Table of Contents

Table of Figures 2
Abstract 3
Introduction to Cryptographic Systems 4
Aim 5
Objectives: 5
Critical role of CIA to deliver quality information security: 7
Cryptography and how it works 8
History of Cryptography 9
Timeline of Cryptography 10
Symmetric Key 16
Asymmetric key 16
Background of the Selected Cryptographic Algorithm 17
Development of a new Cryptographic Algorithm 20
Background of the method used in Encryption: 21
Caeser-Fair Cipher: 23
New Encryption Process: 23
New Decryption Process: 24
Algorithm 25
Flowchart 26
TESTING 28
Critical Evaluation of the new Cryptographic Algorithm 41
Conclusion 43
References 44
Appendix: 46

Table of Figures

Figure 1: CIA triad (Pour & Chai, 2021) 7
Figure 2: Process of Cryptography. (An Introduction To Cryptography, 2002) 9
Figure 3: Hieroglyphic Writings (Hieroglyph, 2023) 11
Figure 4: Kamasutra Cipher (Adomey, 2021) 11
Figure 5: Symmetric Key cryptography (An Introduction To Cryptography, 2002). 17
Figure 6 : Asymmetric Encryption (Symmetric vs. Asymmetric Encryption – What are differences?, 2022) 18
Figure 7: Caeser Cipher (Adomey, 2021) 19
Figure 8: Encryption Flowchart 29
Figure 9: Decryption Flowchart 30

Abstract

Organizations face a growing range of risks in today's dynamic and interconnected business environment that have the potential to disrupt confidentiality, integrity, and availability of data/information, from cyberattacks and geopolitical uncertainties. Cryptography have become an essential element for enterprises looking to increase resilience and guarantee continuous flow of uninterrupted and integrity and confidentiality of data’s in the face of several occasions.

The report drives deeper into the topic Cryptography through a development of new cryptographic algorithm. It mainly focuses on the history and background of the cryptographic algorithms and the modification and development of new cryptographic algorithm by recognizing its underlying weaknesses and patching it to make a new more secure cryptographic algorithm. By analyzing and identifying those underlying weaknesses, this report aims develop and modify a new cryptographic algorithm.

Introduction to Cryptographic Systems

Security

Security is a major concern on a global scale, manifesting itself in various issues such as averting terrorist attacks on our ports, airports, public transportation, and other critical national infrastructure; halting the illicit flow of weapons, drugs, and money across international borders; and protecting our wildlife and forests from poachers and smugglers (Sinha, 2015).

Security in information technology describes the procedures, tools, and personnel used to safeguard a company's digital assets. The objective of information technology security is to stop unauthorized users, or threat actors, from interfering with, stealing from, or abusing these devices, services, and resources. These risks could be internal or external, purposeful, or inadvertent (Bacon, 2021).

There are two aspects of IT security:

Information Security:

Information security, or InfoSec for short, is the term used to describe the procedures and instruments created and implemented to safeguard confidential company data against alteration, disruption, destruction, and inspection (Nieles, Dempsey, & Pillitteri, 2017).

Application Security,

Cloud Security,

Cryptography,

Endpoint Security,

Network Security, Physical

Security.

Physical security is the defense against physical acts, intrusions, and other occurrences that could harm an organization and its assets. It includes people, hardware, software, network information, and data (Nieles, Dempsey, & Pillitteri, 2017).

Examples of physical security: Access Control, Surveillance, Testing:

Aim

The aim of this coursework is to properly define about the cryptography and write in depth about Caesar cipher and create and develop a new cryptographic algorithm based of Caeser Cipher.

Objectives:

The objective of the project is to:

- Provide an overview of Security and CIA.
- Provide an in-depth review of cryptography and its history.
- Research the history and methodology of Caesar cipher.
- Develop a new cryptographic algorithm.
- Evaluate and test the new cryptographic algorithm.
- Critically evaluate and analyze the new cryptographic algorithm.

CIA (Confidentiality, Integrity Availability)

Figure 1: CIA triad (Pour & Chai, 2021)

In the context of information security, the three fundamental ideas that serve as the cornerstone of an all-encompassing security framework are known as the "CIA (Confidentiality, Integrity and Availability) triad."

Confidentiality

When information is shielded from exposure to unapproved parties or systems, it is considered confidential. Only those with the necessary authorization, rights, and privileges to access information can do so thanks to confidentiality. Information is violated when it is viewed by unapproved people or programs (Whitman & Mattord, 2017).

Measures to protect the confidentiality of information:

Classification of Information,

Safekeeping of documents,

Educating end users and information custodians (Whitman & Mattord, 2017).

Integrity

When data is complete, whole, and free of corruption, it has integrity. Information that is subjected to corruption, damage, destruction, or other disruptions of its authentic state poses a threat to its integrity (Whitman & Mattord, 2017).

Availability

Availability implies that users should have easy access to the network. This holds true for both data and systems. The network administrator should keep up with hardware maintenance, upgrade frequently, have a fail-over strategy, and avoid network bottlenecks to guarantee availability (Pour & Chai, 2021).

Critical role of CIA to deliver quality information security:

Data security and privacy:

CIA provides insurance against the sophisticated cyberattacks and other unauthorized attempts to obtain, pilfer, or alter sensitive data. It guarantees that information security protocols are thorough, addressing issues with confidentiality, accuracy, and accessibility (Pour & Chai, 2021).

Comprehensiveness:

Due to these three factors, security teams are also concerned with guaranteeing the availability and accuracy of their data in addition to thwarting attackers. Following the CIA triad, for instance, ensures that the data is accessible and available when needed, especially when a significant amount of data is required for analysis (Pour & Chai, 2021).

Risk management:

The triad, when properly implemented, produces a setting where security threats are proactively avoided. Future threats are averted by identifying and mitigating existing vulnerabilities. It aids businesses in recognizing and controlling information security risks (Pour & Chai, 2021).

Flexibility:

The CIA triad is adaptable and can be used in a variety of settings, including corporate, government, and private settings. It offers a framework for developing and accessing information security policies in a range of settings (Pour & Chai, 2021).

Cryptography and how it works.

The study of encrypting and decrypting data with mathematical formulas is known as cryptography. With the use of cryptography, you can send or store private data over unsecure networks, such as the Internet, so that only the intended recipient can read it (An Introduction To Cryptography, 2002).

A mathematical function used in the encryption and decryption process is called a cryptographic algorithm, or cipher. A word, number, or phrase known as a key is used in conjunction with a cryptographic algorithm to encrypt plaintext. Using different keys, the same plaintext can be encrypted into a different ciphertext. The robustness of the cryptographic algorithm and the key's secrecy are the two factors that determine how secure encrypted data is (Whitman & Mattord, 2017).

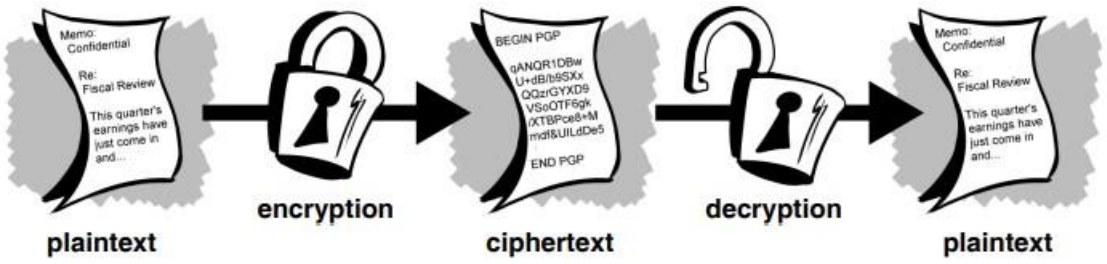

Figure 2: Process of Cryptography. (An Introduction To Cryptography, 2002)

Key Terminology

Plaintext:

Plaintext, also known as cleartext, is data that can be read and understood without the need for extra steps (Whitman & Mattord, 2017).

Encryption:

Encryption is the process of masking plaintext so that its true nature is concealed (Whitman & Mattord, 2017).

Ciphertext:

Encrypting plaintext results in unreadable gibberish called cyphertext (Whitman & Mattord, 2017).

Decryption:

Decryption is the process of translating ciphertext back to plaintext (Whitman & Mattord, 2017).

Key:

The data that is combined with the algorithm to produce the ciphertext from the plaintext; this data can be a set of numbers utilized in a mathematical formula or the understanding of how to work with the plaintext (Whitman & Mattord, 2017).

Algorithm:

Algorithm is the process that transforms an unencrypted message into an encrypted one. Occasionally, this refers to the program that makes the cryptographic operations possible (Whitman & Mattord, 2017).

Substitution Cipher:

A technique for encryption where one value is changed for another (Whitman & Mattord, 2017).

Transposition Cipher:

a type of cryptography where values in a block are just rearranged according to a predetermined pattern. Likewise called a permutation cipher (Whitman & Mattord, 2017).

History of Cryptography

People began to organize into tribes, groups, and kingdoms as civilizations developed. As a result, concepts like politics, dominance, power, and wars came into being. These concepts strengthened people's innate desire to communicate covertly with recipients, which in turn made sure that cryptography would continue to advance (Adomey, 2021).

Hieroglyphic

The use of "hieroglyph" is the earliest known instance of cryptography. The Egyptians utilized hieroglyphic writing to convey messages approximately 4,000 years ago (Hieroglyph, 2023).

Figure 3: Hieroglyphic Writings (Hieroglyph, 2023)

Kamasutra Cipher

One of the oldest substitution techniques that is known to exist is the Kamasutra cipher. It is described in the Kamasutra around 400 BC. Educating women on how to conceal hidden messages from prying eyes was the goal (Adomey, 2021). The method is matching alphabetic letters at random, then replacing each letter in the original message with its corresponding partner.

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

Figure 4: Kamasutra Cipher (Adomey, 2021)

The key is the permutation of the alphabet. Example: INTERNET becomes DWRCTWCR

Timeline of Cryptography

Table 1: History of Cryptography (Whitman & Mattord, 2017)

1900 BC:	The first recorded use of written cryptography was by Egyptian scribes who wrote on clay tablets using nonstandard hieroglyphs.

1500 BC:	The discovery of a tablet containing an encrypted formula for pottery glazes shows how advanced Mesopotamian cryptography was compared to that of the Egyptians. The symbols used on the tablet have context-dependent meanings.
500 BC:	The ATBASH cipher, which substitutes letters in reverse, was utilized by Hebrew scribes to write the book of Jeremiah.
487 B.C:	The skytale is a system that was created by the Spartans of Greece. It is a wooden staff with a papyrus strip wrapped around it. The papyrus was opened, and messages were written down the length of the staff. It was necessary to wrap the papyrus around a shaft of similar material to decrypt it.
50 B.C.	Julius Caesar protected official and military communications with a straightforward substitution cipher. Caesar rearranged the alphabetic characters three positions to create an encrypted text. Caesar improved his encryption by adding a Greek letter substitution scheme to his monoalphabetic substitution cipher.

Fourth to sixth centuries: Cryptography was ranked 44th and 45th out of 64 arts (Yogas) that both men and women should practice according to the Vatsayana Kama Sutra: (44) The ability to decipher writing in cipher and write words in an unusual way; (45) The ability to speak by transforming word forms (Whitman & Mattord, 2017).

725:	A book on cryptography was written by Abu 'Abd al-Rahman al-Khalil ibn Ahmad ibn 'Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, but it is now lost.

	He also cracked a Greek cryptogram by figuring out the plaintext introduction (Whitman & Mattord, 2017).

855:	A learned man named Abu Wahshiyyaan-Nabati wrote several cipher alphabets that were used to encrypt magic formulas (Whitman & Mattord, 2017).
1250:	The English monk Roger Bacon detailed several basic ciphers in his letter Epistle of Roger Bacon on the Secret Works of Art and of Nature and Also on the Nullity of Magic (Whitman & Mattord, 2017).
1392:	An early work called The Equatoria of the Planetis, which may have been authored by Geoffrey Chaucer, included a section using a straightforward substitution cipher (Whitman & Mattord, 2017).
1412-66:	The fourteen-volume Arabic encyclopedia Subhalasha included a section on cryptography that featured ciphers with multiple substitutions, a technique never employed, as well as substitution and transposition ciphers. The inventor of Western cryptography, Leon Battista Alberti, created a cipher disk and experimented with polyalphabetic substitution (Whitman & Mattord, 2017).
1518-63:	The first book on cryptography to be printed was written by Johannes Tritheism, who also created the steganographic cipher, which used a series of columns to represent each letter as a word. Additionally, he presented a now widely used polyalphabetic encryption technique using a rectangular substitution format. He is recognized for having invented the technique of switching replacement alphabets for every letter as it is decoded. Giovan Batista Bellaso is credited with developing the concept of the passphrase, or password, as an encryption key. His polyalphabetic encryption method is now known as the Vigenère Cipher, but it was originally named for someone else who employed the same technique.

	In a classification text he wrote, Giovanni Battista Porta divided encryption techniques into three categories: substitution, transposition, and symbol substitution (Whitman & Mattord, 2017).
1623:	Bacon in his encryption technique. He concealed each letter of the cipher within a random text by subtly altering its font (Whitman & Mattord, 2017).
1790s:	When serving as ambassador to France in the 1790s, Thomas Jefferson invented a 26-letter wheel cipher that he used for official correspondence. The wheel cipher idea was redesigned in 1854 and again in 1913 (Whitman & Mattord, 2017).

1854:	Thomas Jefferson's wheel cipher was redesigned by Charles Babbage in 1854 (Whitman & Mattord, 2017).
1861-5:	Union forces employed a substitution encryption technique during the American Civil War, while the Confederacy employed a polyalphabetic cipher, the solution to which was known prior to the conflict (Whitman & Mattord, 2017).
1914-19:	Throughout World War I, the Germans, British, and French used a series of transposition and substitution ciphers in radio communications. All sides expended considerable effort to try to intercept and decode communications, and thereby created the science of cryptanalysis. British cryptographers broke the Zimmerman Telegram, in which the Germans offered Mexico U.S. territory in return for Mexico’s support. This decryption helped to bring the United States into the war (Whitman & Mattord, 2017). The U.S. government hired William Frederick Friedman, the pioneer of American cryptanalysis, and his wife Elizabeth as civilian cryptanalysts. Later, Friedman established a cryptanalysis school in Riverbank, Illinois.

	An AT&T employee named Gilbert S. Vernam created a polyalphabetic cipher machine that used a random nonrepeating key. Hugo Alexander Koch filed a patent in the Netherlands for a rotor-based cipher machine; in 1927, Koch assigned the patent rights to Arthur Scherbius, the inventor of the Enigma machine (Whitman & Mattord, 2017).
1927-33:	During Prohibition, criminals in the United States began using cryptography to protect the privacy of messages used in illegal activities (Whitman & Mattord, 2017).
1937:	The Japanese developed the purple machine, which was based on principles like those of Enigma and used mechanical relays from telephone systems to encrypt diplomatic messages. By 1940, a team headed by William Friedman had broken the code generated by this machine and constructed a machine that could quickly decode Purple's ciphers (Whitman & Mattord, 2017).
1939-48	Without a doubt, the Allies' covert deciphering of the Enigma cipher helped to shorten World War II. 1942 saw the entry of Navajo code talkers into World War II; in addition to speaking a language that was only known by a small portion of the American population, the Navajos created code words for topics and concepts that were foreign to their mother tongue. Claude Shannon proposed the use of statistical analysis and frequency in the solution of substitution ciphers (Whitman & Mattord, 2017).
1970-78:	The Lucifer cipher was developed by an IBM research team under the direction of Dr. Horst Feistel. The U.S. National Security Agency selected a Lucifer-based design to serve as the Data Encryption Standard, which gained international recognition. Martin Hellman and Whitfield Diffie proposed the concept of public-key cryptography.

	The RSA family of computer encryption algorithms was created by Ronald Rivest, Adi Shamir, and Leonard Adleman when they created a workable publickey cipher for digital signatures as well as confidentiality. Communications of the ACM published the first version of the RSA algorithm (Whitman & Mattord, 2017).
1991- 2000	The original PGP (Pretty Good Privacy) program was created by Phil Zimmermann; it was made available as freeware and quickly rose to prominence as the industry standard for public cryptosystems. 2000 saw the selection of Rijndael's cipher as the Advanced Encryption Standard (Whitman & Mattord, 2017).

Symmetric Key

Algorithms are connected to this technique. It employs a single digital key for both encryption and decryption. Other names for it include shared key, private key, secret key, and personal key. The named keys are related to each other even though they are not exact duplicates. However, symmetric cryptography is a fragile method of data protection. It can be hacked and is vulnerable to criminal attacks due to its ease of decoding. Nonetheless, the chance of decoding is decreased if it is well-thought out and carried out (Gencoglu, 2019).

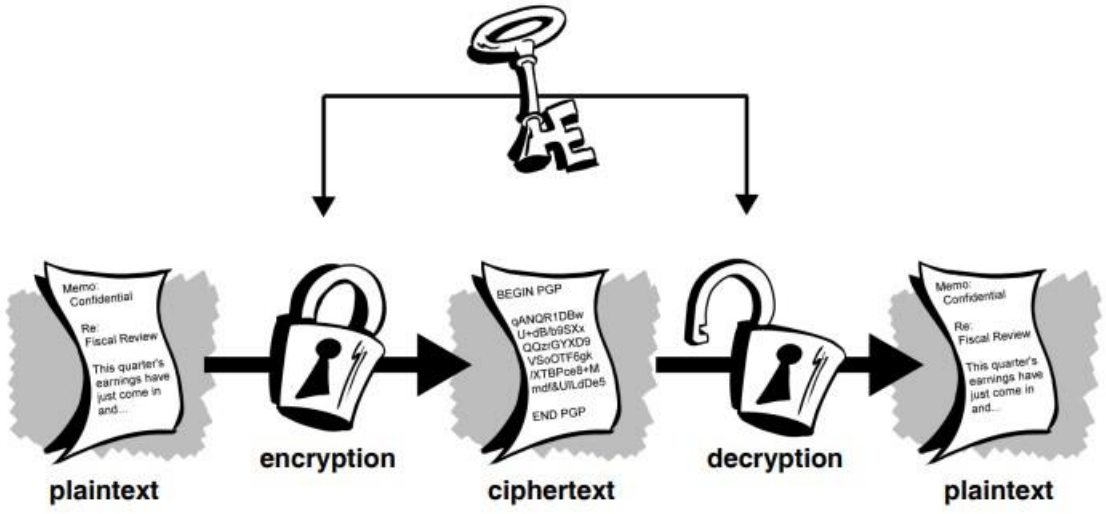

Figure 5: Symmetric Key cryptography (An Introduction To Cryptography, 2002).

Asymmetric key

Several digital keys are used in this cryptography method to both encrypt and decrypt data. The end user uses two digital keys in asymmetric cryptography. Digital keys are allocated with one being used for encryption and another for decryption. The terms "public" and "private" refer to these digital keys. There are differences between the two keys. As a result, asymmetric cryptography is generally thought to be safe and secure. Asymmetric cryptography employs the practice of assigning a key to a specific class of data. A captivating idea in asymmetric cryptography is the use of a randomly generated digital key that is assigned by the sender or the public key keeper (Gencoglu, 2019).

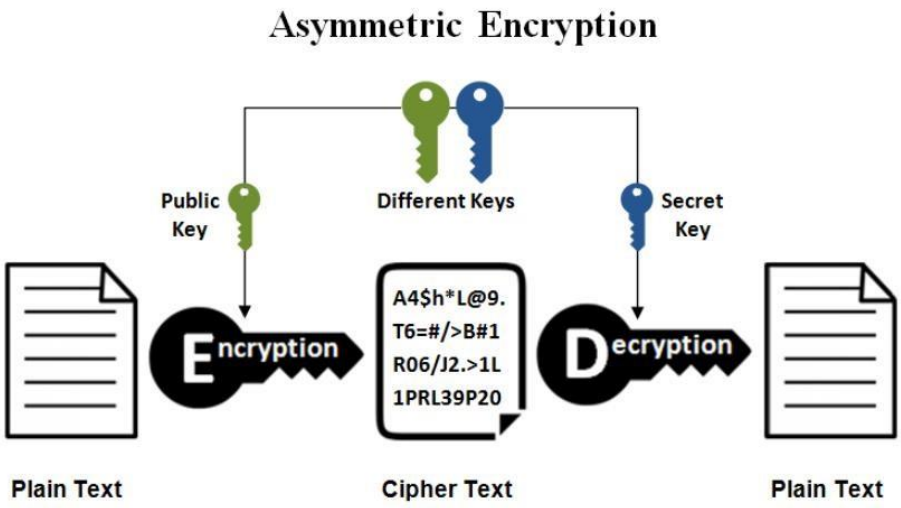

Figure 6 : Asymmetric Encryption (Symmetric vs. Asymmetric Encryption – What are differences?, 2022)

Private Key: A private key is a cryptographic key that is created and used by an individual or system to encrypt messages intended for a particular recipient. The original message can only be decrypted using the same key that is known to the recipient. It is a variable that is used with an algorithm to encrypt and decrypt code, and it is also referred to as the secret key (Chhetri, Khadka, & Thapa, 2019).

Public key: Public key encryption cryptography generates a public key by using asymmetric-key encryption algorithms to create a key that is then encrypted with a public key to transform a secret message into an unintelligible message (Chhetri, Khadka, & Thapa, 2019).

Background of the Selected Cryptographic Algorithm

Caeser Cipher:

One of the simplest and oldest known ciphers is the Caesar cipher. This kind of substitution cipher causes each letter in the plaintext to move down the alphabetic sequence by a predetermined

number of places. A shift of the 2 would, for instance, cause the letters A and B to change to C and D, respectively, and so on (Gowda, 2016). It consists of 25 possible keys in the standard English alphabet.

The Caesar cipher is named after Julius Caesar, who used it with a shift of three to protect messages of military significance (R.F.Churchouse, 2001). Although Caesar's was the first known application of this scheme, there are known earlier uses of other substitution ciphers.

Working methodology of Caeser Cipher:

An integer known as the key serves as the foundation for the encryption. The amount that each letter in the plaintext is shifted depends on the key (An Introduction To Cryptography, 2002).

The alphabet's letters are shifted by the designated amount. For instance, using a 3 key:

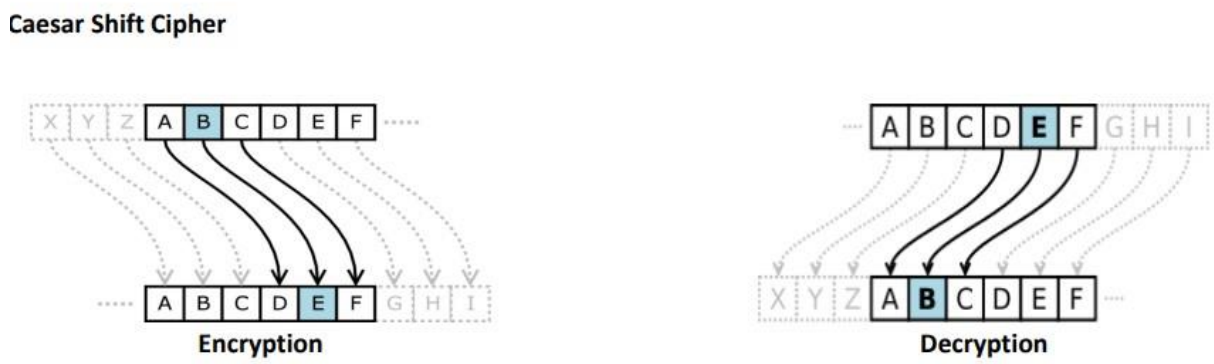

Figure 7: Caeser Cipher (Adomey, 2021)

For Encryption, every letter in the plaintext is changed to a letter one set number of positions higher or lower in the alphabet. In this case the key value is 3 so, Plaintext: Sonam is me.

Encrypted Ciphertext: vrqdp lv ph.
Now for decryption, the letters are moved in the opposite direction to complete the process in reverse.

Decrypted plaintext: Sonam is me.

Advantages (pros) of Caeser Cipher:

- One of the most straightforward encryption techniques to add an extra layer of protection to your data.
- The cipher is simple to learn and has a low learning curve, making it ideal for expanding its applications.
- For the process, only one kind of key needs to be used.
- It requires a small amount of computer power. It is possible to translate and reply to messages fast.
- The Caesar Cipher is the best substitute for straightforward systems that are unable to use complex coding techniques.

Disadvantages of Caeser Cipher:

- Too straightforward and simple for an unauthorized person to decode.
- It offers the barest possible level of protection.
- The hacker can reduce the potential cipher shift from the letter pattern.

Development of a new Cryptographic Algorithm

The Caesar cipher is a straightforward and important cryptographic algorithm in history, but because of its small key space and vulnerability to brute-force attacks. The Caesar cipher has been suggested to be improved and modified in several ways to increase its security. These adjustments usually entail making the encryption procedure more complicated or random. Here are a few noteworthy modifications to make it more secure:

Combination Method:

Multiple encryptions, sometimes referred to as "double encryption," "combiners," or "hybrid encryption," enables the fusion of several distinct cryptographic schemes to produce a single, new, secure scheme. Attacks that aim to compromise just one of its elements are thwarted by this novel combined scheme (Buchmann & Sorceanu, 2023).

Polyalphabetic Method:

Any cipher based on substitution that makes use of multiple substitution alphabets is called a polyalphabetic cipher. The plaintext letters in polyalphabetic substitution ciphers are enciphered in different ways according to where they are installed in the text. Every letter has a one-to-many relationship with its substitutes instead of a one-to-one correspondence (Ginni, 2022).

Incorporate XOR Operation: By comparing two input bits, XOR produces a single output bit. The reasoning is straightforward. The outcome is zero if all the bits are the same. The outcome is 1 if the bits differ. The use of XOR can help to make the encryption more secure.

Block Caeser Cipher: Separate the plaintext into blocks and encrypt each block separately using the Caesar cipher. This change increases complexity and might offer more defense against specific threats.

Different ciphertext compared to plaintext: In this method the number of ciphertext doesn't match the number of words in the plaintext making it harder for attackers to guess the plaintext. This method enhances security as Caesar cipher has same amount of plaintext as compared to ciphertext.

Example: Plaintext: we

Ciphertext: ADZ5

Background of the method used in Encryption:

These modifications are made by taking in consideration of the cons of the Caeser cipher and fixing it solely to improve the security of Caeser Cipher.

1st Modification

Combination Method:

Here, Caeser Cipher is combined with play-fair cipher to create a new algorithm.

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Here the alphabets are arranged in 3 rows and 8 columns. The 4th row is added to add up for the two missing alphabets. The alphabet "Y" is divided into two parts "Y^1" and "Y^2" to balance up the grid. If "y" is present in a plaintext more than once then,

For Example: sysyty here the first Y is always "Y^1" and second one is "Y^2" and third y is again "Y^1".

Here the same rule is applied as Caeser Cipher, but the working mechanism is different.

The shift in cipher

For Example: Key Value:6

Plain text: Sonam

Encryption:

Ciphertext: Y^2LKGJ

For Decryption the key value is "Key- number of columns" (6-9) = 3

Plaintext: Sonam

To further secure the algorithm,

2nd Modification

Polyalphabetic Method:

Here the keys are generated differently letter by letter. Each letter has a unique key.

Plaintext: Shuba

Here the plaintext is changed in a mixed pattern by applying different shifting key value to each letter.

The key is generated randomly.

For Encryption

Key: 24176

Ciphertext: UCVY^1G

Now for Decryption the key will be “Key- number of columns” (2-9) = 7, (4-9) = 5, (1-9) = 8, (79) = 2, (6-9) = 3.

Key: 75829

Plaintext: Shuba

3rd Modification

Different ciphertext compared to plaintext:

Here, the modification is solely targeted to improve the flaw of caeser cipher where the plaintext is equivalent to ciphertext.

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Ciphertext: Poh

Key: 374

Modified Ciphertext = 10403

=AZDZ3

Caeser-Fair Cipher:

New Encryption Process:

Firstly, the two cryptographic algorithm Caesar cipher and Playfair is combined to make a table.

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext = Hi Sonam

Secondly a random key is generated,

First Key = 2516437

The plaintext is shifted according to the key value provided to each alphabet.

So, Cipher Text = AN TLIDK

Now to make the number of cipher text and plaintext different in terms of number of letters we convert it by using the following table.

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Here, the cipher text = AN TLIDK

Second Key = 81 75826

New cipher text = Y^1O RZZFZ = AFZFZ IZ0060

New Decryption Process:

Ciphertext = AFZFZ IZ0060

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Decryption is done through the above table.

AFZFZ IZ0060

Y^1O RZZFZ

Key for decryption: 18 24173

AN TLIDK

Now using the reverse of second key

Key = 7483562

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext: Hi Sonam

Algorithm

Step 1: Start

Step 2: Input:

- Plain Text

- Key

Step 3: Create

-Two Random Keys

Step 4: Generate two Tables:

- Fill an 8x2 matrix table from A-Z, excluding duplicates and unique characters.

- Fill an 8x2 matrix table with all the alphabets and numbers from 0-9 and unique characters.

Step 5: Encrypt the plaintext using the tables and keys.

Step 6: Stop Decryption:

Step 1: Start

Step 2: Input:

- Ciphertext

Step 3: Create

-Two Keys from the previously used keys using a formula.

Step 4: Generate two Tables:

- Fill an 8x2 matrix table from A-Z, excluding duplicates and unique characters.

- Fill an 8x2 matrix table with all the alphabets and numbers from 0-9 and unique characters.

Step 5: Decrypt the ciphertext using the tables and keys.

Step 6: Stop

Flowchart

Encryption

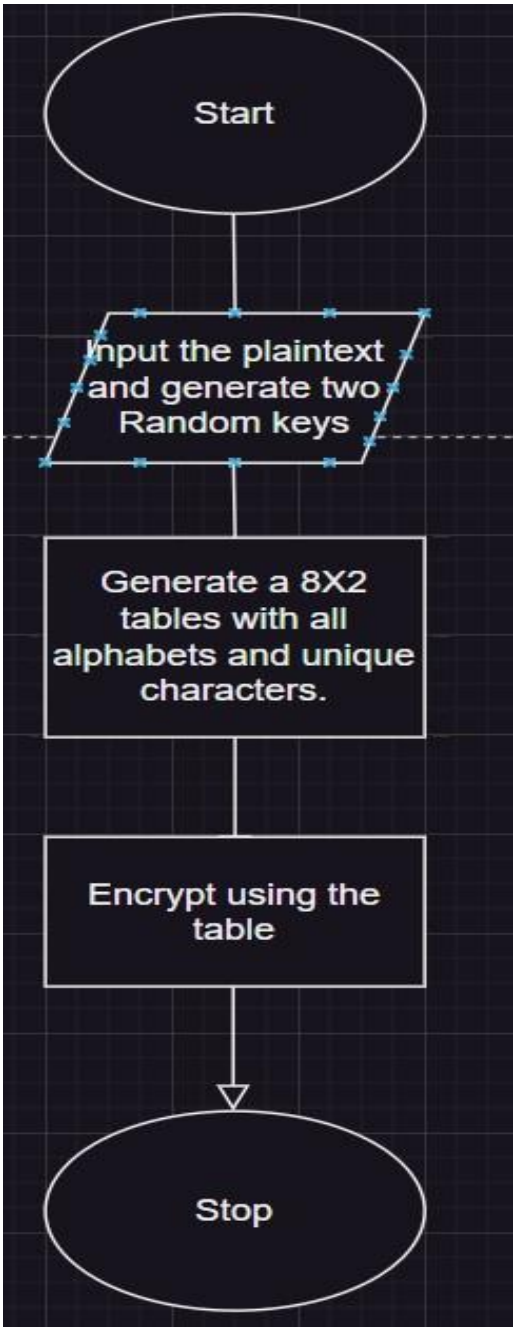

Figure 8: Encryption Flowchart

Decryption

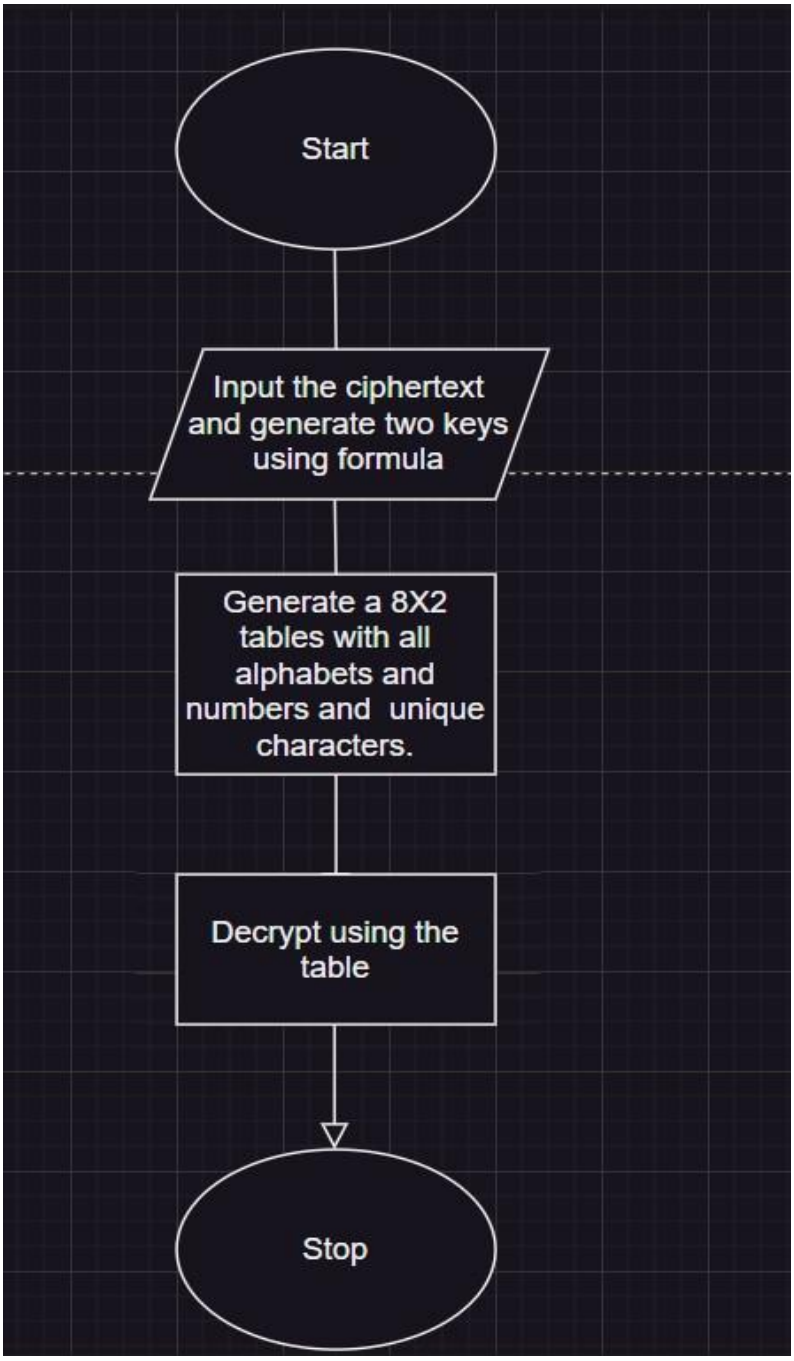

Figure 9: Decryption Flowchart

TESTING

Test 1: Encryption

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext = Abhinav

Secondly a random key is generated,

First Key = 6285741

The plaintext is shifted according to the key value provided to each alphabet.

So, Cipher Text = GDGNLEW

Now to make the number of cipher text and plaintext different in terms of number of letters we convert it by using the following table.

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Here, the cipher text = GDGNLEW

Second Key = 8175826 (Randomly generated)

New cipher text = FEEJKGT = 655AZBZ7AZZ

Decryption

Ciphertext = 655AZBZ7AZZ

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Decryption is done through the above table.

FEEJKGT

Key for decryption: 18 24173

GDGNLEW

Now using the reverse of second key 6285741

Key = 3714258

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext: Abhinav

Encryption

	B	C	D	E	F	G	H	Y^1

Test 2

A

I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext = Hello its me

A random key is generated,

First Key = 78102 537 68 (Randomly Generated)

The plaintext is shifted according to the key value provided to each alphabet.

So, Cipher Text = FDJLZ NWQ JD

Now to make the number of cipher text and plaintext different in terms of number of letters we convert it by using the following table.

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0

Here, the cipher text =

Second Key =

New cipher text =

Decryption:

Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

FDJLZ NWQ JD

77405 782 82 (Randomly generated) 42EZCZDZ

CZACZAZZ 96

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Decryption is done through the above table.

Ciphertext = 42EZCZDZ CZACZAZZ 96

Key = Second Key (77405 782 82) – 9 = 22504 217 17

Ciphertext: FDJLZ NWQ JD

Now,

Key = First Key (78102 537 68) – 9 = 21807 462 31

A	B	C	D	E	F	G	H	Y^1

Encryption

	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Decryption is done through the above table:

Plaintext: Hello its me

Test 3

A

I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext = Bueno Noches

A Random key is generated,

First Key = 57431 326825

The plaintext is shifted according to the key value provided to each alphabet.

Here, the cipher text =

Second Key =

New cipher text =

Decryption:
So, Cipher Text = GSY^1ZP ZZY^1GGX

Now to make the number of cipher text and plaintext different in terms of number of letters we convert it by using the following table.

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

GSY^1ZP ZZY^1GGX

24615 134272(Randomly generated)

AFZADZ69CZ 9BZ4AFZ5HZ

Encryption

	B	C	D	E	F	G	H	Y^1
I = 9	J = 10=	K = 20	L = 30	M = 40	N = 50	O = 60	P = 70	Z = 0
	AZ	BZ	CZ	DZ	EZ	FZ	GZ	
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Decryption is done through the above table.

Ciphertext = AFZADZ69CZ 9BZ4AFZ5HZ

Key for decryption = Second Key (24615 134272) – 9 = 75384 865727

Ciphertext = GSY^1ZP ZZY^1GGX

Now,

Key = First Key (57431 326825)-9 = 42568 673174

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Decryption is done through the above table:

Plaintext: Bueno Noches
Here, the cipher text =

Second Key =

New cipher text =

Decryption:

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ

Test 4

A

I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext = Good Morning

A Random key is generated,

First Key = 5281 3528621

The plaintext is shifted according to the key value provided to each alphabet.

So, Cipher Text = CZNE PKTMOPH

Now to make the number of cipher text and plaintext different in terms of number of letters we convert it by using the following table.

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Encryption

B	C	D	E	F	G	H	Y^1
	CZNE PKTMOPH						

15267 62731512(Randomly generated) Here C's Key is 15 and H's key is 12.

AFZAZBZ3 50DZ90GZGZCZ2

I = 9 J = 10= K = 20 L = 30 M = 40 N = 50 O = 60 P = 70 Z = 0

	AZ	BZ	CZ	DZ	EZ	FZ	GZ	
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Decryption is done through the above table.

Ciphertext = AFZAZBZ3 50DZ90GZGZCZ2

Key for decryption = Second Key (15267 62731512) – 9 = 3732 3726846

Ciphertext = CZNE PKTMOPH

Now,

Key = First Key (5281 3528621)-9 = 4718 6471378

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z

Here, the cipher text =

Second Key =

New cipher text =

Decryption:

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
Q	R	S	T	U	V	W	X	Y^2

Decryption is done through the above table:

Plaintext: Good Morning

	B	C	D	E	F	G	H	Y^1

Test 5

Encryption:

A								
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Plaintext = Your youtube is not working

A Random key is generated,

First Key = 2222 4444444 88 555 7777777

The plaintext is shifted according to the key value provided to each alphabet.

So, Cipher Text = BZWT DJY^2XY^2FY^1 ZR JKY^2 UMY^2IZLE

Now to make the number of cipher text and plaintext different in terms of number of letters we convert it by using the following table.

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ

Here, the cipher text =

Second Key =

New cipher text =

Decryption:

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ
I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

BZWT DJY^2XY^2FY^1 ZR JKY^2 UMY^2IZLE

1111 3333333 66 777 2222222(Randomly generated)

39AEZABZ 7DZAZZIZAZZAFZ3 50AEZ 09ACZ ADZ60IZ20AZ507

I = 9	J = 10= AZ	K = 20 BZ	L = 30 CZ	M = 40 DZ	N = 50 EZ	O = 60 FZ	P = 70 GZ	Z = 0
Q = 80 HZ	R = 90 IZ	S = 100 = AZZ	T = 110 = AAZ	U =120 = ABZ	V =130 =ACZ	W=140 =ADZ	X=150 =AEZ	Y^2=160 =AFZ

Decryption is done through the above table.

Ciphertext = 39AEZABZ 7DZAZZIZAZZAFZ3 50AEZ 09ACZ ADZ60IZ20AZ507

Key for decryption = Second Key (1111 3333333 66 777 2222222) – 9 = 8888 6666666 33 222 7777777

Ciphertext = BZWT DJY^2XY^2FY^1 ZR JKY^2 UMY^2IZLE

Now,

Key = First Key (2222 4444444 88 555 7777777)-9 = 7777 5555555 11 444 2222222

A	B	C	D	E	F	G	H	Y^1
I	J	K	L	M	N	O	P	Z
Q	R	S	T	U	V	W	X	Y^2

Decryption is done through the above table:

Plaintext: Your youtube is not working

Critical Evaluation of the new Cryptographic Algorithm

Strengths:

- The Caesar cipher had same size of texts in both ciphertext and plaintext while the newly created has different size of letters.
- The modification is resistance against frequency analysis as the number of keys are different from one another.
- The size of plaintext is different in comparison to cipher text making it more secure.
- The ciphertext contains numbers which makes the modification more secure as compared to Caeser Cipher.
- There are 4 different keys, and all keys differs from one another.

Weakness:

- The encryption and decryption cannot happen if the number 9 arises cause of the table being of 9 columns.
- The size of the key is equivalent to plaintext and ciphertext making it vulnerable to attacks.
- Easy to predict as encryption and decryption follows the same steps.
- The modification is not that long making it less time consuming for attackers to crack.
- The table is limited making it vulnerable.

Decryption:

A = 1	B = 2	C = 3	D = 4	E = 5	F = 6	G = 7	H = 8	Y^1=160 =AFZ

The application area where the Caeser-Fair Cipher can be used is:

Government Organizations:

Caeser-Fair Cipher is used in protecting confidential data of the organizations, encryption of data and text messages within the organization areas.

Conclusion

In conclusion, the field of cryptography is essential to protecting sensitive data in the digital age. Extensive algorithms and protocols that guarantee data integrity, confidentiality, and authenticity have been developed because of the development of cryptography. The Caesar cipher is a fundamental concept in the evolution of cryptography, despite its apparent simplicity. The Caesar cipher is a historical cipher that helped to establish the foundation for more complex cryptographic techniques that are employed today.

The report discussed about the history of cryptography, its algorithm and also the analysis and evaluation of the development of new cryptographic algorithm by patching up its flaws and modifying it for a secure system.

Furthermore, it emphasizes on the history and beneficiary of cryptography in the modern society.

References

Adomey, M. K. (2021). *AfricaCert.* Retrieved from Introduction to Cryptography : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/01Introduction%20to%20Cryptography.pdf

An Introduction To Cryptography. (2002). USA: PGP Cooeration.

Bacon, M. (2021, June). *Security*. Retrieved from Tech Target: https://www.techtarget.com/searchsecurity/definition/security

Buchmann, N., & Sorceanu, T. (2023). On Multiple Encryption for Public-Key Cryptography. *Cryptography Vol 7*.

Chhetri, B., Khadka, K., & Thapa, S. (2019). Crypto-System: A Modified Ceaser Cipher. In K. D. Sherpa, *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)}* (pp. 251-254). India: INDIACom. Retrieved from IEEE: https://ieeexplore.ieee.org/document/8991352

Gencoglu, M. T. (2019). Importance of Cryptography in Information Security. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 65-68.

Ginni. (2022, March). *What is Polyalphabetic Substitution Cipher in Information Security?* Retrieved from Tutorialspoint: https://www.tutorialspoint.com/what-is-polyalphabeticsubstitution-cipher-in-information-security

Gowda, S. N. (2016). *Innovative Enhancement Of The Caesar Cipher.* Retrieved from Researchgate: https://www.researchgate.net/profile/Shreyank-Gowda/publication/310624556_Innovative_enhancement_of_the_Caesar_cipher_algorithm_for_cryptography/links/5a001f58aca272347a2b2c9a/Innovative-enhancement-of-theCaesar-cipher-algorithm-for-cryptography.pdf

Hieroglyph. (2023, October 17). Retrieved from Britannica, T. Editors of Encyclopaedia: https://www.britannica.com/topic/hieroglyph

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017, June). *An Introduction to Information Security.* Retrieved from NIST : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Pour, C., & Chai, W. (2021). *CIA triad (confidentiality, integrity and availability)*. Retrieved from Tech Target: https://www.techtarget.com/whatis/definition/Confidentiality-integrityand-availability-CIA

R.F.Churchouse. (2001). *Codes and Ciphers Julius Caesar, the Enigma and the internet.* Trumpington Street, Cambridge: The press syndicate of the University of Cambridge. Retrieved from Codes and ciphers Julius Caesar, the Enigma and the internet:

https://d1wqtxts1xzle7.cloudfront.net/66645507/Codes_and_Ciphers_Julius_Caesar_The_Enig20210423-21192-1hfnkee.pdf?1619213665=&response-contentdisposition=inline%3B+filename%3DCodes_and_Ciphers_Julius_Caesar_The_Enig.pdf
&Expires=1704880869&Signature=SOwWJ

Sinha, A. (2015). From physical security to cybersecurity. *Journal of Cybersecurity*, 19-35. Retrieved from https://watermark.silverchair.com/tyv007.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAA10wggNZBgkqhkiG9w0BBwagggNKMIIDRgIBADCCAz8GCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMd_4ELd3V3Gc7buq-AgEQgIIDEEe9lA9vmdNU8i5Mx0S2qxm-Aqza63LI8U47xFWfVlbgF3TW

Symmetric vs. Asymmetric Encryption – What are differences? (2022). Retrieved from SSL2BUY: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-whatare-differences

Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security, Sixth Edition.* Boston: Cengage Learning.

Appendix:

Polyalphabetic Cipher:

Leon Battista Alberti invented the Alberti Cipher in 1467, making it the first polyalphabetic cipher. The plaintext was encrypted using a random alphabet, but it could occasionally switch to a different mixed alphabet, signaling the change in the cipher text with an uppercase letter (Ginni, 2022).

Alberti demonstrated how plaintext letters are connected to cipher text letters using a cipher disc. This cipher can be used. Every ciphertext character in this cipher is determined by the plaintext character's position in the message as well as its corresponding character in the plaintext (Ginni, 2022).

As suggested by the term polyalphabetic, this is accomplished by using several keys as opposed to just one. This suggests that the key should consist of a series of subkeys, each of which is dependent on the plaintext character's position that requires a subkey to be deciphered (Ginni, 2022).

Stated differently, a key stream k = (K1, K2, K3...) is necessary, wherein Ki is utilized to encrypt the character from the plaintext and create the ith character from the ciphertext. The most wellknown and basic algorithm of this type is known as the Vigenère cipher (Ginni, 2022).

Hash Function:

A hash is a compact fixed size bit string created by mapping an input message. Mathematical algorithms known as hash functions are one-way functions that convert an arbitrary-sized input message into a fixed-size hash or message digest (Alenezi, 2020).

Types of Hashing:

Secure Hashing Algorithm (SHA),

RACE Integrity Primitives Evaluation Message Digest (RIPEMD),

Message Digest Algorithm (MD),

Whirlpool (Alenezi, 2020).