A logo for a university

Description automatically generated

**Module Code & Module Title**

**CC5004NI Security in Computing**

**Assessment Weightage & Type**

**30% Individual Coursework**

**Year and Semester**

**2023 -24 Autumn**

**Student Name: Bipina rai**

**London Met ID: 22068719**

**College ID: : NP01NT4A220066**

**Assignment Due Date: January 15, Monday, 2024**

**Assignment Submission Date: January 15, Monday, 2024**

**Word Count (Where Required): 8343**

*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

[1. Introduction: 5](#_Toc156052888)

[1.1 aims and objectives: 5](#_Toc156052889)

[2. Background 6](#_Toc156052890)

[2.1 What is security ? 6](#_Toc156052891)

[1.2 CIA triad 7](#_Toc156052892)

[Confidentiality: 8](#_Toc156052893)

[Integrity: 8](#_Toc156052894)

[Availability: 9](#_Toc156052895)

[1.3 Introduction to cryptography: 9](#_Toc156052896)

[1.4 key terminologies to understand the concept of cryptography 10](#_Toc156052897)

[1.5 History to cryptography: 12](#_Toc156052898)

[1.2 Two types of cipher: 13](#_Toc156052899)

[Symmetric cipher: 13](#_Toc156052900)

[Asymmetric cipher: 14](#_Toc156052901)

[1. Types of asymmetric algorithm: 14](#_Toc156052902)

[2. advantages and disadvantages of asymmetric algorithms: 14](#_Toc156052903)

[3. Background for selected cryptographic algorithm. 15](#_Toc156052904)

[3.1. Introduction to Row transposition cipher: 15](#_Toc156052905)

[3.2. Example of encryption and decryption using this cipher 16](#_Toc156052906)

[4. Pros and cons of the cipher: 18](#_Toc156052907)

[5. Development 19](#_Toc156052908)

[5.1. Modification carried out to make row transposition more secure. 19](#_Toc156052909)

[5.2. Modification of the cipher: 20](#_Toc156052910)

[5.3. why the modification was necessary? 23](#_Toc156052911)

[5.4. encryption algorithm: 23](#_Toc156052912)

[5.5 decryption algorithm 25](#_Toc156052913)

[6. Testing 27](#_Toc156052914)

[6.1. Test 1 27](#_Toc156052915)

[6.2 Test 2 30](#_Toc156052916)

[6.3. Test 3 32](#_Toc156052917)

[6.4. Test 4 35](#_Toc156052918)

[6.5. Test 5 38](#_Toc156052919)

[7. Evaluation 42](#_Toc156052920)

[7.1. strength of rot key transposition cipher: 42](#_Toc156052921)

[7.2. weakness of rot key transposition cipher: 43](#_Toc156052922)

[7.3. Application area: 43](#_Toc156052923)

[8. Conclusion : 45](#_Toc156052924)

[9. Appendix 46](#_Toc156052925)

[1. Types of asymmetric algorithm: 46](#_Toc156052926)

[2. advantages and disadvantages of asymmetric algorithms: 51](#_Toc156052927)

Table of figures

Figure 1: security in technology 9

Figure 2: CIA triad (forinet, cyberglossary, 2023) 10

Figure 3: cryptography (geeks, 2023) 12

Figure 4: symmetric cipher (daniel, 2021) 16

Figure 5: asymmetric algorithm (S, 2023) 17

Figure 6: row transposition cipher 18

Figure 7: Rot 3 letter positions 23

Figure 8: Row transposition letter position 23

Figure 9: flowchart for the basic modification process 25

Figure 10: new encryption algorithm 27

Figure 11: decryption algorithm 29

Figure 12: RSA encrption (S, 2023) 49

Figure 13: digital signature algorithm (mitra, 2020) 50

Figure 14: Elliptic curve digital signature algorithm (ghanmi, 2012) 51

Figure 15:Diffie-Hellman key exchange algorithm (mitra, 2020) 52

Figure 16:Elgamal algorithm (Hussein, 2019) 53

Figure 17: Elliptic curve cryptography algorithm (avinetworks, 2024) 53

**Abstract**

This report focuses on various parts of the cryptography and security as a whole. Better understanding of the role in securing data and communication is what this assignment covers. This includes the CIA triad, introduction to security and cryptography, different types of encryptions including both symmetric and asymmetric encryption. The history of cryptography is mentioned the background study of the selected symmetric and asymmetric cipher as well which will later be used in modification for better and strong implementation of the cryptographic cipher. In this report the row transposition cipher is modified using Rot 3 cipher to generate a stronger key. Then the modified cipher is tested and evaluated. This report also analyses the strengths and weaknesses of the newly developed encryption algorithm and mentions the potential areas of application.

**Acknowledgement**

I would like to thank  Islington College and ofcourse London Metropolitan University for giving me the chance to learn about information security and cryptography. Additionally, I would like to express my gratitude to my module leader, mr Avinav Neupane for their leadership and assistance during this project. i would also like to thank my fellow classmates for always helping me out in the absence of my module leader, without the help of both the completion of this coursework would have been impossible. Their knowledge and direction have been extremely helpful to me in comprehending the difficult subject matter and finishing this report. I appreciate all of your assistance and backing.

# Introduction:

In the world of information technology, security in computing is like the fortress that shields our computer systems, networks, and precious data from sneak attacks, theft, and all sorts of digital mischief. Think of it as the guardian that stands tall against the bad guys, like ransomware, tricky phishing schemes, and the shady characters who create malware, those viruses, spyware, and adware that can mess things up. To keep your digital world safe and sound, it's crucial to be a savvy user. That means crafting robust passwords, keeping your software updated, staying on your toes when clicking on links or installing stuff, and having a trusty antivirus sidekick by your side. In this cyber age, a little caution goes a long way.

Cryptography can be compared to the code that keeps our online environment safe. It is essential because it prevents prying eyes from viewing sensitive data while it is being transferred or stored. Imagine it as the lock on your virtual safe; only individuals possessing the appropriate key can decipher the data that is jumbled and unintelligible. By doing this, we can make sure that hackers and other online miscreants cannot access our passwords, bank information, or personal information. Our internet existence would be considerably riskier without cryptography, it would be like leaving our front door wide open.

## aims and objectives:

* To learn about security in the context of information technology and in cryptography.
* To comprehend the CIA triad and its function in information security
* To learn the nature of cryptography and how it is applied to secure data and information.
* To discover about the various forms of encryption, including symmetric and asymmetric encryption
* To fully understand the applications and constraints of an a selected cypher.
* To comprehend the function of logic gates and how they can be applied to alter the chosen cypher.
* To get the significance of security in contemporary society and the different precautions that can be taken to guard against cyber threat.
* To test and assess the modified cypher

# Background

# What is security ?

The term "security" in general describes all the precautions used to keep someone or something safe or make sure that only authorized individuals enter or exit a location (dictionary, 2024). security for information technology describes the strategies, resources, and personnel employed to protect an organization's digital assets. Preventing unauthorized users, or threat actors, from disrupting, stealing, or exploiting these resources, devices, and services is the aim of IT security. These dangers may originate from the outside or the inside, be malevolent or unintentional, etc.

An efficient security plan employs a variety of techniques to reduce weaknesses and focus on various cyber threats. IT services, software tools, and safety measures are used in the identification, avoidance, and reaction to security threats (bacon, 2021).



Figure 1: security in technology

There are two aspects to IT security: information and physical.

**Physical safety**

Physical security is the defense against physical acts, intrusions, and other occurrences that could harm a business and its property. It includes people, hardware, software, network information, and data. Protecting an organization from threats, mishaps, and catastrophic events like fires, floods, earthquakes, and extreme weather is part of maintaining its physical security. Inadequate physical security puts servers, gadgets, and appliances that facilitate corporate activities and processes at risk of breaking down. Nevertheless, a significant portion of the physical security threat is human.

**Security of information**

Another name for information security is infosec. It consists of tactics for handling the instruments, procedures, and guidelines that safeguard non-digital as well as digital assets. Infosec, when used properly, can optimize an organization's capacity to stop, identify, and react to dangers (bacon, 2021).

# 1.2 CIA triad

The terms "CIA triad" (confidentiality, integrity, and availability) are represented by three distinct letters. One prominent model used to guide the creation of security systems is the CIA triad. They are tools for identifying weak points and strategies for developing fixes.

The organization's safety profile is more powerful and capable of handling threat occurrences when all three standards have been met (forinet, cyberglossary, 2023).

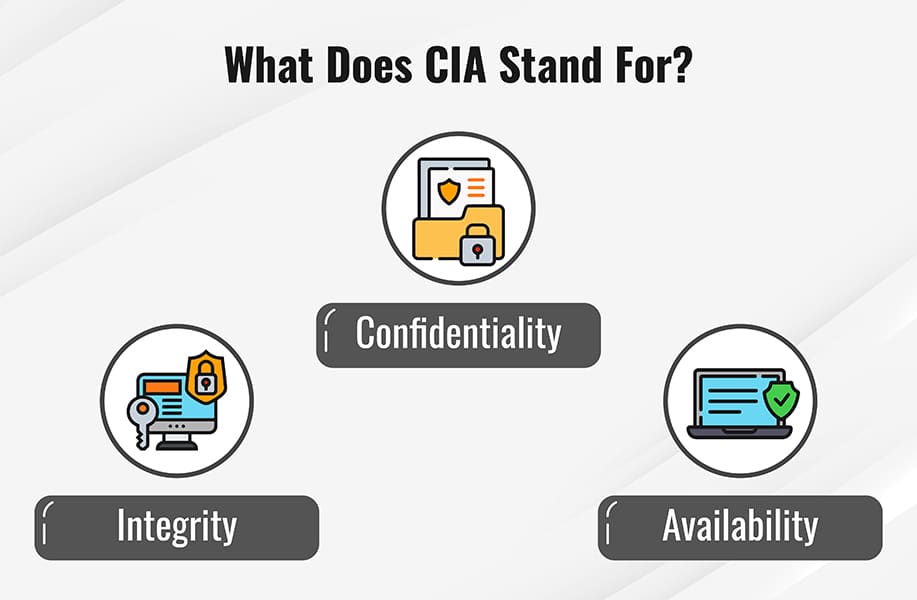


Figure 2: CIA triad (forinet, cyberglossary, 2023)

## Confidentiality:

In order to maintain confidentiality, an organization must take steps to ensure that data remains hidden or private. To do this, accessibility to information needs to be restricted to stop data from being shared without authorization, either on purpose or accidentally. Ensuring that anyone lacking the appropriate authorization cannot access resources that are vital to your company is a crucial part of keeping privacy. On the other hand, a well-functioning system also makes certain that the right people have access rights (forinet, cyberglossary, 2023).

A critical component of many work contexts is confidentiality. The ability to manage secrecy is becoming more and more important as a soft talent in a variety of sectors and businesses. It is a technique used to safeguard individuals, maintain a high level of business security, and preserve confidential information. In addition to helping organizations achieve legal compliance obligations, this protection can help them establish confidence and trust with their clients and associates (team, 2023).

## Integrity:

Maintaining integrity means ensuring that your data is reliable and unaltered. Only when the data is accurate, genuine, and dependable is its integrity preserved.

For instance, the information on top managers that your business posts on its website must be accurate. If it is false, people looking for information on your website can conclude that your company is not reliable. A person who has a personal interest in harming your company's reputation might attempt to hack your website and change the executive bios, images, or titles to harm the individual's or the company's image overall (forinet, cyberglossary, 2023).

Being morally clear-headed, truthful, and decent are traits of integrity. Employees that work for a company with an authentic atmosphere of integrity take their duties meticulously, take initiative whenever they don't know what they're supposed to do, and eventually assume responsibility for their actions. Consequently, the company prospers (perry, 2022).

## Availability:

If data is not accessible to anyone within the business and the clients they serve, it is frequently worthless, even if confidentiality and integrity are upheld. Systems, networks, and applications must therefore operate as intended and at the appropriate times. In addition, the data should not be excessively difficult to get, and those who have access to it need to be able to use it when needed.

Organizations can utilize multiple servers, networks, and apps to guarantee availability. These can be configured to activate if there is a disruption or malfunction with the main system. Maintaining technology and security system updates can also help you increase availability. By doing this, you reduce the possibility that a program will break or that an extremely recent threat may infect your system. Complete disaster recovery plans and backups also aid in an organization's prompt restoration after an unfavourable incident (forinet, cyberglossary, 2023).

# 1.3 Introduction to cryptography:

The term cryptography refers to the process of encoding data so that only the authorized person can access it. The practice of cryptography has been used to encrypt messages or data for thousands of years,. It is still employed today in e-commerce, bank cards, and computer passwords. The encryption and decryption of information is made achievable by current cryptography techniques, such as ciphers and algorithms like 128-bit and 256-bit encryption keys. Modern cryptosystems, like the Advanced Encryption Standard (AES), are believed to be nearly unbreakable. By encrypting communicated messages with an algorithm and a key that is only known to the sender and receiver, cryptography maintains confidentiality. A popular illustration of this is the messaging app WhatsApp, which encrypts user communications to prevent hacking or interception (forinet, 2023).

An initial human-readable message, known as plaintext, is transformed into something that would appear to an untrained observer to be gibberish in cryptography through the use of an algorithm, or sequence of mathematical operations. This gibberish is known as ciphertext. For the intended recipient to be able to use the encrypted message, cryptographic systems require a technique to decrypt the ciphertext back into plaintext. This method is typically, but not always, required (frulinger, 2022).

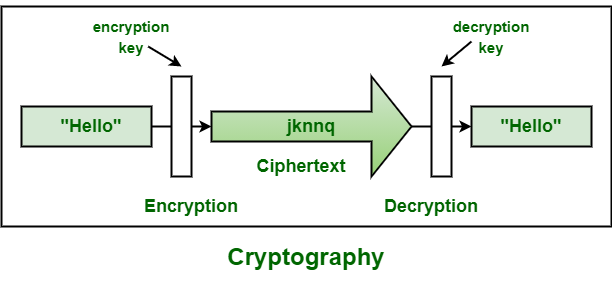


Figure 3: cryptography (geeks, 2023)

# 1.4 key terminologies to understand the concept of cryptography

Plaintext: Plain Text is a representation of the initial message that the sender intended to share with the recipient. The actual message that needs to be sent to the other end in cryptography is given a particular title, such as plain text (ginni, 2022).

* Encrypted Text: This is the message that is encoded after encryption has been used to change plaintext.
* Cryptographic Algorithm/Cipher: An encryption algorithm is called a cipher. The ciphertext is created by using an algorithm to jumble the plain text. The process of converting plain text into ciphertext using a cryptographic algorithm is called encryption and the process of converting encrypted text back into plain text is called decryption (mamun, 2022).
* Encryption: Encryption is the process of converting plain text into cipher text. encryption is required to transfer sensitive data and information from onw medium to another (ginni, 2022).
* Decrypt: Decryption is a method of going backwards in encryption. It is a process that turns plain text into cipher text (ginni, 2022).
* cryptanalysis: The study of ciphertext, ciphers, and cryptosystems with the goal of comprehending their operation and developing methods for subverting or deteriorating them is known as cryptanalysis (mamun, 2022).
* Key: The mathematical values, formulas, or procedures that the cipher uses as an algorithm constitute a key. It establishes the encryption or decryption method for a plaintext message. The only way to interpret the jumbled data is with the key (mamun, 2022).
* Symmetric cryptography: Also referred to as secret key cryptography, symmetric cryptography uses an only shared secret to allow individuals to exchange encrypted data (mamun, 2022).
* Public-key cryptography: Also known as asymmetrical cryptography, public-key cryptography is the study of encryption techniques that employ associated key pairs. Every key pair is made up of a both private key and a public key. Cryptographic techniques based on mathematical puzzles known as single-way functions are used for creating key pairs. Public-key cryptography is secure when the private key is kept confidential. Open distribution of the general key does not jeopardize security (mamun, 2022).
* RSA Algorithm: RSA is a popular public-key encryption system for sending private information. It is among the most ancient as well. The names of Leonard Adleman, Adi Shamir, and Ron Rivest, who published a public description of the algorithm in 1977, are the source of the acronym "RSA" (mamun, 2022).
* Data Encryption Standards (DES): DES constitute block ciphers that apply a cryptographic key and algorithm to a block of information at once as opposed to one bit at a moment. DES divides a simple text message into 64-bit blocks for encryption.
* Digital Signature: Usually, the signature is created by protecting the message digest—also known as the hash of the message—with the author's secret key. The digital signature is a protected message digest. The message's integrity and origin are guaranteed by the signature.
* Message Authentication Code (MAC): A brief bit of information called a message authentication code (MAC) is used to verify the authenticity of a message.
* Hashing: Hashing is the process of converting an array of characters into a fixed-length worth or key that is typically shorter and still reflects the initial string of characters.
* Hashing Mechanism: A hash function is a method or the equation that accepts broad variable-length sets of information as inputs and produces lesser fixed-length information sets as results.
* MD5: The acronym for Message Digest is MD5 MD. It generates a 128-bit digest by dividing the message into 512-bit blocks.
* SHA: The acronym for Secure Hash Algorithm is SHA. The National Institute of Standards and Technology (NIST) created this standard.The SHA typical was published in a number of versions, including SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 (mamun, 2022).

# History to cryptography:

The history of cryptography dates back to the Egyptian hieroglyphics, yet it is still essential for protecting data while it is in transit and keeping unauthorized parties from reading it. To safeguard data privacy, credit card transactions, email, and online browsing, it employs mathematical ideas and algorithms to convert messages into hard-to-decipher codes using methods like digital signature and cryptographic keys (forinet, 2023).

All of this is rather abstract, so a good way to grasp the intricacies of what we're discussing is to examine one of the earliest known cryptographic systems. The reason it's called the Caesar cipher is that Julius Caesar employed it for his private correspondence. His historian Suetonius put it this way: "If he had anything private to say, he wrote it in cipher, that is, by so rearranging the alphabet's letters' order.” To understand these and understand their significance, one must replace letter A with D, the fourth letter of the alphabet, and similarly with the remaining letters (frulinger, 2022).

Throughout most of history, government and military communications were secured through the use of different substitution ciphers, which made up cryptography. Arab mathematicians of the Middle Ages advanced science, especially the art of decryption. For example, patterns can be more easily recognized when researchers discover which letters in a language are more common than others. However, the majority of pre-modern encryption is remarkably straightforward by today's standards, for the obvious reason that it was challenging to execute mathematical transformations quickly enough to justify the use of encryption or decryption prior to the invention of computers (frulinger, 2022).

# Two types of cipher:

## Symmetric cipher:

Encryption is the process of altering a message's format so that it cannot be read by unauthorized parties. Because symmetric-key encryption encrypts and decrypts messages using the same key, it is easy to use but less secure. Additionally, a secure way to move the key from one person to another is needed (geeks, 2023).

A diagram of a cryptography

Description automatically generated

Figure 4: symmetric cipher (daniel, 2021)

## Asymmetric cipher:

Two distinct keys are used by asymmetric cryptography algorithms for both encryption and decryption. The public key acts for encryption, and the private key is relied on for decryption. The person who receives them has to be the owner of the two keys. The issue of key exchange has been mitigated by using distinct keys for encryption and decryption (S, 2023).

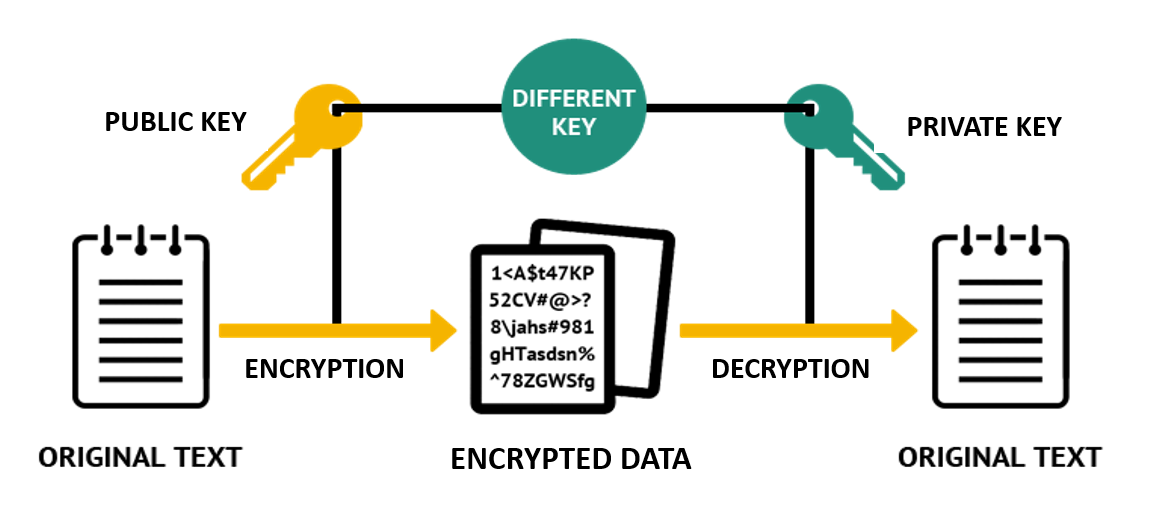


Figure 5: asymmetric algorithm (S, 2023)

# [Types of asymmetric algorithm:](#_1._Types_of)

# [2. advantages and disadvantages of asymmetric algorithms:](#_2._advantages_and)

# Background for selected cryptographic algorithm.

## 3.1. Introduction to Row transposition cipher:

In columnar or row transposition, the ciphertext is taken off in columns after the plaintext is written out in rows. In its most basic version, the route is to read down each column sequentially using the Route Cipher. The plaintext "a simple transposition" with five columns, for instance (corner, 2024).

A computer screen shot of a network security

Description automatically generated

Figure 6: row transposition cipher

Even though row transposition has a fair share of benefits and drawbacks, its simplicity of use makes it possible for the intended user to decipher the message with ease, and its ability to mitigate potential drawbacks to make it a strong cipher is the main reason it was chosen as the basis for this report.

## 3.2. Example of encryption and decryption using this cipher

Plain text: attack postponed until two am

There are 25 letters in the message. Now place the letters of the message in a rectangular array. We also need a keyword with its length the same as the number of columns.

Key word: 4312567

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4 | 3 | 1 | 2 | 5 | 6 | 7 |
| a | t | t | a | c | k | p |
| o | s | t | p | o | n | e |
| d | u | n | t | i | l | t |
| w | o | a | m | x | y | z |

Now write down this letters in the numerical order as in letters in the column 1 and then 2 and so on till 7. That will make:

cipher : ttna aptm tsuo aodw coix knly petz

here,

p = plain text value

k = keyword

c = cipher text

d = decryption text

now for encryption,

c = E(k,p) = (p+k) mod 26

for decryption,

d = d(k,c) = (c-k) mod 26

**example of encrypting and decrypting using the algorithm,**

**encrypting:**

message = hello

let key = 4

now,

c(h) = (p+k) mod 26 = (7+4) mod 26 = 11= l

c(e) = (p+k) mod 26 = (4+4) mod 26 = 8= i

c(l) = (p+k) mod 26 = (11+4) mod 26 = 15= p

c(l) = (p+k) mod 26 = (11+4) mod 26 = 15= p

c(o) = (p+k) mod 26 = (14+4) mod 26 = 18= s

ecryption = lipps

**decrypting:**

d(l)=(c-k) mod 26=(11-4)=7=h

d(i)=(c-k) mod 26=(8-4)=4=e

d(p)=(c-k) mod 26=(15-4)=11=l

d(p)=(c-k) mod 26=(15-4)=11=l

d(s)=(c-k) mod 26=(18-4)=14=o

decryption = hello

# Pros and cons of the cipher:

Advantages:

1. Easy implementation: Compared to other block ciphers the RTC is comparatively simple to implement.

2. High security: When used correctly, the RTC has been demonstrated to be extremely secure despite its simplicity. Its big key size makes it suitable for high-security uses as it is resistant to attacks using brute force.

3. Quick encryption and decryption: Since the RTC utilizes a transformation that is linear, it has faster encryption and decryption times than more complex ciphers.

Disadvantages:

1. More difficult to use and comprehend than the Caesar Cipher.

2. Because of the larger key sizes, more memory space is needed.

3. Choosing a key can still be difficult if the right safety measures aren't followed.

# Development

## 5.1. Modification carried out to make row transposition more secure.

There are various modifications that has been carried out to make one cipher more secure and sustainable. In this case we are going to study some detailed information regarding modification done to the row transposition cipher in the past and see what ideas we can get from it.

Combination of Caesar Cipher Modification with Transposition Cipher by Fahrul Ikhsan Lubis, Hasanal Fachri Satia Simbolon1, Toras Pangidoan Batubara1, Rahmat Widia Sembiring : In this experiment, the caesar cipher modification is combined with the transposition cipher. The ciphertext is encrypted three times: first using the caesar modification, then using transposition to encrypt the result. Finally, the result of transposition is encrypted again using the second caesar modification, and the process is repeated during decryption. The letters in the modified Caesar cipher are shifted according to the ASCII table rather than the alphabet; plaintext will have characters added to it prior to encryption, and the resulting new plaintext will be split into two sections: plaintext that will be encrypted and plaintext that will always remain unencrypted.

Three processes are used in the encryption and decryption process. During the encryption process, the plaintext will be encrypted once using the transposition cipher algorithm and twice using the modified Caesar cipher. Changing the Caesar cipher algorithm, which employs characters from the ASCII table (32-126 characters) in addition to alphabet letters, uses a key that is used dynamically because it is one of the ASCII values of a single plaintext character. Thus, distinct plaintext and distinct key.

The following are the steps involved in encryption and decryption mathematically:

Ex = (A-32) + K mod 127; Dx = (A-32) - K mod 127.

Description: K= Key (one of the ASCII characters from plaintext mod 32) and A= ASCII character in the plaintext.

The final change is to add specific words to the plaintext. During the encryption process, the system will append a specific word to the plaintext's reverse, dividing it into two sections: the encrypted portion and the unencrypted part. On the other hand, the system will automatically remove the extra words during decryption, returning the plaintext to its original state (Lubis, 2017).

## 5.2. Modification of the cipher:

The modification involves combining the ROT3 Caesar cipher and the row transposition cipher to create a new encryption technique. This new technique is called the *Rot key transposition* cipher, since it mostly focuses on making the key for the row transposition cipher stronger. Let's break down the process more briefly:

1. ROT3 Caesar Cipher:

The key for the encryption is generated using ROT3, a Caesar cipher with a fixed shift of 3. For each letter in the plaintext, its position in the ROT3 cipher table (denoted as p1) is shifted by 3 positions, and the result becomes the key for the subsequent row transposition cipher.

Mathematically,

the key (k) is calculated as: ( k = (p1 + 3) mod 26 ),

where 'mod 26' ensures that the resulting key stays within the range of the alphabet.

Here, each key is generated according to the given letter.

A white rectangular object with black numbers

Description automatically generated

Figure 7: Rot 3 letter positions

1. Row Transposition Cipher:

The row transposition cipher is then applied to the plaintext using the key obtained from the ROT3 cipher. Each letter's position in the row transposition cipher table (denoted as p2) is combined with the previously calculated key (k).

Mathematically,

the resulting cipher (c) is calculated as: ( c = (p2 + k) mod 26 ),

where 'mod 26' is used to keep the result within the bounds of the alphabet.

If the sum of position value and the key is greater than the number 25 in row transposition cipher, then the resulting key will get subtracted from the number 26.

By combining these two ciphers, you first apply a Caesar cipher with a fixed shift of 3 to derive the key, and then use this key in the row transposition cipher. This dual-layered encryption approach adds complexity and enhances the security of the overall encryption process. To decrypt, the process is reversed: first, the row transposition cipher is deciphered, and then same key value of ROT3 is applied to obtain the original plaintext.

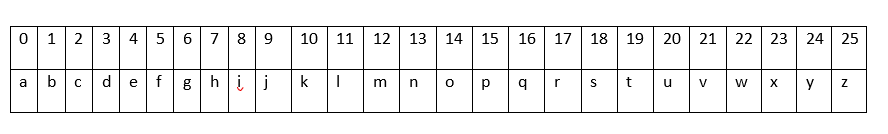


Figure 8: Row transposition letter position

Above given modification in the flowchart:

A screenshot of a computer

Description automatically generated

Figure 9: flowchart for the basic modification process

## 5.3. why the modification was necessary?

Though row transposition cipher has various strong benefits it also has lots of flaws due to which this modification was necessary. Vulnerability to frequency analysis as this method does not alter the frequency, if the language of the plaintext is known to the hackers that can easily exploit patterns and lastly as key plays a vital role in securing the confidentiality maintaining a strong key is a must, all these flaws should be eliminated in order for this encryption cipher to be safe which is why the modification was necessary. The new modification of the row transposition mostly focuses on a stronger key generation. Since the key differs according to each plain text letter, it is much harder for the attackers to figure out the pattern. The proper implementation of this newly developed transposition cipher helps build the key even stronger which directly or indirectly helps reduce other vulnerabilities as well.

## 5.4. encryption algorithm:

Step 1: input a plaintext(p1) letter position in the Rot 3 ceaser cipher.

Step 2: now apply the Rot 3 ceaser cipher formula which is k = (p1+3) mod 26

Step 3: here the output is the (k) which is then used in the Row Transposition Cipher.

Step 4: again put a letter in the plaintext(p2) and calculate the position of the letter as per the Row transposition table

Step 5: now add the generated key (k) from the Rot 3 Ceaser Cipher to the current position in the Row Transposition Cipher.

Step 6: if the sum of the key and the current position in the Row Transposition Cipher is greater than 25, subtract 26 from the result.

Below flowchart shows the clear implementation of the encryption algorithm,

A screenshot of a computer

Description automatically generated

Figure 10: new encryption algorithm

## 5.5 decryption algorithm

Decryption algorithm is quiet easier and shorter in comparison to the encryption algorithm,

Step 1: input cipher text letter position

Step 2: now subract the generated key(k) from the ciphertext position in the row transposition cipher, which is D=(c-k) mod 26

Step 3: if the subtraction of ciphertext and key is less than 0, add 26 to the result.

Below flowchart shows the clear implementation of the decryption algorithm,

A screenshot of a computer

Description automatically generated

Figure 11: decryption algorithm

# Testing

## 6.1. Test 1

Let’s say the plain text is “hello”

Plain letter: h

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (h) = (p1+3) mod 26= (8+3) mod 26 = 11

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(h)=(p2+k) mod 26 = (7+11) mod 26 = 18 = s

here encryption letter of ‘h’ is ‘s’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (h) = (p1+3) mod 26= (8+3) mod 26 = 11

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (s-k)=(18-11)= 7 = h

Therefore, the decryption letter of ‘s’ is ‘h’

Plain letter : e

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (e) = (p1+3) mod 26= (5+3) mod 26 = 8

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(e)=(p2+k) mod 26 = (4+8) mod 26 = 12 = m

here encryption letter of ‘e’ is ‘m’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (e) = (p1+3) mod 26= (5+3) mod 26 = 8

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (m-k)=(12-8)= 4 = e

Therefore, the decryption letter of ‘m’ is ‘e’

Plain letter: l

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (l) = (p1+3) mod 26= (12+3) mod 26 = 15

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(l)=(p2+k) mod 26 = (11+15) mod 26 = 26 since there is no 26 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 15 = (26-15) = 11

Now the new key is 11

Again using row transposition cipher and the new key.

c(l)=(p2+k) mod 26 = (11+11) mod 26 = 22 = w

finally the encryption letter of ‘l’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 11 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-11)= 11 = l

Therefore, the decryption letter of ‘w’ is ‘l’

Plain letter: o

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (o) = (p1+3) mod 26= (15+3) mod 26 = 18

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(o)=(p2+k) mod 26 = (14+18) mod 26 = 32 since there is no 32 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 15 = (26-18) = 8

Now the new key is 8

Again using row transposition cipher and the new key.

c(l)=(p2+k) mod 26 = (14 +8) mod 26 = 22 = w

finally the encryption letter of ‘o’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 8 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-8)= 14 = o

Therefore, the decryption letter of ‘w’ is ‘o’

Atlast the encrypted word for the plaintext “hello” is “smwww”

## 6.2 Test 2

Plain text = cat

Encryption for the first letter ‘c’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (c) = (p1+3) mod 26= (3+3) mod 26 = 6

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(c)=(p2+k) mod 26 = (2+6) mod 26 = 8 = i

here encryption letter of ‘c’ is ‘i’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (c) = (p1+3) mod 26= (3+3) mod 26 = 6

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (i-k)=(8-6)= 2= c

Therefore, the decryption letter of ‘i’ is ‘c’

Encryption for the letter “a”

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (a) = (p1+3) mod 26= (1+3) mod 26 = 4

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(a)=(p2+k) mod 26 = (0+4) mod 26 = 4 = e

here encryption letter of ‘a’ is ‘e’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (a) = (p1+3) mod 26= (1+3) mod 26 = 4

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (e-k)=(4-4)= 0 = a

Therefore, the decryption letter of ‘e’ is ‘a’

Encryption for the third letter “t”

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (t) = (p1+3) mod 26= (20+3) mod 26 = 23

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(t)=(p2+k) mod 26 = (19+23) mod 26 = 42 since there is no 42 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 23 = (26-23) = 3

Now the new key is 3

Again using row transposition cipher and the new key.

c(t)=(p2+k) mod 26 = (19+3) mod 26 = 22 = w

finally the encryption letter of ‘t’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 3 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-3)= 19= t

Therefore, the decryption letter of ‘w’ is ‘t’

Atlast the encryption word for “cat” is “iew”

## 6.3. Test 3

plain text = word

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (w) = (p1+3) mod 26= (23+3) mod 26 = 26

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(w)=(p2+k) mod 26 = (22+26) mod 26 = 48 since there is no 48 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 26 = (26-26) = 0

Now the new key is 0

Again using row transposition cipher and the new key.

c(w)=(p2+k) mod 26 = (22+0) mod 26 = 22 = w

finally the encryption letter of ‘w’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 0 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-0)= 22= w

Therefore, the decryption letter of ‘w’ is ‘w’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (o) = (p1+3) mod 26= (15+3) mod 26 = 18

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(o)=(p2+k) mod 26 = (14+18) mod 26 = 32 since there is no 32 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 15 = (26-18) = 8

Now the new key is 8

Again using row transposition cipher and the new key.

c(l)=(p2+k) mod 26 = (14 +8) mod 26 = 22 = w

finally the encryption letter of ‘o’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 8 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-8)= 14 = o

Therefore, the decryption letter of ‘w’ is ‘o’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (r) = (p1+3) mod 26= (18+3) mod 26 = 21

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(r)=(p2+k) mod 26 = (17+21) mod 26 = 38 since there is no 38 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 21 = (26-21) = 5

Now the new key is 5

Again using row transposition cipher and the new key.

c(r)=(p2+k) mod 26 = (17+5) mod 26 = 22 = w

finally the encryption letter of ‘r’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 5 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-5)= 17 = r

Therefore, the decryption letter of ‘’ w’ is ‘r’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (d) = (p1+3) mod 26= (4+3) mod 26 = 7

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(d)=(p2+k) mod 26 = (3+7) mod 26 = 10 = k

finally the encryption letter of ‘d’ is ‘k’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (d) = (p1+3) mod 26= (4+3) mod 26 = 7

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (k-k)=(10-7)= 3= d

Therefore, the decryption letter of ‘k’ is ‘d’

Atlast the final encryption for the word ‘word’ is ‘wwwk’

## 6.4. Test 4

Plain text= hawai

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (h) = (p1+3) mod 26= (8+3) mod 26 = 11

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(h)=(p2+k) mod 26 = (7+11) mod 26 = 18 = s

here encryption letter of ‘h’ is ‘s’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (h) = (p1+3) mod 26= (8+3) mod 26 = 11

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (s-k)=(18-11)= 7 = h

Therefore, the decryption letter of ‘s’ is ‘h’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (a) = (p1+3) mod 26= (1+3) mod 26 = 4

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(a)=(p2+k) mod 26 = (0+4) mod 26 = 4 = e

here encryption letter of ‘a’ is ‘e’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (a) = (p1+3) mod 26= (1+3) mod 26 = 4

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (e-k)=(4-4)= 0 = a

Therefore, the decryption letter of ‘e’ is ‘a’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (w) = (p1+3) mod 26= (23+3) mod 26 = 26

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(w)=(p2+k) mod 26 = (22+26) mod 26 = 48, since there’s no 48 position in the row transposition cipher then,

here, key (k)= 26= (26-26)=0

again,

c(w)=(p2+k) mod 26 = (22+0) mod 26= 22= w

here encryption letter of ‘w’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 0 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-0)= 22= w

Therefore, the decryption letter of ‘w’ is ‘w’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (i) = (p1+3) mod 26= (9+3) mod 26 = 12

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(i)=(p2+k) mod 26 = (8+12) mod 26 = 20 = u

here encryption letter of ‘i’ is ‘u’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (i) = (p1+3) mod 26= (9+3) mod 26 = 12

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (u-k)=(20-12)= 8= i

Therefore, the decryption letter of ‘u’ is ‘i’

So the encryption for the word ‘hawai’ is ‘seweu’

## 6.5. Test 5

Plain text: xray

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (x) = (p1+3) mod 26= (24+3) mod 26 = 27

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(x)=(p2+k) mod 26 = (23+27) mod 26 = 50, since there’s no 50 position in the row transposition cipher then,

here, key (k)= 27= (27-26)=1

again,

c(p)=(p2+k) mod 26 = (23+1) mod 26= 24 = y

here encryption letter of ‘x’ is ‘y’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 1 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (y-k)=(24-1)= 23= x

Therefore, the decryption letter of ‘y’ is ‘x’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (r) = (p1+3) mod 26= (18+3) mod 26 = 21

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(r)=(p2+k) mod 26 = (17+21) mod 26 = 38 since there is no 38 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 21 = (26-21) = 5

Now the new key is 5

Again using row transposition cipher and the new key.

c(r)=(p2+k) mod 26 = (17+5) mod 26 = 22 = w

finally the encryption letter of ‘r’ is ‘w’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 5 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (w-k)=(22-5)= 17 = r

Therefore, the decryption letter of ‘’ w’ is ‘r’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (a) = (p1+3) mod 26= (1+3) mod 26 = 4

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(a)=(p2+k) mod 26 = (0+4) mod 26 = 4 = e

here encryption letter of ‘a’ is ‘e’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = Rot3 (a) = (p1+3) mod 26= (1+3) mod 26 = 4

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (e-k)=(4-4)= 0 = a

Therefore, the decryption letter of ‘e’ is ‘a’

**Encryption:**

Here, generate a key using the Rot 3 cipher which is,

Key(k) = Rot3 (y) = (p1+3) mod 26= (25+3) mod 26 = 28

Now using row transposition cipher and the key generated using Rot 3 cipher,

c(y)=(p2+k) mod 26 = (24+28) mod 26 = 52 since there is no 52 number position in the row transposition cipher this indicates it’s false

so here,

Key(k) = 28 = (28-26) = 2

Now the new key is 2

Again using row transposition cipher and the new key.

c(y)=(p2+k) mod 26 = (24+2) mod 26 = 26 = z

finally the encryption letter of ‘y’ is ‘z’

**Decryption:**

Here k is the same key generated using the rot 3 cipher which is,

Key(k) = 2 [the new key generated will be used]

Now, D, is the decryption, c is the cipher

Decryption (d) = (c-k) mod 26 = (x-k)=(26-2)= 24 = y

Therefore, the decryption letter of ‘’ x’ is ‘y’

So the final encryption of the plain text “xray” is “ywez”

# Evaluation

The rot key transposition cipher is the modified version of the row transposition cipher that focuses on providing a stronger robust encryption. This newly modified cipher has various strengths and as well as weaknesses which is evaluated below:

## 7.1. strength of rot key transposition cipher:

* The combination of two different cipher automatically adds complexity and enhances security.
* The ROT3 Caesar cipher is used to generate the key for the row transposition cipher. As a result, key generation becomes more complex and variable, making it more difficult for adversaries to predict or brute-force the key.
* The row transposition cipher and the ROT3 Caesar cipher both employ modulo operations to help guarantee that the resultant values remain inside the alphabet. By doing this, possible vulnerabilities related to numeric overflow are avoided.
* Attackers will find it more challenging to use conventional decryption methods and frequency analysis with the shifted alphabet introduced by the ROT3 Caesar cipher.
* An additional degree of unpredictability is added by the fact that the key generation process is distinct for every letter in the plaintext.
* The row transposition cipher adds another level of complexity to the encryption by using modulo operations to prevent the sum of the position value and the key from exceeding 25.

## 7.2. weakness of rot key transposition cipher:

* The entire security of the encryption relies on the strength of the ROT3 Caesar Cipher. An attacker can quickly figure out the row transposition cipher's key if they are able to crack the ROT3 encryption.
* In the ROT3 Caesar Cipher, the fixed shift of 3 is a known and constant parameter. Attackers who are aware of this fixed shift have the ability to potentially crack the ROT3 encryption and compromise the entire system by using techniques like frequency analysis or other cryptographic attacks.
* A single-layer key for the row transposition cipher is produced by the ROT3 Caesar Cipher. An attacker can decode the entire message if they are able to successfully disrupt the key generation process.
* When'mod 26' is used in the row transposition cipher and key generation, it can produce patterns that an attacker could exploit. Because of this restriction on the number of possible keys, brute-force attacks can exploit the system.
* The dual-layered strategy increases complexity, but overall the cryptographic scheme is not as strong as with more sophisticated encryption techniques. It might be vulnerable to contemporary cryptographic methods and attacks.

## 7.3. Application area:

The Rot key transposition cipher is a hybrid of the ROT3 Caesar cipher and the row transposition cipher. It can be used in a number of situations where dual-layered encryption is advantageous for improved security. The following are a few possible uses for this:

Channels for Secure Communication: The Rot key transposition cipher can be used to safeguard confidential data while it is being transmitted in secure communication systems where data integrity and confidentiality are essential.

Military Contacts: Strong encryption is frequently needed for military communications in order to protect sensitive information. An additional layer of protection against unwanted access is offered by the dual-layered strategy of row transposition and ROT3.

Money Exchanges: It is crucial to secure financial transactions. Financial systems can use the Rot key transposition cipher to safeguard sensitive financial data and transactional data.

Data Storage Encryption: Sensitive information must be stored safely in a number of industries, including the legal, financial, and healthcare sectors. To add an additional layer of security, stored data can be encrypted using the dual-layered encryption technique.

Government and Diplomatic Communications: For secure communication, government agencies and diplomatic missions require strong encryption techniques. In these situations, the Rot key transposition cipher may be taken into consideration to improve the security of classified data.

Secure File Transfer: The additional security that this encryption technique offers can be advantageous to organizations that engage in secure file transfer, such as law firms that exchange sensitive data or research institutions that share confidential documents.

Cybersecurity Applications: The Rot key transposition cipher can be used as part of a multi-layered defense strategy to secure communication channels and data in the field of cybersecurity, where defending against cyber threats is essential.

Protection of Critical Infrastructure: This cipher can be used by sectors in charge of energy, water supply, transportation, and other vital infrastructure to improve the security of communication and control systems.

It is important to know that as much as this new cipher is stronger than the original version, it still is not secured completely. So we used to keep this in mind while using this cipher.

# Conclusion :

To sum up, we have thoroughly and incisively examined the subjects of cryptography and information technology security. We started by gaining a basic understanding of the CIA triad before delving into the fundamental concepts of availability, confidentiality, and integrity and realizing how important they are to information security. Understanding cryptography and its uses more deeply through study has made it clear how important it is for protecting data and information. Through testing and evaluation of the modified cipher, the journey culminated in the practical application of knowledge. This practical assessment gave real-world insight into the advantages and disadvantages of the cryptography system in addition to validating theoretical ideas.

All in all, this research has given us a deep understanding of cryptography, information security, and the pragmatic factors that are necessary to protect against constantly changing cyberthreats in our globalized society.

# Appendix

# 1. Types of asymmetric algorithm:

**RSA encryption algorithm:**

A popular asymmetric cryptographic algorithm is Rivest Shamir Adleman (RSA). It uses a private and public key pair for encryption and decryption to secure sensitive data.

A set of private and public keys are used by RSA. The public key is accessible to everyone, while the private key is kept confidential and known only to the person who created the key pair. The second key can be used for decryption, and either the public or private key can be used for encryption. Because of this, RSA is among the encryption methods that are most frequently used globally. However, RSA is a resource-intensive and comparatively less efficient algorithm due to its complexity. Therefore, it is not appropriate for encrypting big files or messages (Wickramasinghe, 2023).



Figure 12: RSA encrption (S, 2023)

**DSA encryption algorithm:**

The Digital Signature Algorithm (DSA), is used to create digital signs. It relies on the discrete logarithm challenge and the modular exponentiation procedures to encrypt the signature digitally.

Public-key primitives for verifying messages in cryptography are called digital signatures. The safety of data in cryptoanalysis is regarded as being achieved through the use of public-key in all cryptographic analysis of digital signatures (sharma, 2023).

A diagram of a person with a sign

Description automatically generated

Figure 13: digital signature algorithm (mitra, 2020)

**Elliptic curve digital signature algorithm:**

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a highly intricate encryption algorithm in public key cryptography. Elliptic curve encryption generates keys that are smaller on average than those produced by digital signing algorithms. Public key cryptography based on the algebraic framework of elliptic curves over finite fields is known as elliptic curve cryptography. Digital signatures and the generation of pseudo-random numbers are among the many applications of elliptic curve cryptography (consulting, 2024).

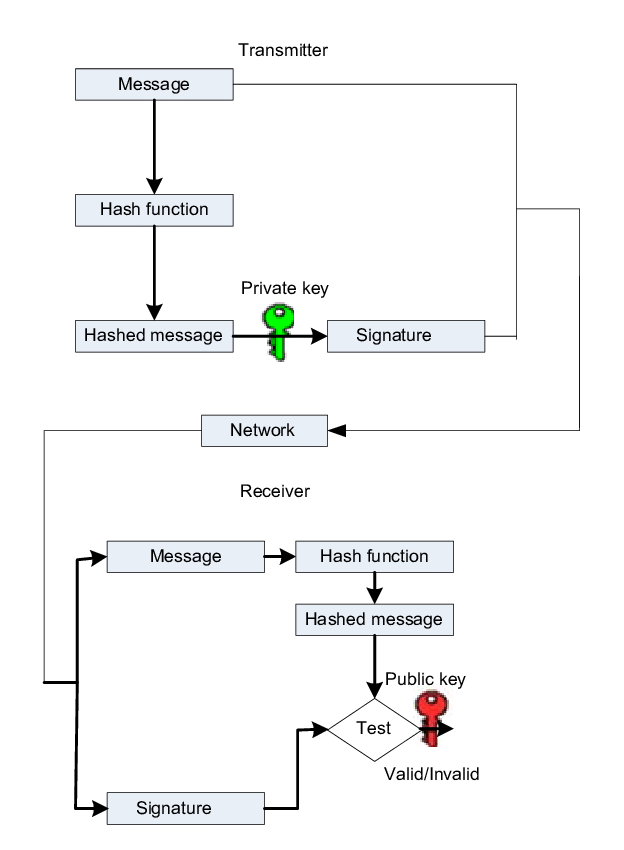


Figure 14: Elliptic curve digital signature algorithm (ghanmi, 2012)

**Diffie-Hellman key exchange algorithm:**

Most commonly employed technique for securely creating and exchanging keys over an unsecure channel was the Diffie-Hellman key exchange. It enables two people who have never met before to safely create a key that they may utilize to encrypt their messages (lake, 2023).

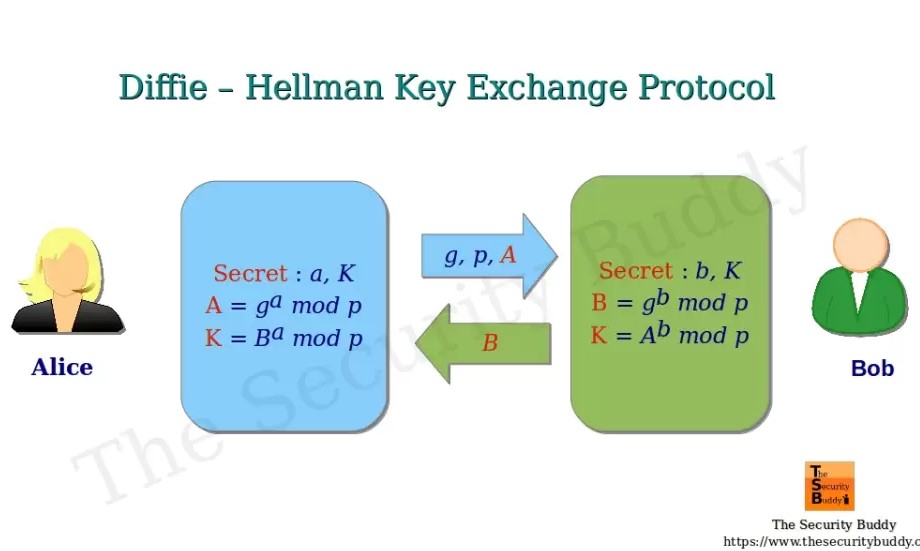


Figure 15:Diffie-Hellman key exchange algorithm (mitra, 2020)

**Elgamal algorithm:**

The challenge of calculating discrete logarithms is exploited by the Elgamal algorithm. We will demonstrate how this challenge gives the algorithm security. However, we must first explain what a primitive root is (Saleh, 2024).

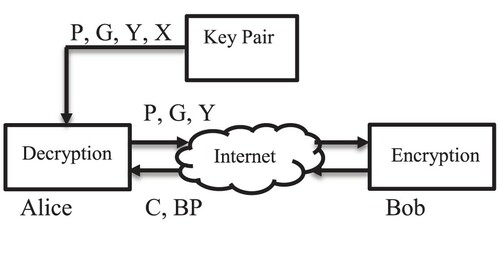


Figure 16:Elgamal algorithm (Hussein, 2019)

**Elliptic curve cryptography algorithm:**

Data encryption using elliptic curve cryptography (ECC) is key-based. Public and private key pairs are the main focus of ECC for both encryption and decryption of internet traffic.

ECC is often discussed in relation to the cryptographic algorithm known as Rivest-Shamir-Adleman (RSA). RSA uses prime factorization to accomplish one-way encryption of items like emails, data, and software (avinetworks, 2024).

A graph of a function

Description automatically generated

Figure 17: Elliptic curve cryptography algorithm (avinetworks, 2024)

# 2. advantages and disadvantages of asymmetric algorithms:

There are various benefits and disadvantages of asymmetric algorithms, some of the known merits and demerits of asymmetric algorithms are listed below in the table:

|  |  |
| --- | --- |
| Merits of asymmetric algorithms (pros) | Demerits of asymmetric algorithms (cons) |
| The use of asymmetric cryptography is more dependable for distributing data on the public the web, but symmetric encryption has only one key, which makes it risky when sending data between different parties. | Because asymmetric encryption is complicated it operates slowly. It is not a suitable option for encrypting servers, hard drives, databases, etc. because it is not appropriate for bulk encryption. |
| Public and private key pairs are required to create security signatures, that add an extra layer of security and guarantee that the message isn't been interfered with and that the person who sent it is who they claim to be. This allows users to authenticate documents. | For information to be useful, it has to be shared using a similar type of encryption by all parties. For the most part, this is not an issue. For instance, all of the main web browsers and service providers use HTTPS, which indicates that they have implemented tools and certificate issuers to guarantee that HTTPS is seamlessly integrated and requires no action from users. The same is true for email, where TLS is used by practically all email suppliers (1kosmos, 2024). |

# References

1kosmos. (2024, 01 05). *asymmetric encrption* . Retrieved from 1kosmos: https://www.1kosmos.com/digital-identity-101/encryption/asymmetric-encryption/

avinetworks. (2024, 01 05). *elliptic curve cryptography* . Retrieved from avinetworks: https://avinetworks.com/glossary/elliptic-curve-cryptography/#:~:text=Elliptic%20Curve%20Cryptography%20(ECC)%20is,Adleman%20(RSA)%20cryptographic%20algorithm.

bacon, m. (2021, 06 29). *security* . Retrieved from techtarget : https://www.techtarget.com/searchsecurity/definition/security

consulting, e. (2024, 01 05). *what is ecdsa*. Retrieved from encryption consulting : https://www.encryptionconsulting.com/education-center/what-is-ecdsa/

corner, c. (2024, 01 10). *columnar transposition cipher* . Retrieved from crypto corner : https://crypto.interactive-maths.com/columnar-transposition-cipher.html

daniel, b. (2021, 05 04). *symmetric vs asymmetric encryption* . Retrieved from trenton systems : https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption

dictionary, c. (2024, 01 05). *security* . Retrieved from collins dictionary : https://www.collinsdictionary.com/dictionary/english/security

forinet. (2023, 12 20). *cyberglossary*. Retrieved from fortinet: https://www.fortinet.com/resources/cyberglossary/cia-triad

forinet. (2023, 12 09). *resources*. Retrieved from forinet: https://www.fortinet.com/resources/cyberglossary/what-is-cryptography

frulinger, j. (2022, 05 22). *what is cryptography*. Retrieved from cso: https://www.csoonline.com/article/569921/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html

geeks, g. f. (2023, 05 22). *difference between symmetric and asymmetric key encrption*. Retrieved from geeks for geeks: https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/

ghanmi, n. (2012). Hardware implementation of elliptic curve digital signature algorithm (ECDSA) on Koblitz curves. *elliptic curve digital signature algorithm (ECDSA)* , 6.

ginni. (2022, 05 15). *tutorialspoint*. Retrieved from what are the basic term used in cyrptography in information security : https://www.tutorialspoint.com/what-are-the-basic-terms-used-in-cryptography-in-information-security

Hussein, H. I. (2019, 10 21). *doi*. Retrieved from tand fonline: https://www.tandfonline.com/doi/full/10.1080/1206212X.2019.1678799

lake, j. (2023, 08 24). *Demystifying Diffie-Hellman key exchange and explaining how it works*. Retrieved from compari tech : https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/

Lubis, F. i. (2017). Combination of Caesar Cipher Modification with Transposition Cipher. *Advances in Science Technology and Engineering Systems Journal*, 25.

mamun, m. (2022, 11 23). *pulse*. Retrieved from linked: https://www.linkedin.com/pulse/basic-terminology-related-cryptography-md-mamun#:~:text=Cipher%2F%20Cryptographic%20Algorithm%3A&text=It%20is%20a%20mathematical%20formula,cryptographic%20algorithm%20is%20called%20decryption.

mitra, a. (2020, 02 21). *how does digital signature algorithm dsa work*. Retrieved from the security buddy : https://www.thesecuritybuddy.com/encryption/how-does-digital-signature-algorithm-dsa-work/

perry, e. (2022, 06 30). *integrity in the work place* . Retrieved from better up : https://www.betterup.com/blog/integrity-in-the-workplace

S, r. A. (2023, 02 20). *tutorials*. Retrieved from simplelearn: https://www.simplilearn.com/tutorials/cryptography-tutorial/asymmetric-encryption

Saleh, M. (2024, 01 05). *elgamal cryptography* . Retrieved from baeldung : https://www.baeldung.com/cs/elgamal-cryptography-algorithm

sharma, m. (2023, 05 25). *digital signature algorithm*. Retrieved from include help: https://www.includehelp.com/cryptography/digital-signature-algorithm-dsa.aspx

team, i. t. (2023, 05 25). *importance of confidentiality* . Retrieved from indeed: https://uk.indeed.com/career-advice/career-development/importance-of-confidentiality

Wickramasinghe, S. (2023, 05 15). *RSA algorithm in cryptography* . Retrieved from splunk: https://www.splunk.com/en\_us/blog/learn/rsa-algorithm-cryptography.html#:~:text=Rivest%20Shamir%20Adleman%20(RSA)%20is,private%20and%20public%20key%20pair.