B	C	D	E	F	G	H	I	J	K	L	M
Ciphered Text	X	W	Y	K	R	L	A	M	B	N	C	O	D

Plain Text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphered Text	P	E	Q	F	Z	G	S	H	T	I	U	J	V

5.4 Affine Cipher

Affine Cipher

The affine cipher is a type of monoalphabetic substitution cipher that uses the equation of a line to encrypt and decrypt text.

- **Encryption:**

$$\boxed{E(x, a, b) = (a \cdot x + b) \ \equiv \ y \ [26]}$$

- **Decryption:**

$$\boxed{D(y, a^{-1}, b) = (y - b) \cdot a^{-1} \ \equiv \ x \ [26]}$$

Where:

- x is the plaintext character (represented as an integer in $[0, 25]$).
- y is the ciphertext character (represented as an integer in $[0, 25]$).
- E is the encryption function.
- D is the decryption function.
- b is the shift value, $b \in [0, 25]$.
- a is the multiplier, $a \in [1, 26]$ that are coprime with 26.
- a^{-1} is the modular inverse of a modulo 26.

Note

- **When** $\underline{a = 0}$: We lose the original plaintext, and the entire ciphertext will be a sequence of b.
- **When** $\underline{a = 1}$: The affine cipher becomes a Caesar (shift) cipher, shifting each character to the right by b positions.

5.4.1 How We Found The Decryption Function

Decryption Function

$$a \cdot x + b \equiv y[26]$$
$$a \cdot x \equiv y - b[26]$$
$$a^{-1} \cdot (a \cdot x) \equiv a^{-1} \cdot (y - b)[26]$$
$$x \equiv a^{-1} \cdot (y - b)[26]$$
$$\boxed{a^{-1} \cdot (y - b) \equiv x[26]}$$

Condition to substitute $a \cdot a^{-1}$ with 1:

$$a \cdot a^{-1} \equiv 1[26]$$

5.4.2 Why a Has To Be Coprime With 26

Why a Has To Be Coprime With 26

1. Ciphertext Collisions When a Is Not Coprime

If a is not coprime with 26, multiple plaintext characters can map to the same ciphertext character, making decryption impossible.

Example for $a = 2$, $b = 2$:

- $x = 0$:
$$2 \cdot 0 + 2 \equiv y[26] \Rightarrow 2 \equiv y[26] \Rightarrow \boxed{y = 2}$$
- $x = 13$:
$$2 \cdot 13 + 2 \equiv y'[26] \Rightarrow 28 \equiv y'[26] \Rightarrow \boxed{y' = 2}$$

Here, both $x = 0$ and $x = 13$ produce the same ciphertext character $y' = y = 2$, causing information loss. This happens because $\gcd(2, 26) = 2 \neq 1$, making decryption impossible.

2. Existence of the Modular Inverse

By definition the modular inverse of a^{-1} is given with :

$$a \cdot a^{-1} \equiv 1[26]$$

However, this inverse **only exists if a and 26 are coprime**, meaning:

$$\gcd(a, 26) = 1$$

Proof: we can prove that From Bézout's identity :

$$\begin{gathered} a \cdot x + n \cdot k = \gcd(a, n) \\ a \cdot x + 26 \cdot k = \gcd(a, 26) = d \\ a \cdot x = d - 26 \cdot k \\ a \cdot x \equiv d[26] \\ a \cdot a^{-1} \equiv d[26] \\ a \cdot a^{-1} \equiv 1[26] \end{gathered}$$

If $d = \gcd(a, 26) = 1$, then a^{-1} exists by definition only if a and 26 are coprime.

5.4.3 Finding a^{-1}

a^{-1}

To find a^{-1}, we solve:

$$\begin{gathered} a \cdot a^{-1} \equiv 1[26] \\ a \cdot a^{-1} = 1 + 26 \cdot k \end{gathered}$$

which gives:

$$\boxed{a^{-1} = \frac{1 + 26 \cdot k}{a}}$$

We try values of k until a^{-1} is an integer, which only happens if $\gcd(a, 26) = 1$. If the result is greater than 26, we reduce it modulo 26 to get a^{-1} in the range $[0, 25]$.

Example With The Key $(a, b) = (5, 18)$

Encryption of SMILE

$y_1 = E(18, 5, 18) \mod 26 = 108 \mod 26 = \boxed{4}$

$y_2 = E(12, 5, 18) \mod 26 = 78 \mod 26 = \boxed{0}$

$y_3 = E(8, 5, 18) \mod 26 = 58 \mod 26 = \boxed{6}$

$y_4 = E(11, 5, 18) \mod 26 = 73 \mod 26 = \boxed{21}$

$y_5 = E(4, 5, 18) \mod 26 = 38 \mod 26 = \boxed{12}$

$$\text{SMILE} \implies \text{EAGVM}$$

Decryption of EAGVM

Finding a^{-1}

Since $\gcd(a, 26) = \gcd(5, 26) = 1$, a^{-1} exists :

$$a^{-1} = \frac{26k + 1}{a}$$

$$a^{-1} = \frac{26(4) + 1}{5}$$

$$\boxed{a^{-1} = 21}$$

$x_1 = D(4, 21, 18) \mod 26 = -294 \mod 26 = \boxed{18}$

$x_2 = D(0, 21, 18) \mod 26 = -378 \mod 26 = \boxed{12}$

$x_3 = D(6, 21, 18) \mod 26 = -252 \mod 26 = \boxed{8}$

$x_4 = D(21, 21, 18) \mod 26 = 63 \mod 26 = \boxed{11}$

$x_5 = D(12, 21, 18) \mod 26 = -126 \mod 26 = \boxed{4}$

$$\text{EAGVM} \implies \text{SMILE}$$

5.5 Hill Cipher With 2x2 Matrix

Hill Cipher

Hill cipher is a polygraphic substitution cipher that uses a square matrix $n \times n$, it split the text into m vector of n size.

- **Encryption:**
$$\boxed{E(p, K) = K \cdot p \;\equiv\; C\;[26]}$$
- **Decryption:**
$$\boxed{D(C, K^{-1}) = K^{-1} \cdot C \;\equiv\; p\;[26]}$$
- C is the ciphered text.
- p is the plain text.
- E is the encryption function.
- D is the decryption function.
- K is the key the square matrix $n \times n$ where $\forall K_{ij} \in [0, 25]$.
- K^{-1} is the inverse matrix.

5.5.1 Finding K^{-1}

K^{-1}

Inverse of any matrix is found using:

$$\boxed{D^{-1} \cdot \text{Adj}(K) \;\equiv\; k^{-1}[26]}$$

where:

- D is the determinant of K.
- $\text{Adj}(K)$ is the transpose of the cofactor matrix of K.

Calculating D determinant

$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \boxed{D = ad - bc \bmod 26}$$

Calculating D^{-1}

Now that we have D, we need to find $\frac{1}{D}$ or D^{-1}. We need to solve the same equation as before in affine cipher:

$$D \cdot D^{-1} \equiv 1[26]$$

$$\boxed{D^{-1} = \frac{26k' + 1}{D}}$$

Adjoint of K

The adjoint of a matrix is the transpose of the cofactor matrix. For a 2×2 matrix:

$$\boxed{\text{Adj}(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) \bmod 26 = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \bmod 26}$$

Note

When a given text cannot be divided into m vectors of size n, we need to append extra characters to fill the gap. Most of the time, we use 'X' or 'Z'.

Example

$$K = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}$$

Encryption Of ATTACK

Divide the word into 3 verctor of size 2

$$p_1 = \begin{pmatrix} A \\ T \end{pmatrix} = \begin{pmatrix} 0 \\ 19 \end{pmatrix} \quad , \quad p_2 = \begin{pmatrix} T \\ A \end{pmatrix} = \begin{pmatrix} 19 \\ 0 \end{pmatrix} \quad , \quad p_3 = \begin{pmatrix} C \\ K \end{pmatrix} = \begin{pmatrix} 2 \\ 10 \end{pmatrix}$$

$$C_1 = K \cdot p_1 = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 19 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 0) + (3 \cdot 19) \\ (3 \cdot 0) + (6 \cdot 19) \end{pmatrix} \bmod 26 = \begin{pmatrix} 57 \\ 114 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 5 \\ 10 \end{pmatrix}}$$

$$C_2 = K \cdot p_2 = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 0 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 19) + (3 \cdot 0) \\ (3 \cdot 19) + (6 \cdot 0) \end{pmatrix} \bmod 26 = \begin{pmatrix} 38 \\ 57 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 12 \\ 5 \end{pmatrix}}$$

$$C_3 = K \cdot p_3 = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 10 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 2) + (3 \cdot 10) \\ (3 \cdot 2) + (6 \cdot 10) \end{pmatrix} \bmod 26 = \begin{pmatrix} 34 \\ 66 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 8 \\ 14 \end{pmatrix}}$$

$$\text{ATTACK} \implies \text{FKMFIO}$$

Encryption Of LATEX

When dividing LATEX into 3 segments of size 2 ,the last part has a missing element therefore we will append it with 'X'

$$p_1 = \begin{pmatrix} L \\ A \end{pmatrix} = \begin{pmatrix} 11 \\ 0 \end{pmatrix} \quad , \quad p_2 = \begin{pmatrix} T \\ E \end{pmatrix} = \begin{pmatrix} 19 \\ 4 \end{pmatrix} \quad , \quad p_3 = \begin{pmatrix} X \\ X \end{pmatrix} = \begin{pmatrix} 23 \\ 23 \end{pmatrix}$$

$$C_1 = K \cdot p_1 = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 0 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 11) + (3 \cdot 0) \\ (3 \cdot 11) + (6 \cdot 0) \end{pmatrix} \bmod 26 = \begin{pmatrix} 22 \\ 33 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 22 \\ 7 \end{pmatrix}}$$

$$C_2 = K \cdot p_2 = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \cdot \begin{pmatrix} 19 \\ 4 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 19) + (3 \cdot 4) \\ (3 \cdot 19) + (6 \cdot 4) \end{pmatrix} \bmod 26 = \begin{pmatrix} 50 \\ 81 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 24 \\ 3 \end{pmatrix}}$$

$$C_3 = K \cdot p_3 = \begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix} \cdot \begin{pmatrix} 23 \\ 23 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 23) + (3 \cdot 23) \\ (3 \cdot 23) + (6 \cdot 23) \end{pmatrix} \bmod 26 = \begin{pmatrix} 115 \\ 207 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 11 \\ 25 \end{pmatrix}}$$

$$\text{LATEXX} \implies \text{WHYOLZ}$$

Decryption Of WHYOLZ

Determinant D

$$D = ad - bc \bmod 26 = 2 \cdot 6 - 3 \cdot 3 \bmod 26 = \boxed{3}$$

Finding D^{-1}

$$D \cdot D^{-1} \;\equiv\; 1[26]$$

$$D^{-1} = \frac{26k' + 1}{D}$$

$$D^{-1} = \frac{26(1) + 1}{D}$$

$$\boxed{D^{-1} = 9}$$

Adj(K)

$$\text{Adj}(\begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}) \bmod 26 = \begin{pmatrix} 6 & -3 \\ -3 & 2 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 6 & 23 \\ 23 & 2 \end{pmatrix}}$$

Finding K^{-1}

$$K^{-1} = D^{-1} \cdot \text{Adj}(K) \bmod 26 = 9 \cdot \begin{pmatrix} 6 & 23 \\ 23 & 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 54 & 207 \\ 207 & 18 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 2 & 25 \\ 25 & 18 \end{pmatrix}}$$

Dividing the ciphered text into 3 vector of size 2 :

$$C_1 = \begin{pmatrix} W \\ H \end{pmatrix} = \begin{pmatrix} 22 \\ 7 \end{pmatrix} \quad , \quad C_2 = \begin{pmatrix} Y \\ O \end{pmatrix} = \begin{pmatrix} 24 \\ 3 \end{pmatrix} \quad , \quad C_3 = \begin{pmatrix} L \\ Z \end{pmatrix} = \begin{pmatrix} 11 \\ 25 \end{pmatrix}$$

$$p_1 = K^{-1} \cdot C_1 = \begin{pmatrix} 2 & 25 \\ 25 & 18 \end{pmatrix} \cdot \begin{pmatrix} 22 \\ 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 22) + (25 \cdot 7) \\ (25 \cdot 22) + (18 \cdot 7) \end{pmatrix} \bmod 26 = \begin{pmatrix} 219 \\ 676 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 11 \\ 0 \end{pmatrix}}$$

$$p_2 = K^{-1} \cdot C_2 = \begin{pmatrix} 2 & 25 \\ 25 & 18 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 24) + (25 \cdot 3) \\ (25 \cdot 24) + (18 \cdot 3) \end{pmatrix} \bmod 26 = \begin{pmatrix} 123 \\ 654 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 19 \\ 4 \end{pmatrix}}$$

$$p_3 = K \cdot C_3 = \begin{pmatrix} 2 & 25 \\ 25 & 18 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 25 \end{pmatrix} \bmod 26 = \begin{pmatrix} (2 \cdot 11) + (25 \cdot 25) \\ (25 \cdot 11) + (18 \cdot 25) \end{pmatrix} \bmod 26 = \begin{pmatrix} 647 \\ 725 \end{pmatrix} \bmod 26 = \boxed{\begin{pmatrix} 23 \\ 23 \end{pmatrix}}$$

$$\text{WHYOLZ} \implies \text{LATEXX}$$

5.6 Playfair Cipher

Playfair Cipher

The Playfair cipher is a polygraphic substitution cipher that encrypts two characters at a time using a 5 × 5 matrix key.

- Each cell in the matrix must contain a unique letter.
- Since the matrix holds only 25 letters, the letter 'J' is usually omitted.
- If the plaintext contains 'J', it is replaced with 'I'.
- The key consists of a unique-lettered word placed at the beginning of the matrix.
- The remaining cells are filled with the rest of the alphabet in order, excluding any letters already used in the key.

Example With Key MONARCHY

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

5.6.1 Splitting Text into Pairs

Splitting

- If the number of characters is odd, the text is appended with the letter 'Z'.
- A pair cannot consist of the same letter, in such cases a filler letter 'X' is inserted between them.

Example

INSTRUMENTS $\Longrightarrow$ IN , ST , RU , ME , NT , TZ

We appended the letter 'Z' because it has an odd number of letters.

HELLO $\Longrightarrow$ HE , LX , LO

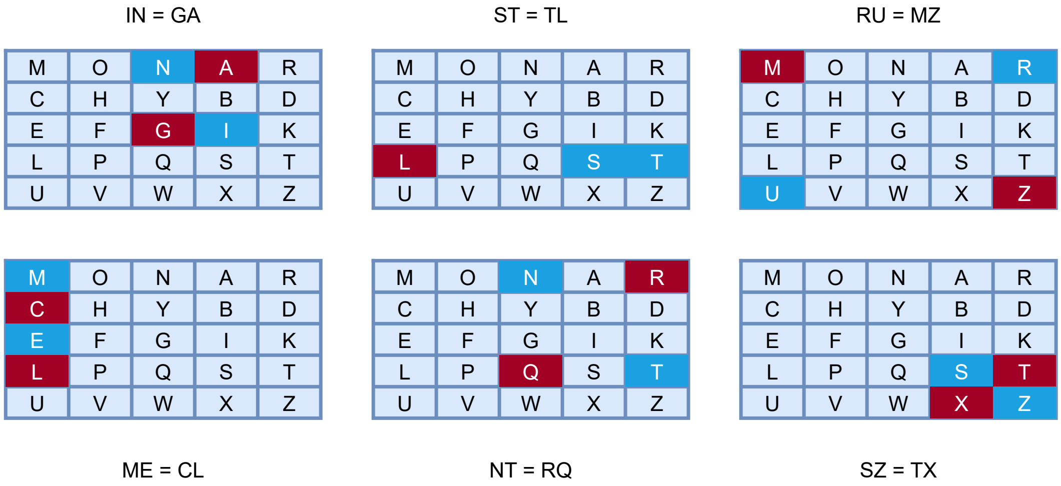
We added the letter 'X' between LL to avoid having pair with same letter.

5.6.2 Encryption

Encryption

- **When the pair is in the same column:** Replace each letter with the one directly below it (wrapping to the top if at the bottom).
- **When the pair is in the same row:** Replace each letter with the one to its right (wrapping to the leftmost if at the rightmost).
- **Otherwise:** Form a rectangle with the pair and replace each letter with the one in its opposite horizontal corner.

Example Encryption Of INSTRUMENTSZ



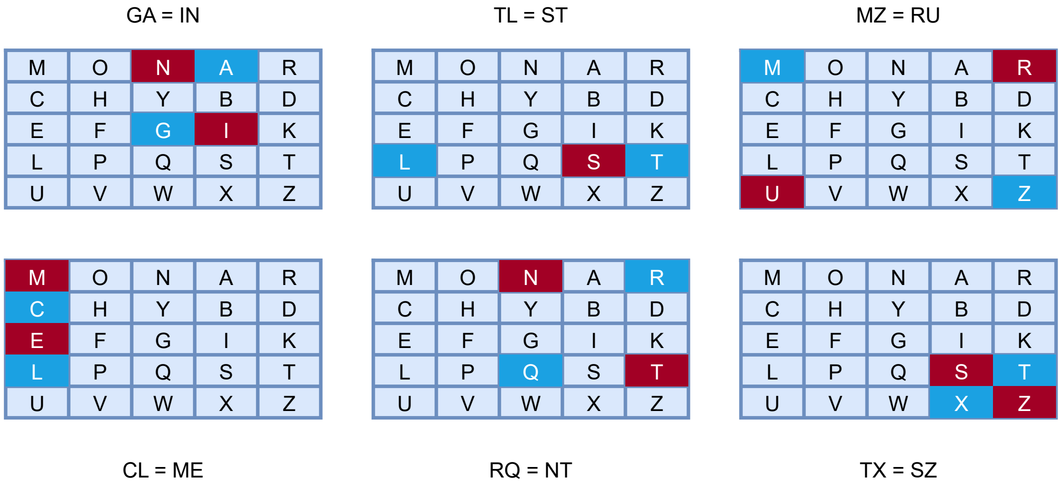
INSTRUMENTSZ $\Longrightarrow$ GATLMZCLRQTX

5.6.3 Decryption

Decryption

- **When the pair is in the same column:** Replace each letter with the one directly above it (wrapping to the bottom if at the top).
- **When the pair is in the same row:** Replace each letter with the one to its left (wrapping to the rightmost if at the leftmost).
- **Otherwise:** Form a rectangle with the pair and replace each letter with the one in its opposite horizontal corner.

Example Decryption Of GATLMZCLRQTX



GATLMZCLRQTX $\Longrightarrow$ INSTRUMENTSZ

5.7 Vigenère Cipher

Vigenère Cipher

The Vigenère cipher is a polyalphabetic substitution cipher that uses a repeating key string.

- **Encryption:**

$$\boxed{C = E(p, k) = (p + k) \mod 26}$$

- **Decryption:**

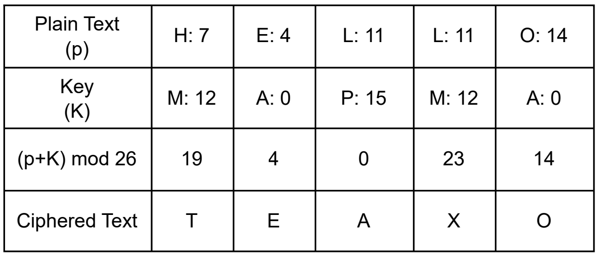
$$\boxed{p = D(C, k) = (C - k) \mod 26}$$

Where:

- C is the encrypted character.
- p is the plaintext character.
- E is the encryption function.
- D is the decryption function.
- k is a character from the key string.

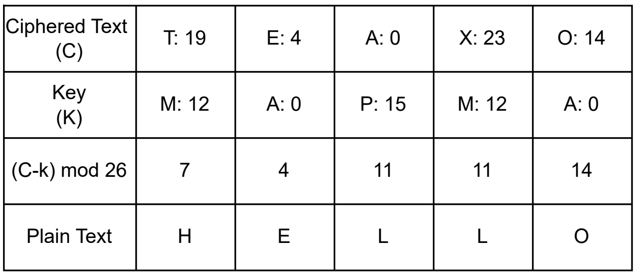
Example With The Key MAP

Encryption Of HELLO



Plain Text (p)	H: 7	E: 4	L: 11	L: 11	O: 14
Key (K)	M: 12	A: 0	P: 15	M: 12	A: 0
(p+K) mod 26	19	4	0	23	14
Ciphered Text	T	E	A	X	O

Decryption Of TEAXO



Ciphered Text (C)	T: 19	E: 4	A: 0	X: 23	O: 14
Key (K)	M: 12	A: 0	P: 15	M: 12	A: 0
(C-k) mod 26	7	4	11	11	14
Plain Text	H	E	L	L	O

Note

Euler's Totient Function:

Euler's Totient Function, denoted $\phi(n)$, counts the number of integers up to n that are coprime to n. For a positive integer n with the prime factorization:

$$n = \prod_{i=1}^{m} p_i^{\alpha_i}$$

where p_i are the distinct prime factors of n and α_i are their respective exponents, the totient function is given by:

$$\phi(n) = n \times \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

Extended Euclidean Algorithm:

The Extended Euclidean Algorithm is used to find the multiplicative inverse of a modulo b , we first perform the normal Euclidean Algorithm till remainer $=1$ then with substitution of the remainers from the bottom we express 1 as a linear combination of a and b:

$$1 = a \cdot x + b \cdot y$$

The coefficient x is the multiplicative inverse of a modulo b

If $x < 0$ use modulo to get the final result.

Example

Find the number of integers coprime to 12:

$$12 = 2^2 \times 3^1$$

$$\phi(12) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = \boxed{4}$$

Find the multiplicative inverse of 5 modulo 12:
Using the extended Euclidean algorithm:

$$12 = 5 \times 2 + 2$$

$$5 = 2 \times 2 + \boxed{1}$$

Back-substituting to express 1 as a linear combination of 5 and 12:

$$1 = 5 - 2 \times 2$$

Since $2 = 12 - 5 \times 2$, we substitute:

$$1 = 5 - (2 \times (12 - 5 \times 2))$$

$$1 = 5 - (2 \times 12 - 5 \times 4)$$

$$1 = 5 + (-2) \times 12 + 5 \times 4$$

$$1 = 5 \times \boxed{5} + 12 \times (-2)$$

Thus, the modular inverse of 5 modulo 12 is $\boxed{5}$.

5.8 Classical Cryptanalysis

Cryptanalysis

- **Brute Force:** A method that systematically tries all possible keys until the correct one is found. It is particularly effective against monoalphabetic ciphers with a small keyspace, such as the Affine cipher (where a must be coprime with 26).
- **Frequency Analysis:** A technique that examines the frequency of letters or groups of letters in a given language. Pioneered by Al-Kindi, it is highly effective against monoalphabetic and polygraphic ciphers, as these ciphers tend to preserve the plaintext's frequency distribution.
- **Kasiski Test:** A method for breaking the Vigenère cipher, a polyalphabetic cipher. It identifies repeated substrings in the ciphertext, assuming that structured languages cause the key to repeat at regular intervals. By analyzing the distances between these repetitions, one can determine the key length using common factors.

5.9 Kasiski Test

Kasiski Test

The Kasiski Test occurs in two steps:

1. Find L the length of the Vigenère key.
2. Apply frequency analysis to all L segments (periodic extraction) to find the key.

5.9.1 Finding Length Of Key

Length Of Key

1. Find repeating substrings (of at least 2-3 characters) in the ciphertext.
2. For each repeating substring, identify a pair of positions: pos_1 and pos_2
3. Compute Distance = pos_2 - pos_1
4. Factorize each distance into its prime factors.
5. The most key length L is the most common factor of the different distances.

5.9.2 Finding the Key

Key

1. Divide the ciphertext into L segments:

$$\text{seg}_1 = L \cdot (k+1),\ \ldots,\ \text{seg}_{n-1} = L \cdot (k + (L-1)),\ \text{seg}_n = L \cdot k$$

2. For each segment compute the letter frequencies and find the most frequent letter, knowing the plaintext language, deduce the shift. Each seg_i then gives the i^{th} character of the key.

Example :

ciphered text (In French) :

CLCJSGEEXJGGOETFEUUUPEIRMOOBTGGRCOAKTLCHRCODGGOTDEFVCJJFHSEFFVKHEPFR
GFSVRUGMAOFMGMEVURGTETBCJJFHSEGEEFJFHFRGOTGTMCOIGSEUMEEIIHGRGEEXJGGO
ETFEZJGGDOONERSEURUGMAVPTCMIVFDGTSATTGNEUEEEIIHGRGNEPUQWFLGTDGVXEPRT
FSRPNFBNVTCQONCJSUFNVVNGDLGGSGDRGUEEPMOVNG

Length Of Key :

CLCJSGEEXJGGOETFEUUUPEIRMOOBTGGRCOAKTLCHRCODGGOTDEFVCJJFHSEFFVKHEPFR
GFSVRUGMAOFMGMEVURGTETBCJJFHSEGEEFJFHFRGOTGTMCOIGSEUMEEIIHGRGEEXJGGO
ETFEZJGGDOONERSEURUGMAVPTCMIVFDGTSATTGNEUEEEIIHGRGNEPUQWFLGTDGVXEPRT
FSRPNFBNVTCQONCJSUFNVVNGDLGGSGDRGUEEPMOVNG

Substring	Pos_1	Pos_2	Distance	Factorization
GT	87	111	24	3×2^3
CJS	3	219	216	$3^2\times2^3$
GEEXJGGOETFE	6	129	123	3×41
CJJFHSE	54	93	39	3×13
RUGMA	73	154	81	3^4
EEIIHGR	122	179	57	3×19

Conclusion

The Length of the key is $\boxed{L = 3}$

Finding The Key We will have 3 segments of 82 characters

seg$_1$

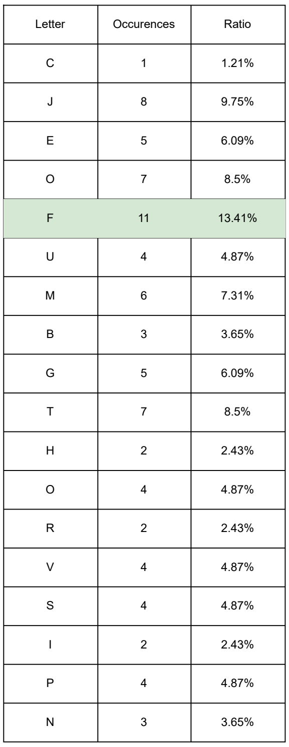
CJEJOFUEMBGOTHOGDVJSFHFFRMFMUTBJSEJFOTOSMIGEJOFJDNSRMPMFTTNEIGNUFTVPF PBTOJFVDGDUPV

seg$_2$

LSEGEEUIOTRALRDOECFEVERSUAMERECFEEFRTMIEEIREGEEGOEEUATIDSTEEIREQLDXRSN NCNSNNLSREMN

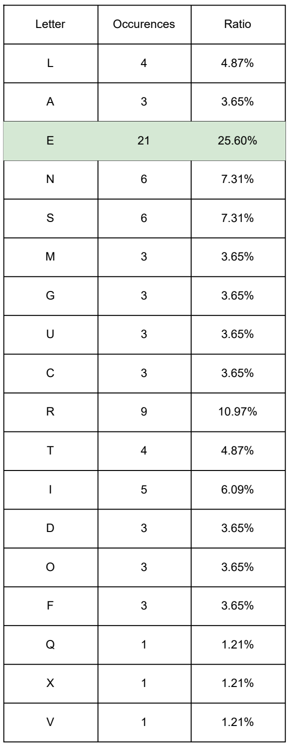
seg$_3$

CGXGTUPROGCKCCGTFJHFKPGVGOGVGTJHGFHGGCGUEHGXGTZGORUGVCVGAGUEHGPWG GETRF VQCUVGGGGEOG



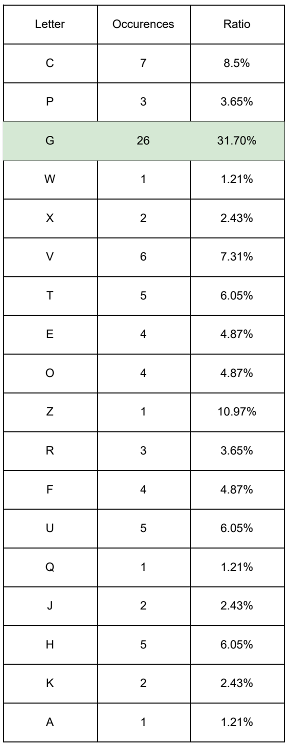
Letter	Occurences	Ratio
C	1	1.21%
J	8	9.75%
E	5	6.09%
O	7	8.5%
F	11	13.41%
U	4	4.87%
M	6	7.31%
B	3	3.65%
G	5	6.09%
T	7	8.5%
H	2	2.43%
O	4	4.87%
R	2	2.43%
V	4	4.87%
S	4	4.87%
I	2	2.43%
P	4	4.87%
N	3	3.65%

seg$_1$



Letter	Occurences	Ratio
L	4	4.87%
A	3	3.65%
E	21	25.60%
N	6	7.31%
S	6	7.31%
M	3	3.65%
G	3	3.65%
U	3	3.65%
C	3	3.65%
R	9	10.97%
T	4	4.87%
I	5	6.09%
D	3	3.65%
O	3	3.65%
F	3	3.65%
Q	1	1.21%
X	1	1.21%
V	1	1.21%

seg$_2$



Letter	Occurences	Ratio
C	7	8.5%
P	3	3.65%
G	26	31.70%
W	1	1.21%
X	2	2.43%
V	6	7.31%
T	5	6.05%
E	4	4.87%
O	4	4.87%
Z	1	10.97%
R	3	3.65%
F	4	4.87%
U	5	6.05%
Q	1	1.21%
J	2	2.43%
H	5	6.05%
K	2	2.43%
A	1	1.21%

seg$_3$

Conclusion

- $k_1 =$ F - E = 1 = B
- $K_2 =$ E - E = 0 = A
- $k_3 =$ G - E = 2 = C

$$\boxed{\text{The key is BAC}}$$

Decryption

BLAISEDEVIGENEREESTUNDIPLOMATEFRANAISLAGRANDEFORCEDUCHIFFREDEVIGENEREES
TQUELAMEMELETTRESERACHIFFREEDEDIFFERENTESMANIERESLECHIFFREDEVIGENEREEXI
GECOMMEPRESQUELATOTALITEDESSYSTEMESDECHIFFREMENTQUELESDEUXCORRESPONDA
NTSCONNAISSENTUNECLEFSECRETECOMMUNE

5.10 Probable-Plaintext Method

Probable-Plaintext

The probable-plaintext method is simpler than the Kasiski test. It works as follows:

1. Guess a likely word or phrase that might appear in the plaintext.
2. Align the crib under each possible position in the ciphertext.
3. For each alignment, derive the key letters by subtracting the crib letters from the corresponding ciphertext letters.
4. Apply the derived key to decrypt surrounding text until the result becomes readable.

Example:

ciphered text :

CLCJSGEEXJGGOETFEUUUPEIRMOOBTGGRCOAKTL

Probable-Plaintext: VIGENERE

C	L	C	J	S	G	E	E	X	J	G	G	O	E	T	F
V	I	G	E	N	E	R	E								
	V	I	G	E	N	E	R	E							
		V	I	G	E	N	E	R	E						
								V	I	G	E	N	E	R	E
Key =								C	B	A	C	B	A	C	

5.11 One-Time Pad (OTP)

OTP

The One-Time Pad is the only cryptographic algorithm proven to be unbreakable. It works like the Vigenère cipher, except the key must be as long as the plaintext.

Conditions:

- The key length equals the plaintext length.
- The key is generated randomly.
- The key is used only once and then discarded.

Note

- In modern implementations, instead of shifting letters (as in Vigenère), each bit of plaintext is XOR-ed with the corresponding key bit.
- Secure key distribution is challenging: the only completely safe method is physical transport in a diplomatic pouch since sharing through network is never 100% safe.
- Generating truly random keys is hard because computers are deterministic. You must rely on physical randomness sources (e.g. electronic noise or radioactive decay).

Example:

Plain Text :

BLAISEDEVIGENEREESTUNDIPLOMATEFRANCAISLAGRANDEFORCEDUCHIFFREDEVIGENEREEST
QUELAMEMELETTRESERACHIFFREEDEDIFFERENTESMANIERESLECHIFFREDEVIGENEREEXIGEC
OMMEPRESQUELATOTALITEDESSYSTEMESDECHIFFREMENTQUELESDEUXCORRESPONDANTSCO
NNAISSENTUNECLEFSECRETECOMMUNE

Vignere Key:

AHFAZBVOIRBVCSKSPOZIEFPAJNBYGSUHXIZFPEOOURTZREJAPOVJNBUIZEFPEFJEFEVEUZFOEH
FEIHFPEFZEBVJNVPAOEIRJZERVEZNBIOREHGREIZITRGNVKPELOEKOVFHUOZPZALXKNZIHIEUP
OGTHJVFPOHFVUEYZOPODFOVFHGRGJODNVODZPKFIYPZHFYPZGOLJPDIDGZPFKPGKHLFEOV
JEPANGKUQMFUJGRUGZPMGOOHAEAZQ

Ciphered Text:

BSFIRFYSDZHZPWBWTGSCRIXPUBNYZWZYXVBFXWZOAITMUIOOGQZMHDBQEJWTHJEMLIIILD
JGXXZITHRTQJKIUOARNTROGPZOEVVZHDQJNTVVLTKIALIGZKEZCAINVMPTMJKYJHVDNPOOR
WQNMGIBAKIYNNVJSSFOIXYKWISGJGNDZZVSNGGRXVLEUBJUCCSXZCADYRPDMFWUXDHUYC
JKUEXGCIWEXSFKXNKZJWUKWMKBGQZSQ VMQUMU

5.12 Index of Coincidence

Index of Coincidence

The Index of Coincidence (IC) is a cryptanalysis technique that helps determine whether ciphertext was encrypted using a monoalphabetic or polyalphabetic substitution cipher by analyzing the frequency distribution of letters in the text. It is calculated using the formula:

$$IC = \sum_{q=A}^{Z} \frac{n_q(n_q - 1)}{n(n-1)}$$

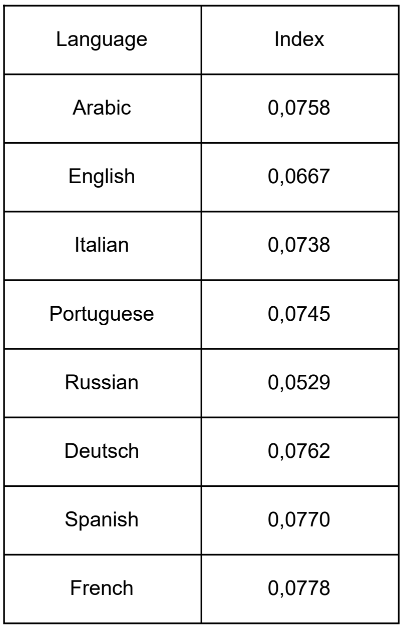
Where:

- n : Length of the ciphertext
- q : Represents letters of the alphabet from A to Z
- n_q : Total number of occurrences of letter q in the ciphertext

Each language has its characteristic index value based on its natural letter frequency distribution. When computing the Index of Coincidence for a message:

- If the calculated IC is close to the language's expected index (approximately 0.067 for English), it likely indicates a monoalphabetic substitution cipher.
- If the calculated IC is significantly lower and closer to 0.038-0.040 (for English), it suggests a polyalphabetic cipher.

This technique works because monoalphabetic ciphers preserve the underlying frequency distribution of the plaintext language, while polyalphabetic ciphers tend to flatten the distribution, making all letters appear with more uniform frequency.



Language	Index
Arabic	0,0758
English	0,0667
Italian	0,0738
Portuguese	0,0745
Russian	0,0529
Deutsch	0,0762
Spanish	0,0770
French	0,0778

5.13 Kerckhoff's Principle (1883)

Kerckhoff's Principle

Kerckhoff's Principle states that:

- A cryptosystem's security should depend **only on the secrecy of the key**.
- The encryption algorithm itself should be assumed to be public knowledge.

This can be summarized as:

The security of encryption should depend only on what can be easily changed (the key), not on what cannot (the algorithm).

Think of it like a door lock:

- The lock mechanism (algorithm) is the same for many doors and widely known
- Your unique key (encryption key) is what keeps your door secure
- If your key is stolen, you can change just the key, not the entire lock

This principle is why modern encryption methods are publicly documented and analyzed by experts, making them more secure through scrutiny rather than secrecy.

Chapter 2: Modern Cryptography