LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2023 -24 Autumn

Student Name: David Budha Magar

London Met ID:22068721

College ID: np01nt4a220119

Assignment Due Date:

Assignment Submission Date:15th, Jan 2024

Word Count (Where Required): 3000+

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Table Of Figure

Abstract

This report introduces cryptography systems. It discusses the core concepts and principles underpinning these systems, underlining their relevance in maintaining secure communication and data protection. The report also analyses numerous types of cryptography algorithms and protocols, along with their strengths and limitations. Additionally, it addresses real-world applications of cryptographic systems and the obstacles they face. Overall, this research offers as a complete overview of cryptographic systems, establishing the framework for additional investigation.

1. Introduction to Cryptographic Systems

1.1 Introduction to Security

Information technology security encompasses the techniques, resources, and individuals employed to safeguard a company's digital assets. The main objective of information technology security is to safeguard these invaluable assets from unauthorised individuals, often known as threat actors, who may cause disruption, theft, or tampering. These dangers can be either intentional or unintentional, and they can originate from any source, whether it be within or external to the company (Bacon, 2024).

IT security encompasses two distinct domains:

1. **Physical security:** Physical security safeguards individuals, equipment, software, and information from unauthorised access, unforeseen events, and natural calamities. It provides protection for organisations against theft, vandalism, and external occurrences that have the potential to cause harm to assets. Physical security breaches, although not reliant on technological expertise, have the potential to cause significant damage to essential business computers and gadgets. Ensuring physical security is essential for minimising these dangers and thwarting potential threats. There are three types of physical security (Bacon, 2024):

    1. Access control: Access control is crucial for ensuring physical security and preventing security breaches, such as unauthorised usage of USB devices. The objective is to oversee and restrict entry to valuable resources by employing physical barriers, identification badges, keycodes, and sophisticated biometric techniques such as fingerprint or facial recognition (Bacon, 2024).

    2. Surveillance: Surveillance technology and tactics are used to monitor activity in the vicinity of buildings and equipment. Businesses frequently deploy closed-circuit television (CCTV) cameras to safeguard their boundaries. These cameras deter trespassers and assist in responding to and analysing incidents. Surveillance technologies encompass cameras, heat sensors, motion detectors, and security alarms (Bacon, 2024).

3. Testing: Testing is a reliable method to enhance physical security. Robust security firms continuously evaluate their rules for improvements. Testing methodologies may involve red teaming, which is using ethical hackers to attempt unauthorised access to a company's cybersecurity infrastructure (Bacon, 2024).

2. **Information security**: **Infosec** is a term that refers to the practice of safeguarding information and ensuring its security. The document encompasses strategies for overseeing the procedures, technology, and policies related to safeguarding both digital and nondigital assets. Implementing information security measures can enhance a company's ability to prevent, identify, and respond to threats. Information security comprises various specialised categories of security technologies, such as (Bacon, 2024):
   1. **Application security:** As a defence against attacks that change, steal, access, or delete data and software, defend apps. Countermeasures are used for application security. These can be software, hardware, or policy. Application firewalls, encryption, patch management, and biometric identification are all common ways to protect your computer. (Bacon, 2024).
   2. **Cloud Security:** Rules and cutting-edge technology are used to make sure that the data and systems of cloud computing are safe. Identity and access management, as well as data privacy, are all parts of cloud security problems. Information security experts keep data safe by doing things like penetration testing, keeping network protocols up to date, finding Man-in-the-Middle attacks, and scanning apps. (Bacon, 2024).

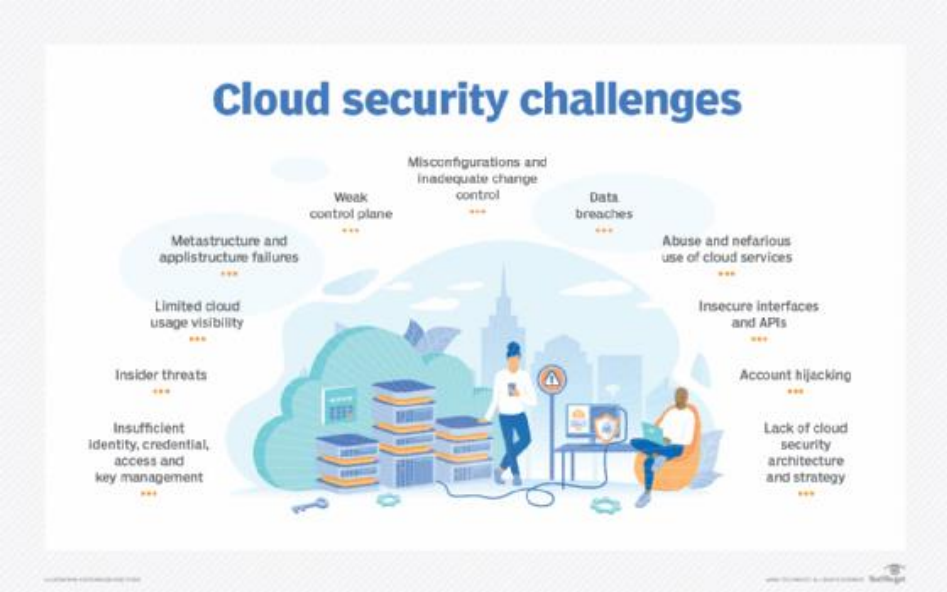

Cloud security challenges
Misconfigurations and inadequate change control
Weak control plane
Data breaches
Metastructure and applistructure failures
Abuse and nefarious use of cloud services
Limited cloud usage visibility
Insecure interfaces and APIs
Insider threats
Account hijacking
Insufficient identity, credential, access and key management
Lack of cloud security architecture and strategy

Figure 1: Cloud security challenges Source: (Bacon, 2024)

3. **Endpoint Security:** Before joining safely, endpoint security requires network nodes to meet Federal Information Security Modernization Act criteria. Nodes include PCs, laptops, tablets, cell phones, POS systems, barcode scanners, sensors, and IoT devices (Bacon, 2024).
4. **Internet Security:** Internet security safeguards and defends software, web browsers, and virtual private networks (VPNs). Encryption safeguards data against malware, phishing, Man-in-the-Middle (MitM) attacks, and denial-of-service (DoS) attacks (Bacon, 2024).

5. **Mobile security:** Wireless technology is used to provide security for mobile devices. It serves as a deterrent against theft, unauthorised data access, and other forms of attacks targeting smartphones, tablets, desktops, and their respective networks (Bacon, 2024).

6. **Network Security:** Network security safeguards the network infrastructure and its linked devices from unauthorised access, malicious exploitation, and alterations (Bacon, 2024).

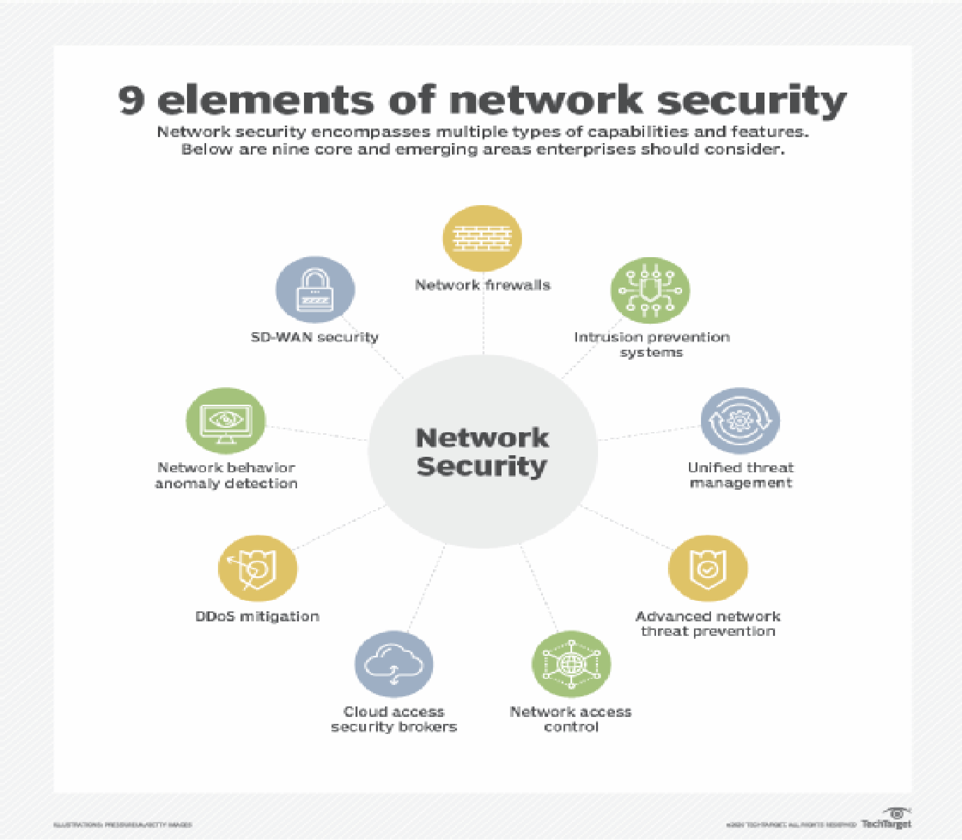

9 elements of network security
Network security encompasses multiple types of capabilities and features.
Below are nine core and emerging areas enterprises should consider.
Network firewalls
SD-WAN security
Intrusion prevention systems
Network Security
Network behavior anomaly detection
Unified threat management
DDoS mitigation
Advanced network threat prevention
Cloud access security brokers
Network access control
TechTarget

Figure 2: 9 elements of network security Source: (Bacon, 2024)

7. **Supply chain Security:** Supply chain security ensures the protection of the network connecting a company with its suppliers, who frequently have access to sensitive employee and intellectual property information (Bacon, 2024).

1.1.1 Information technology security concepts and principles

Several fundamental concepts and principles serve as the basis for IT security. Several of the most significant ones are:

- **Application Lifecycle management:** This protects every step of the application development process by making it less likely that software bugs, design flaws, and setup errors will happen (Bacon, 2024).
- **Defence in depth:** This is a plan to keep information safe that uses several defences at the same time. Endpoint detection and response, antivirus software, and kill switches are some of these ways. Defence in depth is based on the military idea that an enemy will find it harder to get through a defence system with more than one layer than one with only one (Bacon, 2024).
- **Patch Management:** For applications, operating systems, and firmware with broken code, patches and updates are bought, tried, and then installed (Bacon, 2024).
- **Principle of least privilege:** By giving users and programmes only the minimal amount of access rights they need to do their jobs, this principle makes IT security stronger (Bacon, 2024).
- **Risk Management:** In this step, security risks that pose a danger to an organization's IT environment are found, evaluated, and managed (Bacon, 2024).
- **Vulnerability Management:** With this method, security administrators regularly check for holes by finding, confirming, fixing, and patching IT security holes as they appear (Bacon, 2024).

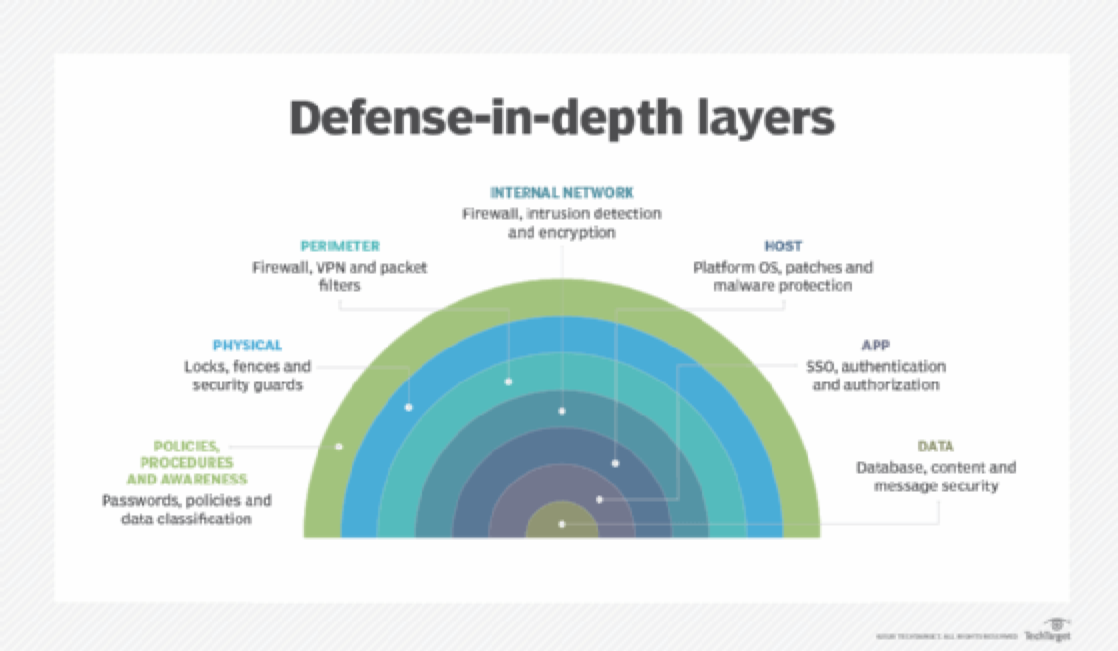

Defense-in-depth layers
INTERNAL NETWORK
Firewall, intrusion detection and encryption
PERIMETER
Firewall, VPN and packet filters
HOST
Platform OS, patches and malware protection
PHYSICAL
Locks, fences and security guards
APP
SSO, authentication and authorization
POLICIES, PROCEDURES AND AWARENESS
Passwords, policies and data classification
DATA
Database, content and message security
TechTarget

Figure 3: Defence-in-depth layers Source: (Bacon, 2024)

1.1.2 CIA Triad

The CIA Triad is a fundamental information security framework consisting of the principles of Confidentiality, Integrity, and Availability. It provides guidance for organisational security policies, with a focus on the significance of protecting data, networks, and devices. Although it shares a similar name, it is not affiliated with the Central Intelligence Agency. Instead, it is a crucial framework in the field of cybersecurity that improves the entire security stance. The CIA triad has three components (Fasulo, 2021):

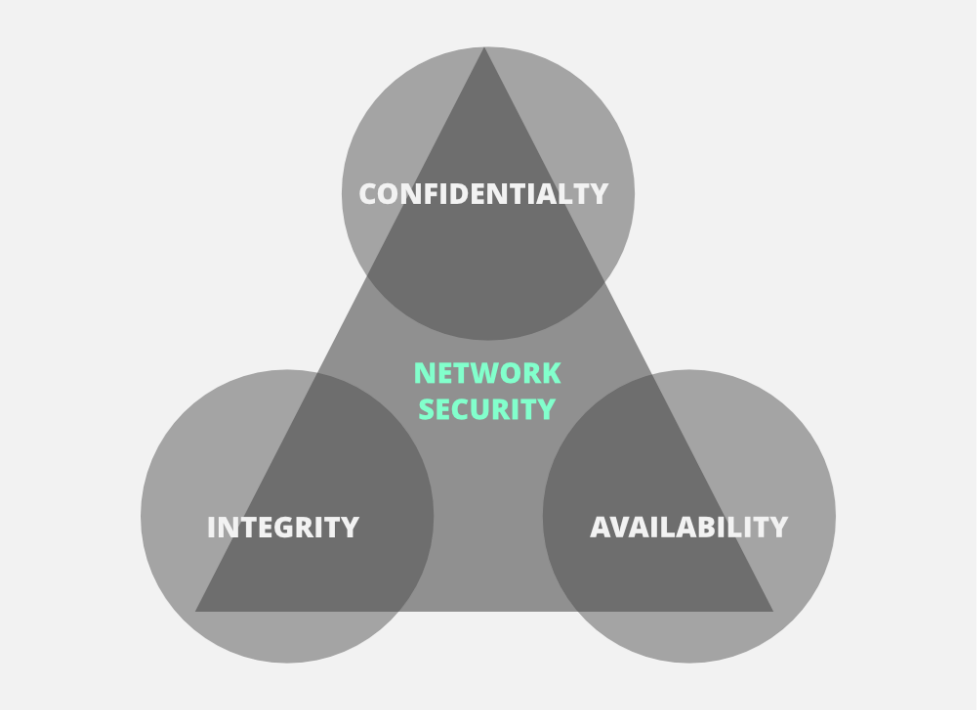


Figure 4: CIA Triad Source: (geeksforgeeks, 2024)

- **Confidentiality:** Confidentiality refers to the restriction of sensitive or classified information to only those individuals or systems who have been granted authorization. It is imperative that unauthorised individuals are prevented from accessing the data transmitted over the network. The assailant may attempt to seize the data utilising various techniques accessible on the Internet and acquire entry to your information. One effective method to prevent this is to employ encryption methods to protect your data. This ensures that even if an attacker manages to obtain your data, they will be unable to decipher it. Common encryption standards encompass AES (Advanced Encryption Standard) and DES (Data Encryption Standard). One other method to safeguard your data is by utilising a VPN tunnel. A VPN, short for Virtual Private Network, ensures secure transmission of data across a network (geeksforgeeks, 2024).

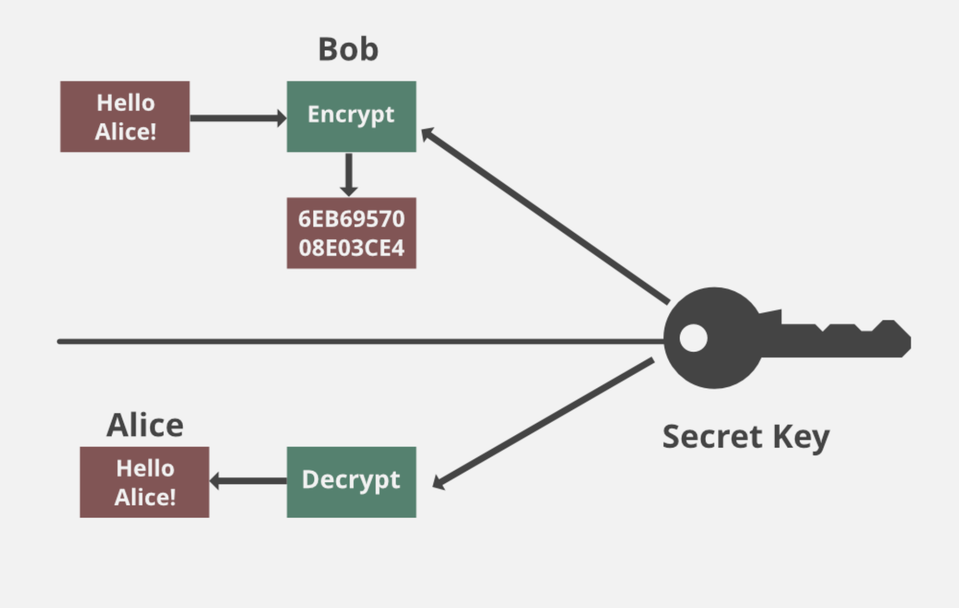


Figure 5: Example of Confidentiality Source: (geeksforgeeks, 2024)

- **Integrity:** Integrity means that the info is accurate and can be trusted. The information should be kept in its original form and protected from being changed without permission. It should also be checked to make sure it is accurate, authentic, and reliable. For example, Data should be kept in the right format, and no one should be able to change it in an incorrect manner, either by accident or on purpose. (Fasulo, 2021).
- **Availability**: This implies that the network should be easily accessible to its users. This is applicable to both systems and data. To guarantee availability, the network administrator must uphold the hardware, perform frequent updates, establish a fail-over plan, and

mitigate bottlenecks in the network. DoS or DDoS attacks can cause a network to become inaccessible by depleting its resources. The impact could have a substantial effect on the organisations and users who depend on the network as a crucial business instrument. Hence, it is imperative to implement appropriate steps to thwart such attacks (geeksforgeeks, 2024).

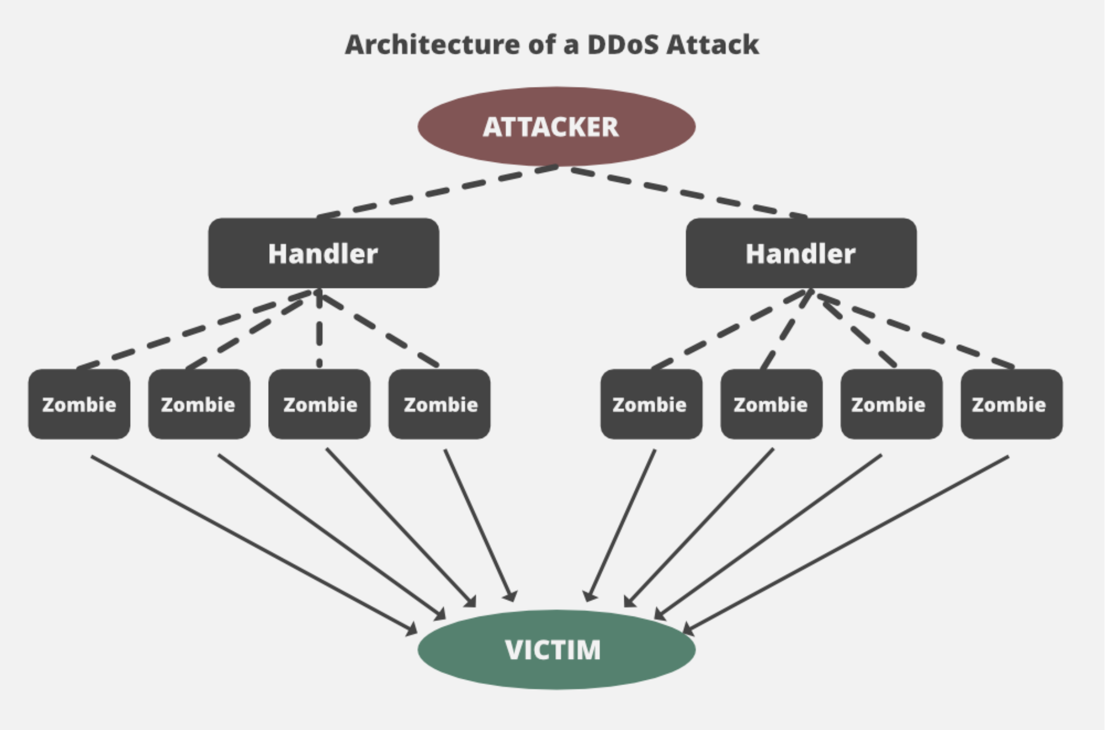


Figure 6: Example of Availability Source: (geeksforgeeks, 2024)

1.2 About Cryptography.

Figure 7:Cryptography Source: (Fortinet, 2024)

Cryptography employs encryption techniques to ensure that only the designated recipient possesses the means to decrypt and comprehend the material. The term originates from the Greek words "kryptós" meaning hidden and "graphein" meaning writing. While the term cryptography literally refers to secret writing, its primary purpose is to ensure secure transfer of data. The origins of cryptography can be traced back to the hieroglyphics used by the ancient Egyptians. Throughout the course of thousands of years, coding has undergone advancements, leading to the utilisation of intricate computer technology, engineering, and arithmetic in modern cryptography. This enables the creation of sophisticated and secure algorithms and cyphers that safeguard sensitive data in the digital era. Cryptography develops encryption protocols necessary for safeguarding data. SSL, TLS, and encryption with either 128-bit or 256-bit keys serve as illustrations. These encryption technologies protect passwords, emails, ecommerce, and financial transactions. Various types of cryptography serve distinct purposes. One of the most straightforward methods is symmetric key cryptography. The recipient is provided with the encrypted communication and a confidential key to decipher it. Regrettably, if the transmission is intercepted, a third party might easily decode and acquire the contents. Asymmetric cryptography, sometimes known as "public key" cryptography, was created by cryptologists with the aim of enhancing the security of encoding. Now, every user possesses both public and private keys. Senders require the public keys of recipients to encrypt messages. Therefore, only the private key of the recipient has the capability to decrypt it. This serves as a safeguard against any unauthorised decryption of the communication in the event of interception (Kaspersky, 2023).

1.2.1. Importance of Cryptography

Cryptography is essential to cybersecurity. This technology protects data and users by ensuring privacy and preventing data theft. Cryptography is useful in many ways (Kaspersky, 2023).

- Confidentiality keeps discussions and data private by limiting access to the intended recipient (Kaspersky, 2023).
- Cryptography protects data integrity during transmission by preventing unauthorised changes. Digital signatures show how this security method leaves marks (Kaspersky, 2023).
- Authentication verifies identities and destinations or origins.
- Non-repudiation means message senders are liable for their actions and cannot deny sending them. Digital signatures and email tracking implement non-repudiation (Kaspersky, 2023).

1.2.2. Types of cryptographic Algorithms

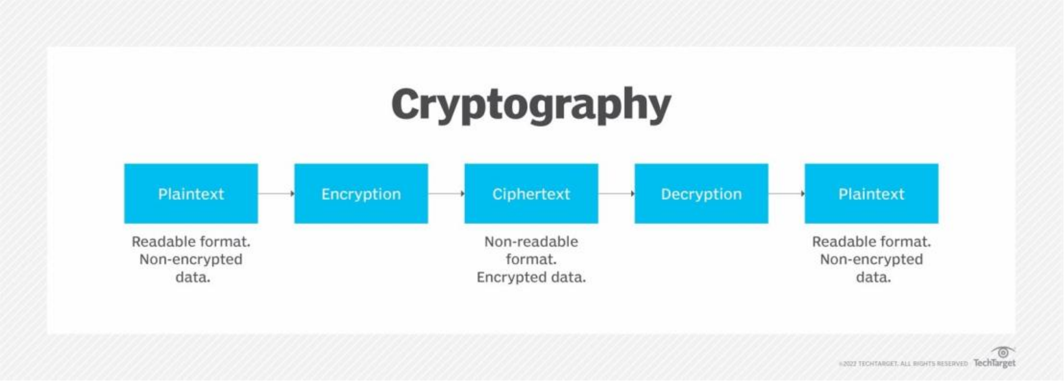

Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Figure 8: Cryptography process if encryption and decryption data Source: (Richards, 2024)

Cryptography definitions are complex. This is because the phrase covers many processes. Many cryptographic systems provide various levels of security depending on the information. Three main cryptography classifications (Kaspersky, 2023):

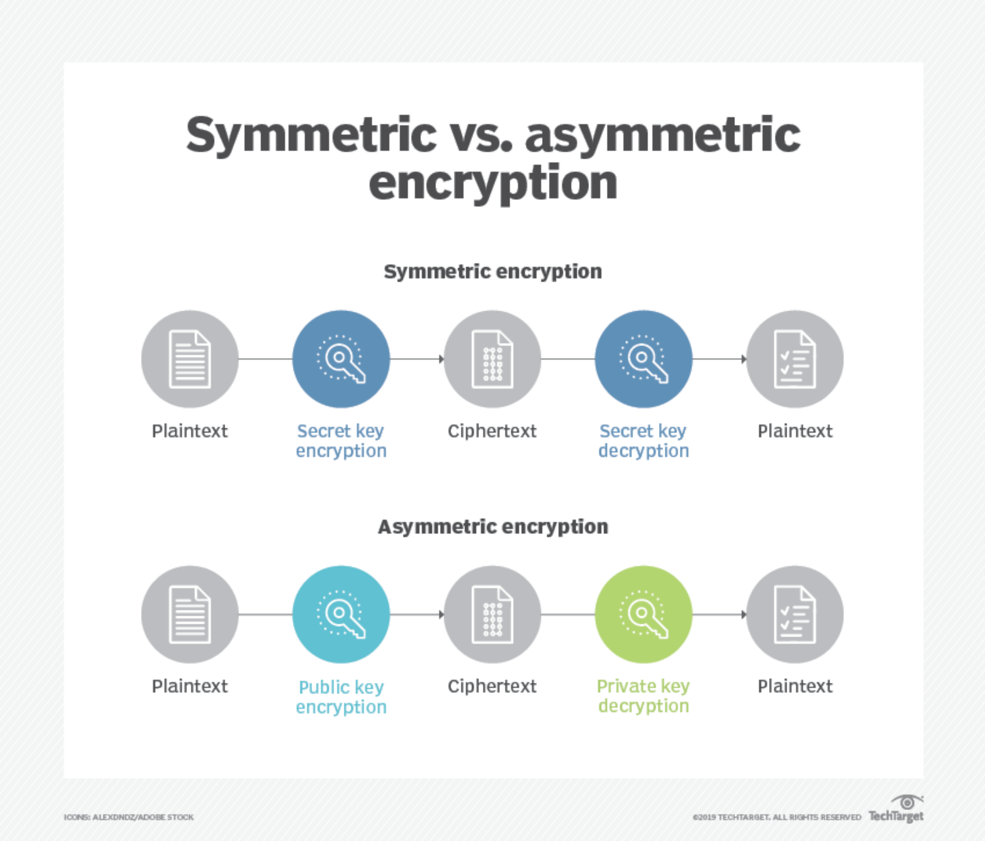


Figure 9: Symmetric vs asymmetric encryption Source: (Richards, 2024)

1. **Symmetric key cryptography**: Symmetric Key Cryptography uses the same key to encrypt and decrypt data. **DES** and **AES** are examples. The biggest challenge is securing key exchange between sender and recipient this type of cryptography exists, including are (Kaspersky, 2023):
    - **Stream ciphers**: Stream ciphers operate on individual bytes of data and frequently alter the encryption key. During this process, the keystream might either be synchronized with or separate from the message stream. These are referred to as self-synchronizing and synchronous, respectively (Kaspersky, 2023).
    - **Block ciphers**: Block ciphers such as the Feistel cipher, are a type of encryption that encode and decode data one block at a time (Kaspersky, 2023).
2. **Asymmetric key crypto**: Public-key cryptography is a secure encryption technology that requires a public and private key for both parties. The sender uses the receiver's public key to encode the message, while the recipient uses their private key to decode it. The private key is unique to the receiver, so only they can decipher the information. The most popular asymmetric cryptography algorithm is RSA (Kaspersky, 2023).

    Asymmetric key cryptography employs techniques to both encrypt and decrypt messages. These cryptographic techniques rely on mathematical principles such as multiplication, factorization, exponentiation, and logarithms. For example, by multiplying two large prime numbers, a highly complex and difficult-to-crack random number can be generated. Similarly, exponentiation and logarithms can create extremely intricate numbers that are nearly impossible to decrypt, as seen in 256-bit encryption. Various categories of asymmetric key algorithms exist, including (Kaspersky, 2023):
    - **RSA**: The initial form of asymmetric cryptography serves as the foundation for digital signatures and key exchanges, among other

applications. The algorithm relies on the notion of factorization (Kaspersky, 2023).

- **Elliptic Curve Cryptography (ECC): ECC** is a cryptographic technique commonly used in cellphones and cryptocurrency exchanges. It leverages the mathematical properties of elliptic curves to create sophisticated algorithms. Notably, it necessitates minimal storage capacity and consumption bandwidth, rendering it particularly advantageous for electronic devices with constrained computational capabilities (Kaspersky, 2023).
- **The Digital Signature Algorithm (DSA): DSA** is a cryptographic algorithm used for generating and verifying digital signatures. DSA, which stands for Digital Signature Algorithm, is a widely accepted method for verifying electronic signatures. It was developed by the National Institute of Standards and Technologies and is based on the principles of modular exponentiations (Kaspersky, 2023).
- **Identity-based Encryption (IBE)**: IBE is a cryptographic scheme that allows encryption and decryption of data depending on the identity of the user. This approach eliminates the requirement for the recipient of a message to furnish their public key to the sender. Alternatively, the sender uses a recognized distinct identifier, such as an email address, to create a public key for encrypting the communication. Subsequently, a dependable intermediary server generates an associated confidential key that the recipient can utilize to decipher the data (Kaspersky, 2023).

3. **Hash Functions**: Key-free cryptography. The length of the plain text information is used to construct a hash value, a fixed-length number that identifies data. The data is encrypted using this hash value. This strategy is used by several operating systems to protect passwords (Kaspersky, 2023).

1.2.3. Applications of Cryptography

Cryptography finds extensive use in various domains of contemporary communication, encompassing:

- **Secure online transactions**: Ensuring secure online transactions: Cryptography is employed to safeguard online transactions, such as those in online banking and e-commerce, by employing encryption to shield sensitive data and prevent unauthorized access.
- **Digital signatures**: Digital signatures serve the purpose of verifying the genuineness and unaltered state of digital documents.
- **Password protection**: Passwords are commonly secured using cryptographic methods to safeguard them against theft or interception.
- Cryptography plays a crucial role in military and intelligence domains, where it is extensively employed to safeguard confidential information and secure communication channels.

1.2.4. Challenges of Cryptography

Cryptography, although a potent means of safeguarding data, has various difficulties, such as (geeksforgeeks, 2023):

- **Key management:** Key management is a crucial aspect of cryptography as it involves the careful handling and maintenance of keys to ensure the security of communication (geeksforgeeks, 2023).
- **Quantum computing:** The advancement of quantum computing presents a possible risk to existing encryption algorithms, as they may become susceptible to attacks (geeksforgeeks, 2023).
- **Human error:** Human error poses a significant risk to the security of communication as cryptography's strength is limited by its weakest component (geeksforgeeks, 2023).

1.2.5. Cryptographic attacks

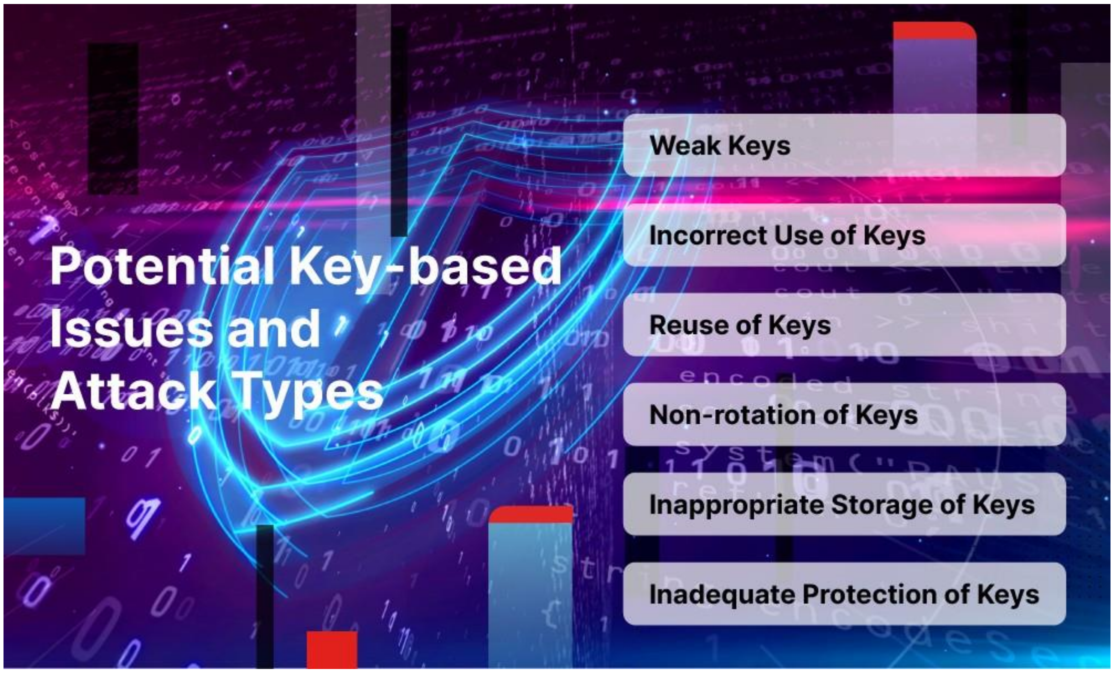

Potential Key-based Issues and Attack Types
Weak Keys
Incorrect Use of Keys
Reuse of Keys
Non-rotation of Keys
Inappropriate Storage of Keys
Inadequate Protection of Keys

Figure 10: Attack Types Source: (Fortinet, 2024)

The field of cryptography has progressed in a similar manner to other technological advancements. Nevertheless, these encryptions are susceptible to being deciphered. An infiltrated key enables an external party to decipher the encryption and access the safeguarded data. The following are potential concerns (Kaspersky, 2023):

- **Weak keys:** Random numbers are employed in an encryption technique to obfuscate data. Keys with greater length possess a larger number of digits, rendering them more challenging to decipher and hence more effective in safeguarding data (Kaspersky, 2023).
- **Improper key utilization:** Cybercriminals can effortlessly decipher keys to get entry to safeguarded information (Kaspersky, 2023).
- **Reusing keys:** Keys must possess uniqueness akin to passwords, as sharing them compromises the integrity of cryptography's safeguarding of data (Kaspersky, 2023).

- **Key rotation:** Cryptographic keys have a short lifespan, therefore constantly changing them safeguards data (Kaspersky, 2023).
- **Recklessly storing keys:** Ensure keys are securely stored to avoid theft and unauthorized access to data (Kaspersky, 2023).
- **Inside attacks:** Insider attacks occur when employees illicitly acquire and subsequently sell keys (Kaspersky, 2023).
- **Failure to create a backup:** In the event of key failure, the data they safeguard may become unavailable (Kaspersky, 2023).
- **Inaccurate key recording**: Inputting keys manually into a spreadsheet or writing them on paper may appear logical, but it is susceptible to mistakes and theft (Kaspersky, 2023).

There are specialized cryptographic attacks that aim to bypass encryptions by identifying the correct key. Here are some of the prevalent (Kaspersky, 2023):

- **Brute force attacks:** Brute force attacks refer to extensive and indiscriminate attempts to guess private keys by employing the known technique (Kaspersky, 2023).
- **Ciphertext-only attacks:** These attacks entail a third party intercepting the encrypted message, rather than the plaintext, and attempting to deduce the decryption key to access the information, including the plaintext, at a later stage (Kaspersky, 2023).
- **Chosen ciphertext attack:** In contrast to a chosen plaintext attack, this type of attack involves the analysis of a portion of ciphertext to deduce the associated plaintext and uncover the encryption key (Kaspersky, 2023).
- **Chosen plaintext attack:** In this scenario, a third party selects the plaintext and uses it to determine the encryption key that corresponds to a specific ciphertext (Kaspersky, 2023).

- **Known plaintext attack:** In this scenario, the assailant gains unauthorized access to a portion of the original message and a portion of the encrypted message and proceeds to deduce the encryption key. This is less applicable for contemporary cryptography as it is most effective with uncomplicated ciphers (Kaspersky, 2023).
- **Algorithm attack:** During these assaults, the cybercriminal scrutinizes the algorithm to deduce the encryption key (Kaspersky, 2023).

1.2.6. Way to mitigate the threat of cryptography attack.

There are several strategies that individuals and organizations can employ to mitigate the risk of a cryptographic assault. Essentially, this entails guaranteeing the effective administration of keys to minimize the risk of interception by a third party, or to ensure their usability even in the event of interception. Below are few recommendations (Kaspersky, 2023):

- Assign a distinct key for each specified function, such as utilizing separate keys for authentication and digital signatures.
- Enhance the security of cryptographic keys by utilizing more robust Key-encryption-keys (KEKs).
- Utilize hardware security modules for the purpose of managing and safeguarding keys. These modules operate in a similar manner to conventional password managers.
- Regularly update keys and algorithms.
- Apply encryption to every data that contains sensitive information.
- Generate robust and distinct keys for every encryption objective.
- Ensure that keys are stored in a highly secure manner to prevent unauthorized access by external entities.
- Verify the accurate execution of the cryptographic system.
- Incorporate cryptography into the security awareness training provided to employees.

2. Background of the selected Cryptographic Algorithm

2.1. Caesar **Cipher**

The Shift (or Caesar) Cipher is a type of monoalphabetic substitution cipher. While the Atbash Cipher is relatively more secure than other ciphers, it remains susceptible to decryption, particularly when compared to modern cryptographic standards. Initially, Julius Caesar employed it for transmitting encoded messages to his soldiers, as documented by Suetonius (Corner, 2024):

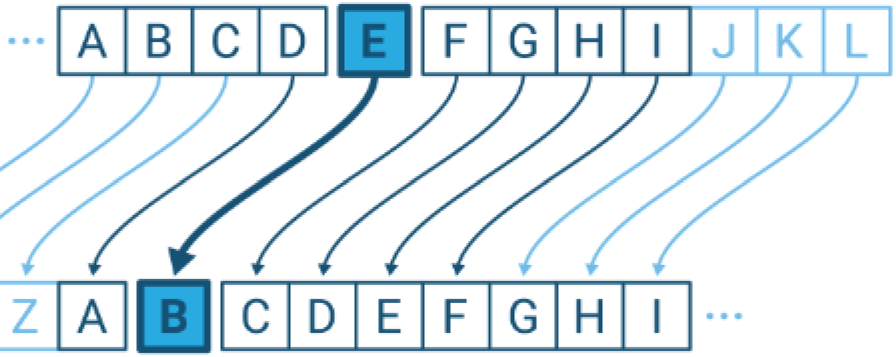


Figure 11: Caesar Cipher Source: (Sarkar, 2020)

Process of Encryption:

- Key Generation: The shift is determined by a number ranging from 1 to 25, excluding 26 (Sarkar, 2020).
- Encryption Algorithm: The process of shifting each letter of the plaintext by a specific key value to generate the corresponding ciphertext (Sarkar, 2020).

Process of decrypting:

- Decryption Algorithm: Reverses the encryption process by shifting each letter of the ciphertext backwards according to the key (Sarkar, 2020).

Limitations:

- There are only 25 distinct options for encoding a plaintext letter into a ciphertext letter (Sarkar, 2020).
- Lacking security because of easily identifiable patterns in the encrypted message (Sarkar, 2020).

Lack of confidence or self-assurance Reasons:

- Retains the inherent structures inside the text, facilitating the decryption process for anybody attempting to crack the code (Sarkar, 2020).
- -A brute force attack can be performed since the key range is confined to numbers between 1 and 25 (Sarkar, 2020).
- Modern processing power enables rapid decryption attempts (Sarkar, 2020).

Key Points:

- Pattern Preservation: Encryption maintains the patterns present in the plaintext within the ciphertext (Sarkar, 2020).
- Predictability: The constrained range of possible keys facilitates straightforward decryption through brute force methods (Sarkar, 2020).
- Vulnerability: Adversaries can leverage persistent patterns to decrypt code without requiring the precise key (Sarkar, 2020).

Although the Caesar cipher has been historically utilized and is straightforward, it is no longer secure in contemporary times because of its predictable patterns and vulnerability to brute force attacks. Although it may possess historical significance, it is not appropriate for ensuring safe communication in the present day (Sarkar, 2020).

Advantage	Disadvantage
- Simplicity - Ease of Memorization - Single Key Usage - Low Computing Resource Requirement - Quick Message Translation - Suitable for simple system	- Vulnerability to Unauthorized Access - Minimum Security Layer - Pattern Recognition

(Gatekeeper, 2024)

2.2. Rail fence cipher

A transposition cipher is a cryptographic technique that employs a specific algorithm based on a zigzag pattern to rearrange the order of characters in a message (Sharma, 2023).

Process of Encryption:

- The plaintext message is arranged in a zigzag manner across rows, often known as rails (Sharma, 2023).
- In the technique of Alternate Line Writing, letters are arranged diagonally on consecutive rails, resulting in a rectangular box-like depiction (Sharma, 2023).
- Nulls/Placeholders: If necessary for alignment purposes, nulls (such as the letter "X") are inserted as placeholders to ensure equilibrium between the top and bottom rows (Sharma, 2023).

Cipher Text: IOAOTMRG

- Encrypted message: "I AM GROOT" with a key size (number of rails) of 4.
- Encryption Method: The plaintext is arranged in a zigzag pattern over rails, with the possibility of introducing nulls for alignment purposes.
- The encrypted text is "IOAOTMRG" after applying the encryption algorithm.

Decryption Process:

- Matrix Reconstruction: Rebuilding the rail fence matrix using the identical key size employed during encryption (Sharma, 2023).
- Ciphertext Placement: The arrangement of ciphertext characters in the matrix according to the zigzag pattern (Sharma, 2023).
- Zigzag Path Reversal: Extracting the original plaintext by reading the matrix in a pattern that alternates between upward and downward movements (Sharma, 2023).

Key Points:

- **Zigzag Enciphering:** The text is arranged in a zigzag fashion along rails, creating a rectangular box (Sharma, 2023).
- **Transposition Technique:** The transposition technique involves rearranging the sequence of characters, so functioning as a transposition cipher (Sharma, 2023).
- -**Nulls for Alignment:** Optional placeholders employed to establish parity in the number of characters between the upper and lower rows, facilitating the process of decipherment (Sharma, 2023).

The Rail Fence Cipher functions by rearranging the plaintext message in a zigzag pattern along rails and subsequently recovering the original message by adhering to the same pattern during decryption. The transposition cipher is a fundamental encryption method that is relatively simple to execute. However, it may not be sufficiently secure for contemporary cryptographic requirements because of its predictable nature (Sharma, 2023).

Advantage	Disadvantage
• Simplicity • Ease of use • Flexibility	• Lack Of Security • Limited Effectiveness • Vulnerability to Attacks • No Key Management • Not Suitable for secure Communication

(Datta, 2023)

2.3. Playfair Cipher

Symmetric encryption technique that employs digraph encryption, encrypting pairs of two letters instead of individual letters. The Playfair Cypher employs a symmetrical encryption method, where pairs of letters are encrypted. This is achieved by utilising a key matrix that is derived from a keyword and other non-repeating letters of the alphabet. The encryption and decryption procedures of this system utilise matrix retrieval and particular algorithms based on the letter positions inside the matrix (intellipaat, 2023).

Key Matrix Creation:

- A 5x5 matrix is initially generated using a keyword (e.g., "ATHENS").
- The use did not provide any text. The keyword establishes the initial row, consisting of distinct letters in a specific order, followed by the other letters of the alphabet without any repetitions (intellipaat, 2023).

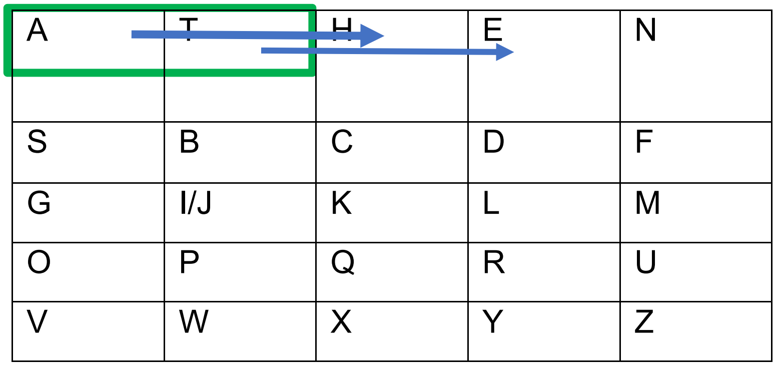
A	T	H	E	N
S	B	C	D	F
G	I/J	K	L	M
O	P	Q	R	U
V	W	X	Y	Z

Rules for Encryption:

- Digraph Formation: The process of splitting plaintext into digraphs. If the number is odd, add the letter "X" to form pairs (intellipaat, 2023).
- Matrix Lookup: Identify the positions of the letters in the key matrix for each digraph (intellipaat, 2023).

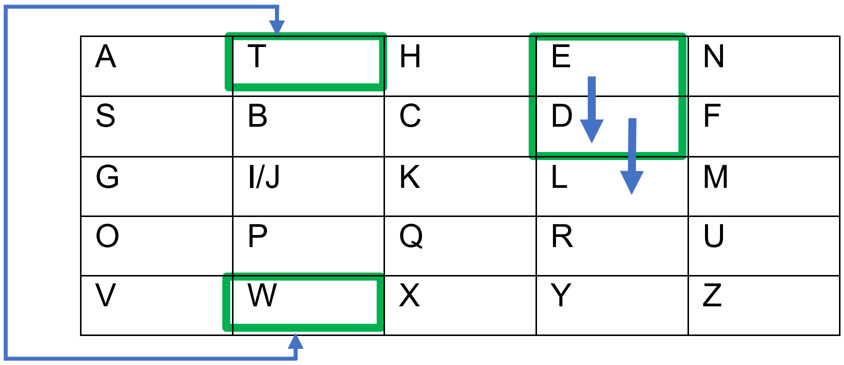
There are three possible scenarios:

1. In the same row, substitute each letter with the letter directly to its right. Enclose as necessary (intellipaat, 2023).



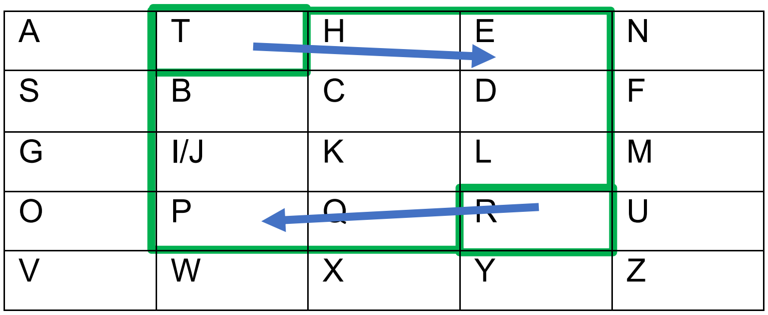
A	T	H	E	N
S	B	C	D	F
G	I/J	K	L	M
O	P	Q	R	U
V	W	X	Y	Z

2. In the same column: Substitute each letter with the one directly beneath it. If necessary, encircle or surround (intellipaat, 2023).



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

3. Correspondence between rows and columns: Select the diagonally opposite corner of the rectangle created by the two letters (intellipaat, 2023).



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

Decryption Rules:

- The decryption method involves undoing the encryption stages by utilising the identical key matrix to convert digraphs back into plaintext (intellipaat, 2023).
- The user did not provide any text. The process entails traversing horizontally across rows and vertically upwards along columns to locate the original letters (intellipaat, 2023).

Key Points:

- **Digraph Encryption**: Functions by encrypting letter pairings via a key matrix.
- **Matrix Generation**: The primary matrix is created by combining a keyword with the remaining non-repetitive letters of the alphabet.
- **Encryption Process:** The encryption process encompasses several scenarios depending on the arrangement of letters within the matrix, such as being in the same row, same column, or creating a rectangle.
- **Symmetric encryption**: Symmetric encryption employs an identical key and procedure for both encryption and decryption.

Advantages	Disadvantages
• Strong Encryption • Polygram Substitution • simplicity	• Key Distribution • Limited Key Space • Vulnerability to known Plaintext Attacks • Lack of Perfect Secrecy

(Sileshi, 2023)

3. Development of a New Algorithm (**RootInRoot**)

3.1. Modifications that can be carried out in Caesar Cipher.

1. Caesar Cipher with Unique Word Keys:

- The keys for each word are determined by prime integers; for example, I=2, A=3, M=5, G=7, R=11, O=13, and T= 19.
- By assigning unique keys to each word, this update makes the Caesar cipher more difficult to crack.

3.1.1. Encryption Example with modification:

KEY Value: Ascending Prime number for every letter.

Plain Text: I AM GROOT

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T

20	21	22	23	24	25
U	V	W	X	Y	Z

Formula for encryption: C = (p + k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19

I = (8 + 2) mod26 = 10 = K	R = (17 + 11) mod26 = 28 mod=2 = C
A = (0 + 3) mod26 = 3 = D	O = (14 +13) mod26 = 27 mod=1 = B
M = (12 + 5) mod26 = 17 = R	O = (14 +17) mod26 = 31 mod= 5 =F
G = (6 + 7) mod26 = 13 = N	T = (19 + 19) mod26 = 38 mod= 12= M

Cipher Text: KDRNCBFM

3.1.2. Decryption Example with modification:

P = (c - k) mod26

K = (10 - 2) mod26 = 8 = I	C = (2 - 11) mod26 = -9 mod=17 = R
D = (3 - 3) mod26 = 0 = A	B = (1 -13) mod26 = -12 mod=14 = O
R = (17 - 5) mod26 = 12 = M	F = (5 -17) mod26 =-12 mod=14 = O
N = (13 - 7) mod26 = 6 = G	M= (12 - 19) mod26 = -7 mod=19 = T

Plain Text: I AM GROOT

3.2. Modifications that can be carried out in Rail fence cipher.

2. The Rail Fence Cipher with Key Value 4:

- The plaintext for the Rail Fence cipher is the ciphertext created by the modified Caesar cipher.
- Encryption and decryption keys for the Rail Fence cipher are set to 4 as a further modification.

3.2.1. Encryption Example with modification:

Key Size :4

Plain Text: I AM GROOT

I						**O**	
	A				**O**		**T**
		M		**R**			
			G				

Cipher Text: IOAOTMRG

3.2.2. Decryption Example with modification:

Key Size :4

Cipher Text: IOAOTMRG

I						O	
	-				-		-
		-		-			
			-				

I						O	
	A				O		T
		-		-			
			-				

I						O	
	A				O		T
		M		R			
			-				

I						O	
	A				O		T
		M		R			
			G				

Plain Text: I AM GROOT

3.3. Modifications that can be carried out in Playfair Cipher.

3. Playfair Cipher with Shifts and Rules:

- Playfair cipher, which uses shifts and rules. It takes the decipher text from the Rail Fence cipher and applies it to it.
- And we give a Key in this section which will be used for encryption and decryption process.
- After that we start the process of encryption by using 5*5 box matrix.

Regarding the Playfair cipher:

- Letters that appear in the same column will be moved down two spaces.
- They are moved two spaces to the right if they share a row.
- If the columns and rows containing the letters are not the same, then the usual Playfair rules are applicable.

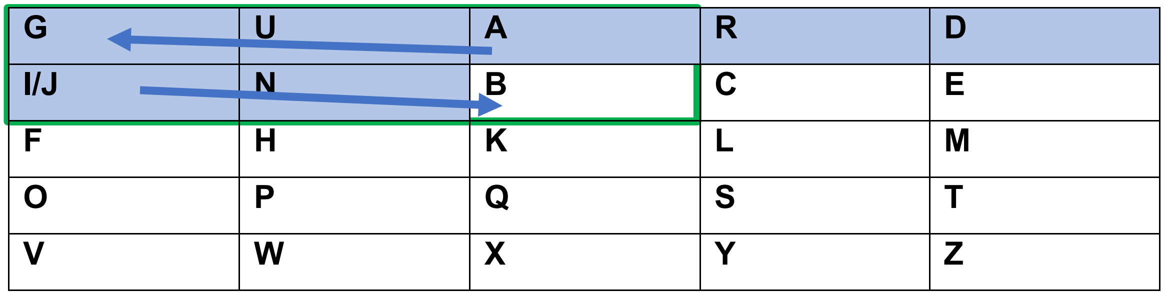
3.3.1. Encryption Example with modification: While sifting in “Column” or “Row” shift by 2.

Key Value: GUARDIAN

Plain Text: I AM GROOT

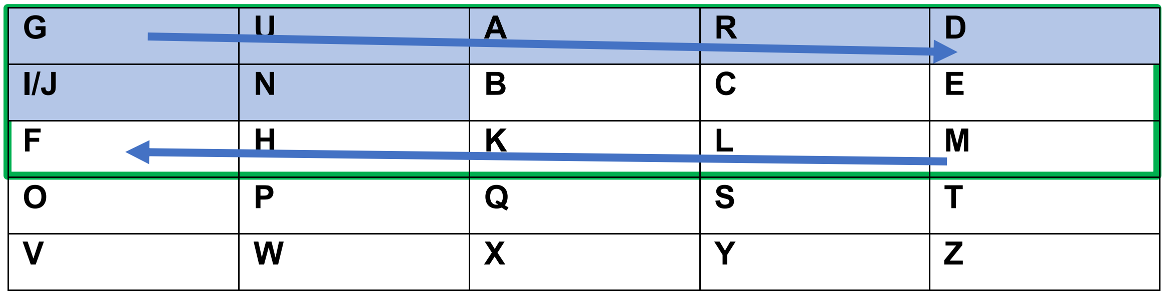
Diagram: IA MG RO OT

Using 5*5 Matrix



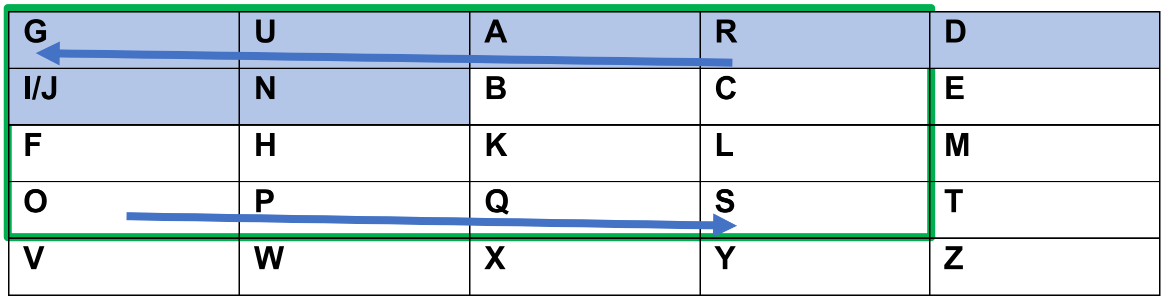
G	U	A	R	D
I/J	N	B	C	E
F	H	K	L	M
O	P	Q	S	T
V	W	X	Y	Z

IA= BG



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

MG = FD



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

RO = GS

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

OT =QP

Cipher Text: BG FD GS QP

Final Cipher Text= BGFDGSQP

3.3.2. Decryption Example with modification: While sifting in “Column” or “Row” shift by 2.

Key Value: GUARDIAN

Cipher Text: BGFDGSQP

Diagram: BG FD GS QP

Using 5*5 Matrix

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

BG = IA

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

FD = MG

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

GS = RO

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

QP = OT

Plain Text: I AM GROOT

3.4. Summary

In this comprehensive encryption approach, a series of distinct keys are utilized at each step. In the Caesar cipher, prime numbers serve as key values for encryption, introducing an additional layer of complexity. The resulting ciphertext from the Caesar cipher is then subjected to the Rail Fence cipher, using a fixed key value of 4. Subsequently, the key generated by the Rail Fence cipher is further encrypted using the Playfair cipher, with a specific key provided for this encryption step. The entire process is repeated until all three techniques are applied, generating a new ciphertext at each stage.

To decipher the message, the reverse order of operations is performed, with Playfair, Rail Fence, and Caesar decryptions executed sequentially using the same set of keys. This multi-layered method significantly enhances the security of the encryption procedure, as each cipher builds upon the complexity introduced by the preceding one.

4. Test Cases of New cryptographic algorithm named **RootInRoot.**

4.1.1. Test 1: Encryption

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T

20	21	22	23	24	25
U	V	W	X	Y	Z

KEY Value: Ascending Prime number for every letter.

Plain Text: PATRICK THE PRO

Formula for encryption: C = (p + k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

P = (15+ 2) mod26 = 17= R
A = (0 + 3) mod26= 3 =D
T = (19 +5) mod26= 24 =Y
R = (17 + 7) mod26= 24 = Y
I = (8 + 11) mod26= 19 =T
C = (2 + 13) mod26= 15 = P
K = (10 + 17) mod26=27= mod=1=B
T = (19 + 19) mod26= 38= mod=12=M
H = (7 + 23) mod26= 30= mod=4=E
E = (4 + 29) mod26= 33= mod=7=H
P = (15 + 31) mod26=46= mod=20=U
R = (17 + 37) mod26= 54=mod=2=C
O = (14 + 41) mod26= 55=mod=3=D

Cipher Text: RDYYTPBMEHUCD

Again, using Cipher Text as a Plain text

Key Value: 4

Plain Text: RDYYTPBMEHUCD

now,

R						B						D
	D				P		M				C	
		Y		T				E		U		
			Y						H			

Cipher Text: RBDDPMCYTEUYH

Again, using Cipher Text as a Plain text

Key Value: FATHER

Plain Text: RBDDPMCYTEUYH

Diagram: RB DX DP MC YT EU YH

Now,

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

Plain Text	RB	DX	DP	MC	YT	EU	YH
Cipher Text	CD	CY	BS	LD	XH	NE	DM

Final Cipher Text: CDCYBSLDXHNEDM

4.1.1.1: Decryption:

Key Value: FATHER

Cipher Text: CDCYBSLDXHNEDM

Diagram: CD CY BS LD XH NE DM

Now

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

Cipher Text	CD	CY	BS	LD	XH	NE	DM
Plain Text	RB	DX	DP	MC	YT	EU	YH

Diagram: RB DX DP MC YT EU YH

Plain Text: RBDDPMCYTEUYH

Again, **Using Plain Text as a Cipher Text**

Key Value: 4

Cipher Text: RBDDPMCYTEUYH

now,

R						B						D
	D				P		M				C	
		Y		T				E		U		
			Y						H			

Plain Text: RDYYTPBMEHUCD

Again, **Using Plain Text as a Cipher Text**

KEY Value: Ascending Prime number for every letter.

Cipher Text: RDYYTPBMEHUCD

Formula for encryption: C = (p + k) mod26

Prime Number: 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

R = (17 - 2) mod26 = 15 = P
D = (3 - 3) mod26= 0 = A
Y = (24 -5) mod26= 19 =T
Y = (24 - 7) mod26= 17 = R
T = (19 - 11) mod26= 8 =I
P = (15 - 13) mod26= 2 = C
B = (1 - 17) mod26= -16= mod=10=K
M = (12 - 19) mod26= -7 = mod=19=T
E = (4 - 23) mod26= -19 = mod=7=H
H = (7 - 29) mod26= -22 = mod=4=E
U = (20 - 31) mod26= -11= mod=15=P
C = (2 - 37) mod26= -35 =mod=17=R
D = (3 - 41) mod26= -38 =mod=14=O

Final Plain Text: PATRICK THE PRO

4.1.2. Test 2: Encryption

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T

20	21	22	23	24	25
U	V	W	X	Y	Z

KEY Value: Ascending Prime number for every letter.

Plain Text: IN THE WOODS

Formula for encryption: C = (p + k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

I= (8 + 2) mod26 =10 = K
N= (13 + 3) mod26 =16 =Q
T= (19 + 5) mod26 =24 =Y
H= (7 + 7) mod26 =14 =O
E= (4 + 11) mod26 =15 =P
W= (22+13) mod26 =35 mod26= 9 =J
O= (14+17) mod26 =31 mod26=5 =F
O= (14+19) mod26 =33 mod26=7 = H
D= (3+23) mod26 =26 mod26=0 =A
S= (18+29) mod26 =47 mod26=21 =V

Cipher Text: KQYOPJFHAV

Again, using Cipher Text as a Plain text

Key Value: 4

Plain Text: KQYOPJFHAV

now,

K						F			
	Q				J		H		
		Y		P				A	
			O						V

Cipher Text: KFQJHYPAOV

Again, using Cipher Text as a Plain text

Key Value: MAKE

Plain Text: KFQJHYPAOV

Diagram: KF QJ HY PA OV

Now,

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

Plain Text	KF	QJ	HY	PA	OV
Cipher Text	NS	MV	GZ	LB	YI

Final Cypher Text: NSMVGZLBYI

4.1.2.1. Decryption:

Key Value: MAKE

Cipher Text: NSMVGZLBYI

Diagram: NS MV GZ LB YI

Now,

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

Cipher Text	NS	MV	GZ	LB	YI
Plain Text	KF	QJ	HY	PA	OV

Diagram: KF QJ HY PA OV

Plain Text: KFQJHYPAOV

Again, Using Plain Text as a Cipher Text

Key Value: 4

Cipher Text: KFQJHYPAOV

now,

K						F			
	Q				J		H		
		Y		P				A	
			O						V

Plain Text: KQYOPJFHAV

Again, Using Plain Text as a Cipher Text

KEY Value: Ascending Prime number for every letter.

Cipher Text: KQYOPJFHAV

Formula for encryption: P = (c - k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

Now,

K= (10 - 2) mod26 =8 = I
Q= (16 - 3) mod26 =13 =N
Y= (24 - 5) mod26 =19 =T
O= (14 - 7) mod26 =7 =H
P= (15 - 11) mod26 =4 =E
J= (9-13) mod26 = -4 mod26= 22=W
F= (5-17) mod26 = -12 mod26= 14=O
H= (7-19) mod26 = -12 mod26= 14 = O
A= (0-23) mod26 = -23 mod26= 3 =D
V= (21-29) mod26 = -8 mod26= 18 =S

Plain Text: IN THE WOODS

Final Plain Text: IN THE WOODS

4.1.3. Test 3: Encryption

Encryption:

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T

20	21	22	23	24	25
U	V	W	X	Y	Z

KEY Value: Ascending Prime number for every letter.

Plain Text: I AM IRON MAN

Formula for encryption: C = (p + k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

I = (8+2) mod26= 10=K
A= (0+3) mod26=3=D
M= (12+5) mod26=17=R
I= (8+7) mod26=15 =P
R= (17+11) mod26=28 mod26=2=C
O= (14+13) mod26=27 mod26=1=B
N= (13+17) mod26=30 mod26=4 =E
M= (12+19) mod26=31 mod26=5 =F
A= (0+23) mod26=23 =X
N= (13+29) mod26=42 mod26=16=Q

Cipher Text: KDRPCBEFXQ

Again, **using Cipher Text as a Plain text**

Key Value: 4

Plain Text: KDRPCBEFXQ

now,

K						E			
	D				B		F		
		R		C				X	
			P						Q

Cipher Text: KEDBFRCXPQ

Again, using Cipher Text as a Plain text

Key Value: MANGO

Plain Text: KEDBFRCXPQ

Diagram: KE DB FR CX PQ

Now,

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

Plain Text	KE	DB	FR	CX	PQ
Cipher Text	LD	FD	CU	DW	HU

Diagram: LD FD CU DW HU

Final Cipher Text: LDFDCUDWHU

4.1.3.1. Decryption:

Key Value: MANGO

Cipher Text: LDFDCUDWHU

Diagram: LD FD CU DW HU

Now,

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

Cipher Text	LD	FD	CU	DW	HU
Plain Text	KE	DB	FR	CX	PQ

Diagram: KE DB FR CX PQ

Plain Text: KEDBFRCXPQ

Again, Using Plain Text as a Cipher Text

Key Value: 4

Cipher Text: KEDBFRCXPQ

now,

K						E			
	D				B		F		
		R		C				X	
			P						Q

Plain Text: KDRPCBEFXQ

Again, Using Plain Text as a Cipher Text

KEY Value: Ascending Prime number for every letter.

Cipher Text: KDRPCBEFXQ

Formula for encryption: P = (c - k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

K= (10-2) mod26= 8=I
D= (3-3) mod26=0=A
R= (17-5) mod26=12=M
P= (15-7) mod26=8 =I
C= (2-11) mod26= -9 mod26=17=R
B= (1-13) mod26= -12 mod26=14=O
E= (4-17) mod26= -13 mod26=13 =N
F= (5-19) mod26= -14 mod26=12 =M
X= (23-23) mod26=0 =A
Q= (16-29) mod26= -13 mod26=13=N

Final Plain Text: I AM IRON MAN

4.1.4. Test 4: Encryption

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T

20	21	22	23	24	25
U	V	W	X	Y	Z

KEY Value: Ascending Prime number for every letter.

Plain Text: THE ONE AND ONLY

Formula for encryption: C = (p + k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

Now,

T = (19+2) mod26=21 =**V**
H= (7+3) mod26=10 =**K**
E= (4+5) mod26=9=**J**
O= (17+7) mod26=21=**V**
N= (13+11) mod26=24=**Y**
E= (4+13) mod26=17=**R**
A= (0+17) mod26=17=**R**
N= (13+19) mod26=32 mod26=6=**G**
D= (3+23) mod26=26 mod26=0=**A**
O= (14+29) mod26=43 mod26=17=**R**
N= (13+31) mod26=44 mod26=18=**S**
L= (11+37) mod26=48 mod26=22=**W**
Y= (24+41) mod26=65 mod26=13=**N**

Cipher Text: VKJVYRRGARSWN

Again, **using Cipher Text as a Plain text**

Key Value: 4

Plain Text: VKJVYRRGARSWN

now,

V						R						N
	K				R		G				W	
		J		Y				A		S		
			V						R			

Cipher Text: VRNKRGWJYASVR

Again, using Cipher Text as a Plain text

Key Value: IRONMAN

Plain Text: VRNKRGWJYASVR

Diagram: VR NK RG WJ YA SV RX

Now,

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

Plain Text:	VR	NK	RG	WJ	YA	SV	RX
Cipher Text:	WI	KY	GW	VR	VD	PX	OW

Final Cipher Text: WIKYGWVRVDPXOW

4.1.4.1. Decryption:

Key Value: IRONMAN

Cipher Text: WIKYGWVRVDPXOW

Diagram: WI KY GW VR VD PX OW

Now,

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

Cipher Text:	WI	KY	GW	VR	VD	PX	OW
Plain Text:	VR	NK	RG	WJ	YA	SV	RX

Plain Text: VRNKRGWJYASVRX

Again, Using Plain Text as a Cipher Text

Key Value: 4

Cipher Text: VRNKRGWJYASVRX

now,

V						R						N
	K				R		G				W	
		J		Y				A		S		
			V						R			

Plain Text: VKJVYRRGARSWN

Again, **Using Plain Text as a Cipher Text**

KEY Value: Ascending Prime number for every letter.

Cipher Text: VKJVYRRGARSWN

Formula for encryption: P = (c - k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

Now,

V = (21-2) mod26=19 =**T**
K = (10-3) mod26= 7=**H**
J = (9-5) mod26=4=**E**
V = (21-7) mod26=14=**O**
Y = (24-11) mod26=13=**N**
R = (17-13) mod26=4=**E**
R = (17-17) mod26=0=**A**
G = (6-19) mod26=-13 mod26=13=**N**
A = (0-23) mod26= -23 mod26=3=**D**
R = (17-29) mod26= -12 mod26=14=**O**
S = (18-31) mod26= -13 mod26=13=**N**
W = (22-37) mod26= -15 mod26=11=**L**
N = (13-41) mod26= -28 mod26=24=**Y**

Final Plain Text: THE ONE AND ONLY

4.1.5. Test 5: Encryption

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T

20	21	22	23	24	25
U	V	W	X	Y	Z

KEY Value: Ascending Prime number for every letter.

Plain Text: AVENGERS ASSEMBLE

Formula for encryption: C = (p + k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

Now,

A= (0+2) mod26= 2 =**C**
V= (21+3) mod26=24 =**Y**
E= (4+5) mod26=9 =J =**J**
N= (13+11) mod26=24 =**Y**
G= (6+13) mod26=19 =**T**
E= (4+17) mod26=21=**V**
R= (17+19) mod26=36 mod26=10 =**K**
S= (18+23) mod26=41 mod26=15 =**P**
A= (0+29) mod26=29 mod26=3 =**D**
S= (18+31) mod26=49 mod26=23 =**X**
S= (18+37) mod26=55 mod26=3 =**D**
E= (4+41) mod26=45 mod26=19 =**T**
M= (12+43) mod26=55 mod26=3 =**D**
B= (1+47) mod26=48 mod26=22 =**W**
L= (11+53) mod26=64 mod26=12 =**M**
E= (4+59) mod26=63 mod26=11 =**L**

Cipher Text: CYJYTVKPDXDTDWML

Again, using Cipher Text as a Plain text

Key Value: 4

Plain Text: CYJYTVKPDXDTDWML

Now,

C						K						D			
	Y				V		P				T		W		
		J		T				D		D				M	
			Y						X						L

Cipher Text: CKDYVPTWJTDDMYXL

Again, using Cipher Text as a Plain text

Key Value: LOKI

Plain Text: CKDYVPTWJTDDMYXL

Diagram: CK DY VP TW JT DX DM YX LX

Now,

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

Plain Text	CK	DY	VP	TW	JT	DX	DM	YX	LX
Cipher Text	DO	EX	ZG	RY	NI	SD	SX	VZ	KV

Final Cipher Text: DOEXZGRYNISDSXVZKV

4.1.5.1. Decryption:

Key Value: LOKI

Cipher Text: DOEXZGRYNISDSXVZKV

Diagram: DO EX ZG RY NI SD SX VZ KV

Now,

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

Cipher Text	DO	EX	ZG	RY	NI	SD	SX	VZ	KV
Plain Text	CK	DY	VP	TW	JT	DX	DM	YX	LX

Diagram: CK DY VP TW JT DX DM YX LX

Plain Text: CKDYVPTWJTDDMYXL

Again, Using Plain Text as a Cipher Text

Key Value: 4

Cipher Text: CKDYVPTWJTDDMYXL

Now,

C						K						D			
	Y				V		P				T		W		
		J		T				D		D				M	
			Y						X						L

Plain Text: CYJYTVKPDXDTDWML

Again, Using Plain Text as a Cipher Text

KEY Value: Ascending Prime number for every letter.

Cipher Text: CYJYTVKPDXDTDWML

Formula for encryption: P = (c - k) mod26

Prime Number: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61……

Now,

C= (2-2) mod26= 0 =A
Y= (24-3) mod26=21 =V
J= (9-5) mod26=4 =E
Y= (24-11) mod26=13 =N
T= (19-13) mod26=6 =G
V= (21-17) mod26=4=E
K= (10-19) mod26= -9 mod26=17 =R
P= (15-23) mod26=-8 mod26=18 =S
D= (3-29) mod26= -26 mod26=0 =A
X= (23-31) mod26= -8 mod26= 18 =S
D= (3-37) mod26= -34 mod26=18 =S
T= (19-41) mod26= -22 mod26=4 =E
D= (3-43) mod26= -40 mod26= 12 =M
W= (22-47) mod26= -25 mod26=1 =B
M= (12-53) mod26= -41 mod26= 11 =L
L= (11-59) mod26= -48 mod26=4 =E

Final Plain Text: AVENGERS ASSEMBLE

5. New cryptographic algorithm

Within this section, we shall thoroughly evaluate both the advantages and disadvantages of the recently devised encryption algorithm, drawing from the information presented.

Strengths:

1. **Simplicity:** The algorithm's simplicity makes it user- and developer-friendly. The ease of use and connection into different systems makes it a potential advantage for rapid deployment.
2. **Customizable Key Size:** Since the technique uses ascending prime integers for each letter to determine the key value, it allows for a changeable key size. By giving consumers the option to choose stronger keys, this flexibility can improve security.
3. **Reversibility:** The original message can be correctly reconstructed if the key is known because the encryption and decryption operations are reversible. For cryptography to be useful, this quality is required.
4. **Resistance to known-Plaintext Attacks:** Since it may not be easy to discover the key by analysing the relationships between the provided plaintext and ciphertext, the approach shows resilience to known-plaintext attacks.
5. **Applicability to Various Texts:** The algorithm's ability to encrypt any given text makes it useful in many contexts where the security of text-based data is important.

Weaknesses:

1. **Limited Key Space:** The climbing prime numbers restrict the key space, which could make it susceptible to brute-force attacks. For better security, a bigger key space is usually better.
2. **Dependence on Prime Numbers:** The security of the technique is highly dependent on prime number features. An attacker could potentially break the encryption if they find a pattern in the series of prime numbers.

3. **Vulnerability to Frequency Analysis:** When applied to bigger datasets, the algorithm's simplicity makes it vulnerable to frequency analysis assaults.
4. **Lack of Avalanche Effect:** To mitigate the algorithm's avalanche effect, minor modifications to the input (plaintext) might not have a major impact on the output (ciphertext). This may affect how well it withstands linear and differential cryptanalysis.
5. **No Initialization Vector (IV):** In some use cases, the method could be susceptible to assaults like replay attacks because it lacks an initialization vector.

Application Area:

The suggested cryptographic algorithm is applicable in cases that require a lightweight and easily implementable encryption mechanism. Illustrative instances comprise of encrypted messaging platforms, authentication of data integrity in communication channels, and scenarios where emphasis is placed on simplicity rather than complex security attributes. Nevertheless, it is important to exercise caution when evaluating the suitability of this method for applications that demand robust security and resilience against advanced threats.

5.1. Algorithm

5.1.1. Encryption:

Step 1. Caesar Cipher with Unique Word Keys:

- Assign prime integer keys to each word.
- Encrypt the plaintext using the Caesar Cipher with the corresponding word keys.

Step 2. Rail Fence Cipher with Key Value 4:

- Use the resulting Caesar Cipher ciphertext as the plaintext.
- Encrypt the plaintext using the Rail Fence Cipher with a fixed key value of 4.

Step 3. Playfair Cipher with Shifts and Rules:

- Apply the Playfair Cipher to the Rail Fence ciphertext.
- Use a specific key for encryption.
- Follow Playfair rules, such as moving letters down or to the right based on their positions in the matrix.
- Repeat these steps until all three techniques are applied, generating a new ciphertext at each stage.

5.1.2. Decryption:

Perform the reverse operations in the following order:

Step 1. Playfair Decryption:

- Use the Playfair Cipher with the same key for decryption.
- Apply Playfair rules in reverse.

Step 2. Rail Fence Decryption with Key Value 4:

- Decrypt the Rail Fence ciphertext using a fixed key value of 4.

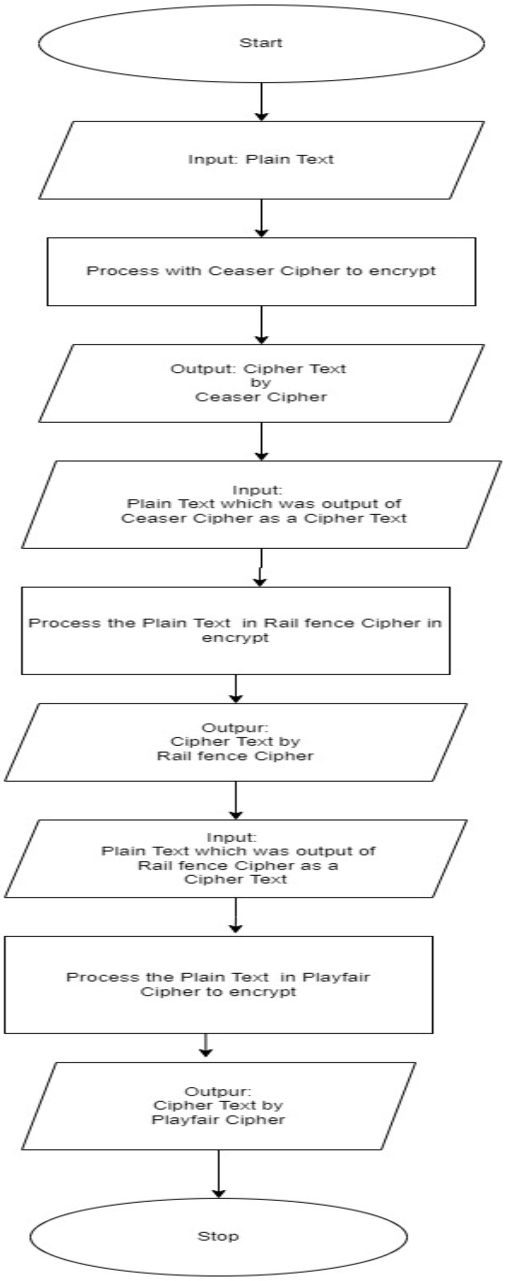
Step 3. Caesar Decryption with Unique Word Keys:

- Decrypt the resulting Rail Fence plaintext using the Caesar Cipher with the corresponding word keys.

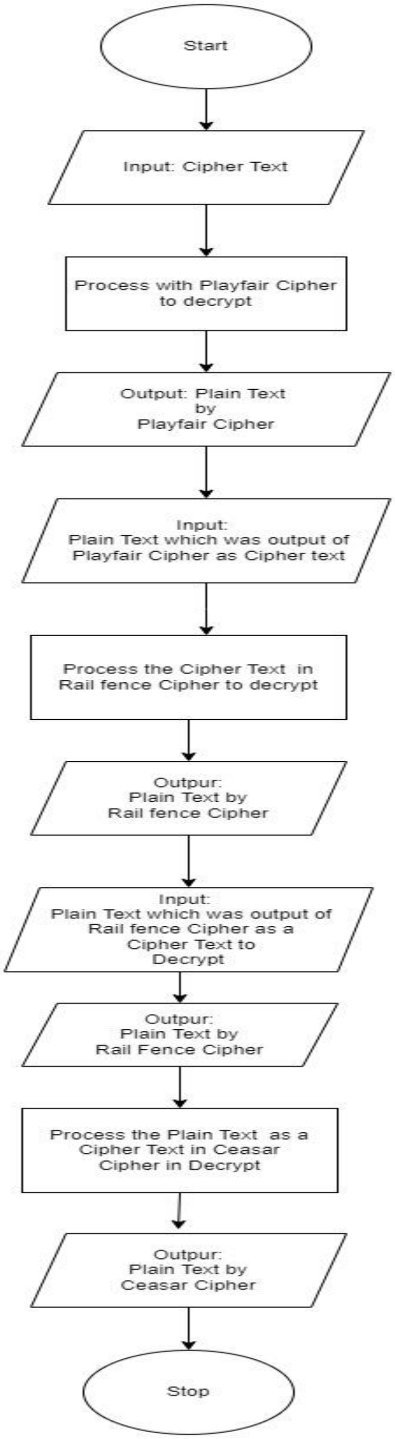
Using a chain of different keys and encryption algorithms greatly improves the security of the whole encryption process. An unauthorized party would have a harder and harder time deciphering the original message with each successive cipher. The encryption process can be made more secure with this innovative multi-layered technique.

5.2. Flow Chart

5.2.1. Encryption


Start
Input: Plain Text
Process with Ceaser Cipher to encrypt
Output: Cipher Text by Ceaser Cipher
Input: Plain Text which was output of Ceaser Cipher as a Cipher Text
Process the Plain Text in Rail fence Cipher in encrypt
Outpur: Cipher Text by Rail fence Cipher
Input: Plain Text which was output of Rail fence Cipher as a Cipher Text
Process the Plain Text in Playfair Cipher to encrypt
Outpur: Cipher Text by Playfair Cipher
Stop

5.2.2 Decryption


Start
Input: Cipher Text
Process with Playfair Cipher to decrypt
Output: Plain Text by Playfair Cipher
Input: Plain Text which was output of Playfair Cipher as Cipher text
Process the Cipher Text in Rail fence Cipher to decrypt
Outpur: Plain Text by Rail fence Cipher
Input: Plain Text which was output of Rail fence Cipher as a Cipher Text to Decrypt
Outpur: Plain Text by Rail Fence Cipher
Process the Plain Text as a Cipher Text in Ceasar Cipher in Decrypt
Outpur: Plain Text by Ceasar Cipher
Stop

6. Conclusion

The newly suggested encryption technique provides simplicity, adjustable key size, and reversibility enabling convenient and adaptable implementation. The main advantages of this encryption method are its ability to withstand known-plaintext attacks and its suitability for use with different types of texts. Nevertheless, there are constraints, such as a limited range of possible keys and susceptibility to frequency analysis. The technique is suitable for lightweight encryption requirements, such as messaging platforms and data integrity authentication. However, care is recommended for applications that require strong security. The use of a multi-layered encryption procedure significantly augments security measures, hence becoming the task of decoding increasingly arduous. In general, the appropriateness is contingent upon the unique requirements of the use-case and the desired degrees of security.

7. Bibliography

Bacon, M., 2024. *TechTarget.* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/security [Accessed 03 01 2024].

Corner, C., 2024. *Crypto Corner.* [Online] Available at: https://crypto.interactive-maths.com/caesar-shift-cipher.html#intro [Accessed 09 01 2024].

Datta, S., 2023. *Baeldung.* [Online] Available at: https://www.baeldung.com/cs/cryptography-rail-fence-technique [Accessed 11 01 2024].

Fasulo, P., 2021. *SecurityScorecard.* [Online] Available at: https://securityscorecard.com/blog/what-is-the-cia-triad/ [Accessed 03 01 2024].

Fortinet, 2024. *Fortinet.* [Online] Available at: https://www.fortinet.com/resources/cyberglossary/what-is-cryptography#:~:text=In%20computer%20science%2C%20cryptography%20is,disguise%20the%20content%20of%20messages.
[Accessed 07 01 2024].

Gatekeeper, 2024. *Gatekeeper.* [Online] Available at: https://gkaccess.com/support/information-technology-wiki/caesar-cipher/
[Accessed 11 01 2024].

geeksforgeeks, 2023. *geeksforgeeks.* [Online] Available at: https://www.geeksforgeeks.org/cryptography-introduction/?ref=lbp [Accessed 01 01 2024].

geeksforgeeks, 2024. *geeksforgeeks.* [Online] Available at: https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/ [Accessed 03 01 2024].

intellipaat, 2023. *intellipaat.* [Online] Available at: https://intellipaat.com/blog/playfair-cipher/ [Accessed 10 01 2024].

Kaspersky, 2023. *Kaspersky.* [Online] Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography
[Accessed 21 12 2023].

Richards, K., 2024. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/cryptography
[Accessed 07 01 2024].

Sarkar, S., 2020. *IBM.* [Online]
Available at: https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/04/caesar-cipher
[Accessed 09 01 2024].

Sharma, M., 2023. *includehelp.* [Online]
Available at: https://www.includehelp.com/cryptography/rail-fence-cipher.aspx
[Accessed 09 01 2024].

Sileshi, D., 2023. *Baeldung.* [Online]
Available at: https://www.baeldung.com/cs/playfair-cipher#:~:text=Advantages%20and%20Disadvantages%20of%20Playfair%20Cipher&text=This%20characteristic%20enhances%20the%20encryption,substitution%20is%20its%20key%20strength.
[Accessed 11 01 2024].