



 slingshot college
(इस्लिङ्टन कलेज)

Module Code & Module Title
CC5009NI Cyber Security in Computing

Assessment Weightage & Type
40% Individual Coursework 01

Year and Semester
2024 -25 Autumn Semester

Student Name: Nishant Kasaudhan
London Met ID: 23047560
College ID: NP01NT4A230221

Assignment Due Date: Monday, 20 January 2025
Assignment Submission Date: Monday, 20 January 2025
Word Count (Where Required): 5841





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.






8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **39 Not Cited or Quoted 8%**
Matches with neither in-text citation nor quotation marks
-  **3 Missing Quotations 0%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 2%  Internet sources
- 1%  Publications
- 8%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Abstract

This coursework introduces the concept of cryptography by looking into the CIA Triad, and by learning about the Caesar cipher, which is one of the oldest methods of cryptography. The three types of aims in Information security are the CIA triad, with Confidentiality the aim that only the permitted people are able to get to the information, Integrity aiming to protect the information from being changed and Availability that the information and services are available at the right time to the permitted persons. These principles form the foundation on which security is established for information in different electronic systems.

The Caesar cipher remains an important model for understanding past and present cipher systems even as it is easy to penetrate with present day cryptographic tools. This coursework deals with the detailed description of the Caesar cipher and its implications in ciphering systems in addition to studying more advanced encryption techniques. Through studying these concepts, this coursework gives a broad understanding of the basic methods of cryptography and their use in protection of information according to the overall principles of the CIA Triad.

Table of Contents

Abstract.....	3
1 Task 1:.....	6
1.1 Introduction	6
1.2 CIA in Cryptography:.....	6
1.3 History Of Cryptography	7
1.4 The symmetric ciphers and The Asymmetric ciphers.....	9
2. Task 2:.....	12
2.1 Caeser Cipher	12
Introduction	12
How Caeser Cipher Works:.....	12
2.2 Example of Encryption and Decryption.....	12
2.3 Advantage and Disadvantages	13
3 Task 3.....	14
3.1 Mathematical and Logical	14
3.2 Introduction of Mathematical and Logical Operartions	15
3.3 New Encryption and Decryption Cryptographic.....	16
3.4 Name your new Cryptographic Algorithm.....	16
3.5 Why was the modification necessary?	16
3.6 New Mothodology Implied	16
3.7 New Encryption Algorithm.....	16
3.8 New Decryption Algorithm.....	17
4 Testing.....	17
Text 1: IOS	17
Text 2: MAC	19
Text 3: CAT.....	20
Text 5: SAD.....	22
Task 5.....	23
5.1 Strengths of the Combined Cipher	23
5.2 Weakness of the Combined Cipher	23
Conclusion	23

Figure 1 Figure Of Cryptography	6
Figure 2 CIA triad.....	7
Figure 3 History of Cryptography.....	8
Figure 4 Symmetric Cipher.....	10
Figure 5 Asymmetric Ciphers.....	11

Cryptography

1 Task 1:

1.1 Introduction

The science and art of converting data into a safe format that only authorised parties can access and comprehend is known as cryptography. From ancient cyphers to contemporary digital encryption methods, cryptography which comes from the Greek words "kryptos" (hidden) and "graphien" (writing) has been used for centuries to protect sensitive data.

Cryptography is the study and application of methods to protect data and communications against unwanted access or modification. It is employed to guarantee the confidentiality, integrity and availability information. In fields like digital signatures, secure communications, cybersecurity, and cryptocurrency, cryptography is crucial.

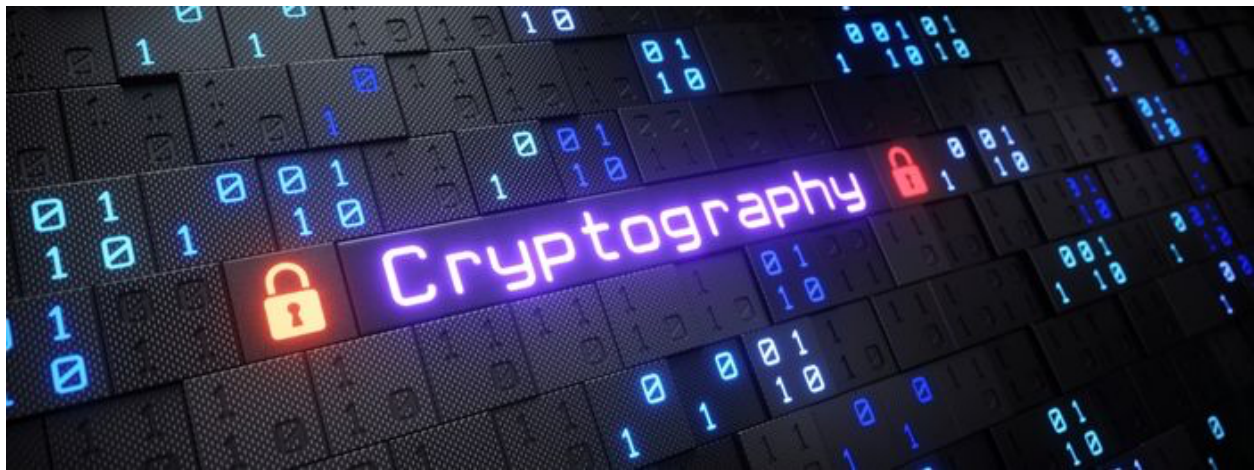


Figure 1 Figure Of Cryptography

1.2 CIA in Cryptography:

The three main goals of cryptography and information security are described in the CIA Triad model. Consider it the cornerstone upon which a secure system is constructed, guaranteeing that systems and data are shielded from dangers and weaknesses.

- ❑ Confidentiality: Making sure that only those individuals or systems with the proper authorisation can access sensitive data is the aim here.
- ❑ Integrity: This guarantees that the data is accurate and unaltered. Making sure that no one intentionally or accidentally tampers with your information is the goal.
- ❑ Availability: This guarantees that systems and data are available whenever authorised users require them.



Figure 2 CIA triad

Role of CIA in Cryptography:

- ❑ Confidentiality: Accomplished by using encryption methods such as RSA or AES (Advanced Encryption Standard).
- ❑ Integrity: Digital signatures and hashing techniques (like SHA-256) are used to ensure security.
- ❑ Availability: Protected by cryptographic techniques such as secure key transfers and attack-resistant protocols.

1.3 History Of Cryptography

The history of cryptography is vast and fascinating, covering thousands of years, from basic secret-writing methods to sophisticated mathematical algorithms used in modern computing. It has always been essential for securing communication, protecting private data, and affecting historical developments.

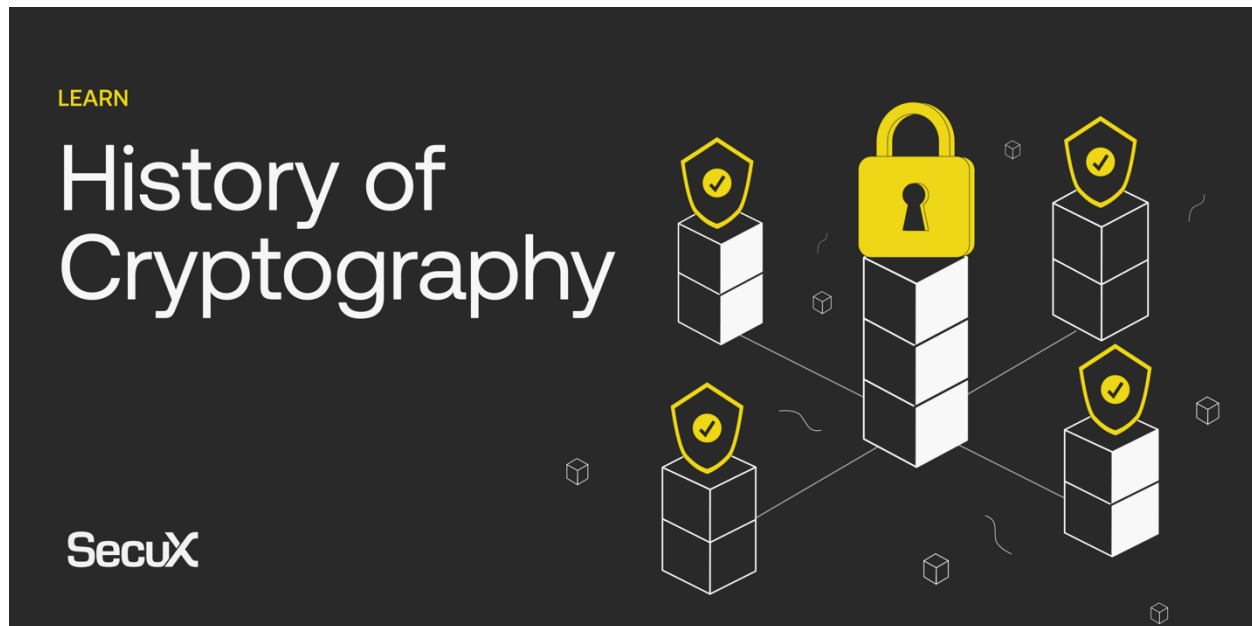


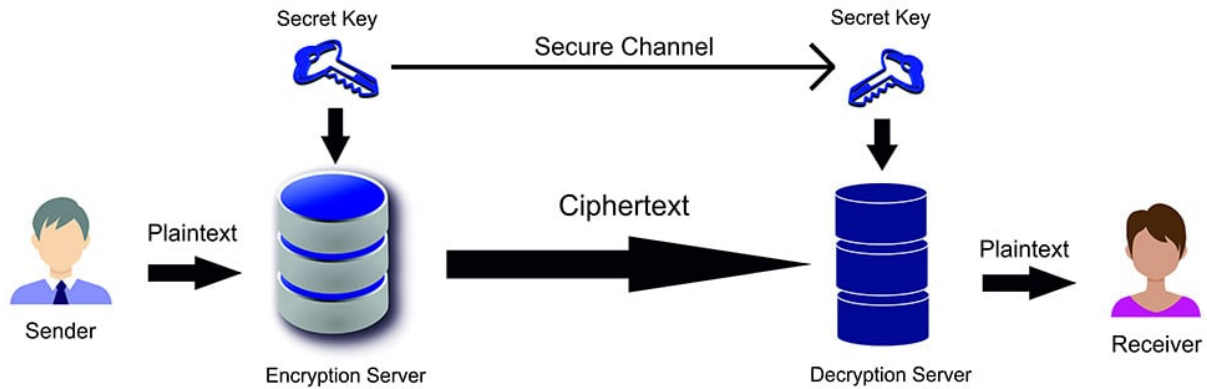
Figure 3 History of Cryptography

- Ancient Cryptography: The Beginnings
 - 2000 BCE(Egypt): Ancient Egypt is where cryptography was first used, when hieroglyphs were purposefully changed in inscriptions to make them less clear.
 - 500 BCE(Scytale): The Spartans employed a device known as the scytale, which was a wooden rod coiled with a piece of parchment. It was only readable when wrapped around a rod with the same diameter as the messages inscribed on it.
 - Caesar Cipher(100 BCE): One of the most basic and well-known cyphers, which involves shifting each letter in a message by a predetermined number of positions in the alphabet, is attributed to Julius Caesar. For instance, changing "A" by three turns it into "D."
- Middle Ages: Religious and Military Codes
 - Vigenere Cipher(16th Century): This cypher, which was created by Giovan Battista Bellaso and made popular by Blaise de Vigenère, encrypted messages using a repeating key, which made it far more difficult to crack than monoalphabetic cyphers.
 - Arab Cryptography(9th Century): The first scientific method of cryptanalysis was developed by the Arab mathematician Al-Kindi, who developed the idea of frequency analysis to crack cyphers.
- Renaissance to Early Modern Period
 - Substitution and Transposition Ciphers: During the Renaissance, methods advanced, combining transposition (rearranging letters) and substitution (replacing letters).

- Advancements in Cryptanalysis: To crack enemy codes, governments and armed forces started hiring specialised cryptographers.
- World Wars and Machine Cryptography
 - World War I (1914-1918): Although manual cypher methods were used, cryptography and cryptanalysis became essential for intelligence as the war went on.
 - World War II (1939-1945): With the invention of machines, cryptography advanced significantly.
- The Computer Era and Modern Cryptography
 - 1940s-1950s: The development of computers transformed cryptography by enabling the creation and deciphering of cyphers at previously unheard-of speeds.
 - Public-key Cryptography (1970s): In 1977, Rivest, Shamir, and Adleman created the RSA algorithm, which established asymmetric cryptography and enabled safe communication without the need for pre-shared keys.
 - Hashing Algorithms (1980s): For data integrity and authenticity, cryptographic hash functions like MD5 and SHA have become indispensable.
- Modern Cryptography: The Digital Age
 - Symmetric Algorithms: The industry standard for safe data encryption is algorithms such as AES (Advanced Encryption Standard).
 - Public-Key Infrastructure (PKI): Used in securing websites, emails, and digital signatures.
 - Blockchain Technology: Introduced digital signatures and hashing, two cryptographic ideas that underpin cryptocurrencies like Bitcoin.
 - Quantum Cryptography: Uses quantum mechanical concepts to protect data, posing a challenge to established encryption methods while also offering previously unheard-of security.

1.4 The symmetric ciphers and The Asymmetric ciphers

The Symmetric Ciphers: Symmetric cyphers encrypt and decrypt data using the same key. For secure communication, the sender and the recipient must share the same key.



Symmetric Cryptography

Figure 4 Symmetric Cipher

Example of Symmetric Algorithms:

- ☐ AES (Advanced Encryption Standard): Widely used, highly secure.
- ☐ DES (Data Encryption Standard): Older algorithm, now considered insecure.
- ☐ 3DES: An enhancement of DES with triple encryption for added security.
- ☐ Blowfish and Twofish: Fast and secure ciphers, often used in embedded systems

How Symmetric Ciphers Work:

- A sender creates ciphertext by encrypting plaintext using a shared secret key.
- To obtain the plaintext, the recipient uses the same key to decrypt the ciphertext.

Example:

- Plaintext: HELLO
- Key: 12345
- Encrypted: 9KF8X
- Decryption uses the same key to revert to HELLO.

The Asymmetric Ciphers: Two keys are used in asymmetric cyphers: a private key for decryption and a public key for encryption. While the private key is kept confidential, the public key is freely exchanged.

Asymmetric Encryption

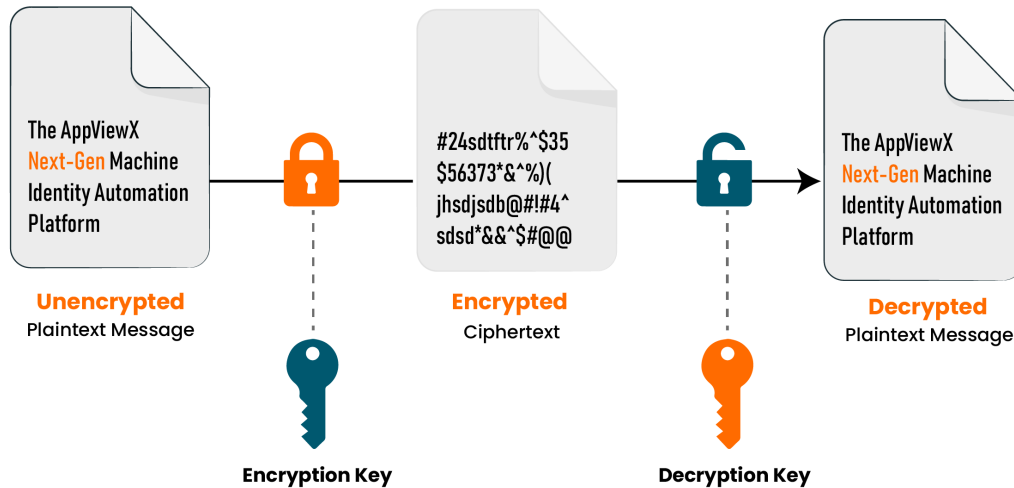


Figure 5 Asymmetric Ciphers

Examples of Asymmetric Algorithms:

- ☐ RSA (Rivest–Shamir–Adleman): One of the first widely used public-key cryptosystems.
- ☐ Elliptic Curve Cryptography (ECC): Provides similar security to RSA but with smaller keys, making it faster and more efficient.
- ☐ Diffie-Hellman: Used for secure key exchange.
- ☐ DSA (Digital Signature Algorithm): Used for digital signatures.

How Asymmetric Ciphers work:

- The public key of the recipient is used by the sender to encrypt a message
- The communication can only be decrypted by the recipient who has the private key.

Example:

- Public Key: Shared openly.
- Private Key: Kept secret by the recipient.
- Encrypted: Only the recipient's private key can decrypt the message.

2. Task 2:

2.1 Caesar Cipher

Introduction

The Caesar cipher, named after Julius Caesar, is one of the earliest and simplest methods of encryption. It is a substitution cipher that shifts each letter in the plaintext by a fixed number of positions in the alphabet. While it is not secure by modern standards, it holds historical significance as one of the foundational techniques in cryptography.

Key Features of the Caesar Cipher:

- **Simplicity:** Caesar Cipher is easy to learn and understand and it is good choice for educational purpose.
- **Historical use:** Julius Caesar used this cipher to communicate with his generals during military campaigns.
- **Substitution-Based:** Each letter in the plaintext is replaced with another letter that is a fixed number of positions away.
- **Key:** The Key in the Caesar cipher is the number of positions by which letters are shifted. For example, with a key of 2, 'E' becomes 'G', 'T' becomes 'V', and so on.

How Caesar Cipher Works:

Encryption: Each letter in the plaintext is shifted forward in the alphabet by the key value. For example, with a key of 3:

Plaintext: NISHANT

Ciphertext: QLVKDQW

Decryption: The ciphertext changes back to the plaintext using the same key value.

2.2 Example of Encryption and Decryption

The example of encrypting and decryption a message using in the Caesar cipher are scenario of key shift 3 and plaintext message is “WELCOME TO BOUDHA”to encrypt the plaintext message in shift each letter forward in the alphabet by using 3 positions and wrap around the shift goes past Z and non-alphabet characters are like spaces to remain unchanged for e.g,

Plaintext	Ciphertext
W	Z
E	H
L	O
C	F
O	R
M	P
E	H
SPACE	SPACE
T	W

O	R
SPACE	SPACE
B	E
O	R
U	X
D	G
H	K
A	D

Ciphertext message: ZHOFRPH WR ERXGKD

To Decrypt the ciphertext message in shift each letter to backward in the alphabet by 3 positions and wrap around If the shift goes before the A. Non-alphabet characters remains too unchanged.

Ciphertext	Plaintext
Z	W
H	E
O	L
F	C
R	O
P	M
H	E
SPACE	SPACE
W	T
R	O
SPACE	SPACE
E	B
R	O
X	U
G	D
K	H
D	A

Decrypted message: WELCOME TO BOUDHA

2.3 Advantage and Disadvantages

Advantages of Caesar Cipher:

1. **Simplicity:** The Caesar cipher is straightforward and easy to understand. Its encryption and decryption processes require minimal effort, making it an excellent introduction to cryptography.
2. **Speed:** Due to its simplicity, the Caesar cipher is computationally fast and can be easily implemented in software or manually on paper.
3. **Historical Importance:** It introduced the fundamental concept of encryption, marking the beginning of cryptography. It's a cornerstone in the history of secure communication.
4. **No Need for Complex Resources:** The cipher doesn't require advanced tools or algorithms, making it usable in low-resource environments.

5. Good for Learning: It's commonly used to teach the basics of cryptographic principles and substitution ciphers.

Disadvantages of Caesar Cipher:

1. Weak Security: The Caesar cipher is highly vulnerable to brute force attacks, as there are only 25 possible shifts (for English alphabets). An attacker can try all shifts to decrypt the message.
2. Frequency Analysis Vulnerability: Since the cipher preserves letter frequencies, analyzing the most common letters in the ciphertext (like 'E' or 'T' in English) can help attackers deduce the key and decrypt the message.
3. Limited Keyspace: The small number of possible keys makes it impractical for modern encryption needs. More sophisticated algorithms have replaced it.
4. No Protection Against Known-Plaintext Attacks: If an attacker has a piece of both the plaintext and the corresponding ciphertext, it's trivial to deduce the shift and decrypt the entire message.
5. Not Suitable for Modern Cryptography: The Caesar cipher is outdated and cannot withstand modern cryptographic analysis or attacks, making it unsuitable for secure communications.

3 Task 3

3.1 Mathematical and Logical

Improving this security of the Caesar Cipher has been mentioned earlier and it is in fact very necessary to improve because of how much insecure it is. The few modifications and enhancement that can be made to make them stronger as follows. These modifications can be divided into mathematical and logical enhancements.

Mathematical Modifications are increasing the key space which is currently limitations, and this technique has 25 possible employed key shift which makes it drastically easy to crack through brute attacks. Modifications are the use of a large set of characters such as numbers, symbols, or even the Unicode characters slow down the rate of getting through the key space. Through attacking independent keys, the key space expands dynamically. Key and modular arithmetic are $C = (P + K) \bmod n$ and $C = (P + K) \bmod n$, where K depends on each character in accordance with a given sequence. Affine cipher: Replace the simple shift operation with an affine transformation: $C = (aP + b) \bmod n$. a : Multiplicative key ((to be coprime with n)). b : Additive key. This greatly increases the overall number of input key numbers and destroys linearities in the obtained combination.

Logical Modifications combine the Caesar ciphers where at the least one of the letters in the corresponding position must apply a different shift. For e.g. The second type of encryption algorithm one should implement is the cipher that dynamically determines shifts based on a keyword "KEY" and plaintext "PREETI" and ciphertext. Every letter displaced depends on the relative letter of the keyword. A Caesar cipher is to be implemented in connection with a transposition cipher. For e.g. encrypt the text first with the Caesar cipher and second permute letters according to one rule or another. Cipher Block Chaining (CBC). Encrypt block 1 with key K for block 2 the output of the first block used as the key randomized shift is the

instead of the using a shift value of a number between 0-25 for each character and different random use to shift values for each character. Encryption layer is the shift by 3, 5, 7 this is the implement the Caesar cipher for multiple rounds employing a different key value for each round the multi-round encryption.

Implementation example Affine cipher is key $a=5$, $b=3$ and plaintext is PREETI ($P=15$, $R=17$, $E=4$, $E=4$, $T=19$, $I=8$)

Encrypt

$$C=(5P+3) \bmod 26$$

$$A \ C=(5*0+3) \bmod 26$$

3.2 Introduction of Mathematical and Logical Operations

In term of improving the Caesar Cipher through mathematical and logical changes, it is possible to specify several addition operations and notions. The following is an explanation of the new mathematical and logical operation to add on the improved version of the Caesar Cipher. It is math that works like a circle and when a number has reached a certain value or modulus, it rolls over to the beginning on the circle. Another reason that it is used in many cryptographic algorithms is that it makes sure that operations are within a certain size, such as the size of the alphabet that is used. Mathematical Operation: $(a + b) \bmod n$ $(a+b) \bmod n$ where: a a and b b are numbers. n n is the modulus. Use in Caesar Cipher: The shift operation in the Caesar Cipher is realised through modular arithmetic, that implies the alphabet forms a cyclic group (and moreover, the final letter in the alphabet 'Z' is immediately followed by the first letter of the alphabet 'A'). instance, when applying the Caesar Cipher with a shift of three, the position of a letter in the alphabet ascends by three; if the shift crosses 'Z,' the shift begins over at the same position as 'A'. To find the position of 'B' the value of $(24+3) \bmod 26 = 27 \bmod 26 = 1$ a Caesar Cipher with a shift of 3, the position of a letter in the alphabet is incremented by 3, and if the shift surpasses 'Z', If the alphabet has 26 letters ($n=26$) and the letter 'Y' (position 24) is shifted by 3 positions: $(24 + 3) \bmod 26 = 27 \bmod 26 = 1$ (position of 'B') $(24+3) \bmod 26=27 \bmod 26=1$ (position of 'B') Thus, 'Y' becomes 'B'. The Affine Cipher is another real advanced version of the Caesar Cipher that utilizes both the addition and multiplication rather than fixed shift cipher. It uses two keys, the multiplication key and the addition key meaning that the mappings employ more steps than the simple ones. Mathematical Operation: $C = (aP + b) \bmod n$ $C=(aP+b) \bmod n$ where: C C is the ciphertext. P P is the plaintext. a a is the multiplicative key (a and m are, in fact, coprime). n n is the size of the alphabet, which is 26 for English alphabet.

3.3 New Encryption and Decryption Cryptographic

Apply new encryption and decryption algorithm to the plaintext message RAM using the key here convert plaintext numbers R=17, A=0, M=12 the plaintext RAM Become (17,0,12).

Convert the key to numbers K=10, E=4, Y=24

The key becomes (10,4,24). First letter R= 17 key is k shift 10 shift $17+10=27$, mode 26=1 “B” second letter A=0 key is E shift 4 shift $0+4=4$ “E” Third letter M= 12 Key is Y shift 24 shift $12+24=36$, 36 mode 26= 10 “K”

The cipher become “BEK”.

Decryption process in ciphertext BEK and key KEY convert ciphertext to number, B= 1, E= 4, K= 10 The ciphertext BEK become (1,4,10). Convert the key to numbers. K=10, E=4, Y=24 reverse the shift based on the key B= 1 key is K shift 10 and reverse shift $1-10=-9$, $-9 \bmod 26=17$ R, E= 4 key is E shift 4 reverse shift $4-4=0$ A, K=10 key is Y shift 24 reverse shift $10-24=-14$, $-14 \bmod 26=12$ M,

The plaintext become “RAM”

Plaintext: RAM, Key: KEY, Ciphertext: BEK and Decrypted Text: RAM.

3.4 Name your new Cryptographic Algorithm

I name my new cryptographic Algorithm as “Combined Cipher”

Newly created cryptographic algorithm

3.5 Why was the modification necessary?

Modifications to the Caesar Cipher were necessary because its original form is highly insecure and unsuitable for modern cryptographic needs. It will help to secure from attackers because it is not a simple cipher that is Caesar Cipher. Pattern Recognition in long messages employing a static shift, the same pattern is repeated in the ciphertext which makes it vulnerable to being attacked by frequency analysis.

3.6 New Methodology Implied

In Caesar Cipher, we change the plaintext letter into ciphertext by the help of key value. In this new cipher we will first change the plaintext into the numeric value and then the word “KEY” into a numeric value and then add the plaintext numeric value and numeric value generated from word KEY and make a new text that will be ciphertext and to decrypt the text we will do the vise-versa.

3.7 New Encryption Algorithm

Step 1- Input the plain text

Step 2- convert the text into numeric value

Step 3- Covert the work “KEY” from Caesar cipher into numeric value

Step 4- add the text numeric value and the numeric value generated from word “KEY”

Step 5- Then use the numbers to create a new text

Step 6- Then the text will be encrypted

3.8 New Decryption Algorithm

Step 1- Input the Encrypted text

Step 2- Convert the text into numeric value

Step 3- Convert the word "KEY" from Caesar cipher into numeric value

Step 4- Subtract the numeric value generated from word "KEY" from the text numeric value

Step 5- Then use the numbers to create a text

Step 6- Then the text will again be decrypted

4 Testing

Using the new modified Cryptographic Algorithm named "Combined Cipher" to encrypt and decrypt five text.

Text 1: IOS

Text 2: MAC

Text 3: CAT

Text 4: DOG

Text 5: SAD

Text 1: IOS

Encryption process

Converting plaintext number I=8, O=14, S=18 the plain text IOS becomes (8,14,18). Convert the key to numbers K=10, E=4, Y=24

The key becomes (10,4,24). First letter I= 8 key is k shift 10 shift $8+10=18$ "S" second letter O=14 key is E shift 4 shift $14+4=18$ "S" Third letter S= 18 Key is Y shift 24 shift $18+24=42$, $42 \text{ mode } 26=16$ "Q"

The cipher text becomes "SSQ"

Encryption Process for "IOS" with Key "KEY" in Binary:

Step 1: Convert Plaintext and Key to Numbers

- Plaintext: I = 8, O = 14, S = 18
- Key: K = 10, E = 4, Y = 24

Step 2: Convert Numbers to 5-bit Binary

We'll convert the numerical values of the plaintext and key into binary, using 5-bit binary representation.

- Plaintext to Binary:
 - I = 8 \rightarrow 01000
 - O = 14 \rightarrow 01110
 - S = 18 \rightarrow 10010
- Key to Binary:
 - K = 10 \rightarrow 01010
 - E = 4 \rightarrow 00100
 - Y = 24 \rightarrow 11000

Step 3: Apply the Key and Perform Shift (Addition)

Next, we perform the addition of the corresponding binary values from the plaintext and key:

1. First letter (I = 8):

- Key: $K = 10 \rightarrow 01010$
- Shift: $01000 (I) + 01010 (K) = 10010$ (18 in decimal \rightarrow "S").
- 2. Second letter (O = 14):
 - Key: $E = 4 \rightarrow 00100$
 - Shift: $01110 (O) + 00100 (E) = 10010$ (18 in decimal \rightarrow "S").
- 3. Third letter (S = 18):
 - Key: $Y = 24 \rightarrow 11000$
 - Shift: $10010 (S) + 11000 (Y) = 101010$ (42 in decimal, and $42 \bmod 26 = 16 \rightarrow$ "Q").

Decryption process

Converting ciphertext SSQ and key KEY to number, S= 18, S= 18, Q= 16 The ciphertext SSQ become (18,18,16). Convert the key to numbers. K=10, E=4, Y=24 reverse the shift based on the key S= 18 key is K shift 10 and reverse shift $18-10= 8$ I, S= 18 key is E shift 4 reverse shift $18-4=14$ O, Q=16 key is Y shift 24 reverse shift $16-24= -8$, $-8 \bmod 26= 18$ S

The plain text becomes IOS

Decryption Process for "SSQ" with Key "KEY" in Binary:

Step 1: Convert Ciphertext and Key to Numbers

- Ciphertext: S = 18, S = 18, Q = 16
- Key: K = 10, E = 4, Y = 24

Step 2: Convert Numbers to 5-bit Binary

We'll convert the numerical values of the ciphertext and the key into 5-bit binary representation.

- Ciphertext to Binary:
 - S = 18 $\rightarrow 10010$
 - S = 18 $\rightarrow 10010$
 - Q = 16 $\rightarrow 10000$
- Key to Binary:
 - K = 10 $\rightarrow 01010$
 - E = 4 $\rightarrow 00100$
 - Y = 24 $\rightarrow 11000$

Step 3: Reverse the Shift and Subtract Key (Decryption)

We reverse the encryption by subtracting the key values from the ciphertext values:

1. First letter (S = 18):
 - Key: $K = 10 \rightarrow 01010$
 - Reverse shift: $10010 (S) - 01010 (K) = 01000$ (8 in decimal \rightarrow "I").
2. Second letter (S = 18):
 - Key: $E = 4 \rightarrow 00100$
 - Reverse shift: $10010 (S) - 00100 (E) = 01110$ (14 in decimal \rightarrow "O").
3. Third letter (Q = 16):
 - Key: $Y = 24 \rightarrow 11000$
 - Reverse shift: $10000 (Q) - 11000 (Y) = -01000$ (-8 in decimal, and $-8 \bmod 26 = 18 \rightarrow$ "S").

Text 2: MAC

Encryption process

Converting plaintext number $M=12$, $A=0$, $C=2$ the plain text MAC becomes $(12,0,2)$. Convert the key to numbers $K=10$, $E=4$, $Y=24$

The key becomes $(10,4,24)$. First letter $M=12$ key is K shift 10 shift $12+10=22$ "W" second letter $A=0$ key is E shift 4 shift $0+4=4$ "E" Third letter $C=2$ Key is Y shift 24 shift $2+24=26$, $26 \text{ mode } 26 = 0$ "A"

The cipher text becomes "WEA"

Encryption Process for "MAC" with Key "KEY" in Binary:

Step 1: Convert Plaintext and Key to Numbers

- Plaintext: $M = 12$, $A = 0$, $C = 2$
- Key: $K = 10$, $E = 4$, $Y = 24$

Step 2: Convert Numbers to 5-bit Binary

We will convert the numerical values of both the plaintext and the key to 5-bit binary.

- Plaintext to Binary:
 - $M = 12 \rightarrow 01100$
 - $A = 0 \rightarrow 00000$
 - $C = 2 \rightarrow 00010$
- Key to Binary:
 - $K = 10 \rightarrow 01010$
 - $E = 4 \rightarrow 00100$
 - $Y = 24 \rightarrow 11000$

Step 3: Apply the Key and Perform Shift (Addition)

We will add the key's binary value to the corresponding plaintext binary value:

1. First letter ($M = 12$):
 - Key: $K = 10 \rightarrow 01010$
 - Shift: $01100 (M) + 01010 (K) = 10110$ (22 in decimal \rightarrow "W").
2. Second letter ($A = 0$):
 - Key: $E = 4 \rightarrow 00100$
 - Shift: $00000 (A) + 00100 (E) = 00100$ (4 in decimal \rightarrow "E").
3. Third letter ($C = 2$):
 - Key: $Y = 24 \rightarrow 11000$
 - Shift: $00010 (C) + 11000 (Y) = 11010$ (26 in decimal, and $26 \bmod 26 = 0 \rightarrow$ "A").

Decryption process

Converting ciphertext WEA and key KEY to number, $W=22$, $E=4$, $A=0$ The ciphertext WEA become $(22,4,0)$. Convert the key to numbers. $K=10$, $E=4$, $Y=24$ reverse the shift based on the key $W=22$ key is K shift 10 and reverse shift $22-10=12$ M , $E=4$ key is E shift 4 reverse shift $4-4=0$ A , $A=0$ key is Y shift 24 reverse shift $0-24=-24$, $-24 \bmod 26 = 2$ C

The plain text becomes MAC

Convert Ciphertext and Key to Numbers:

- Ciphertext: $W = 22$, $E = 4$, $A = 0$.

- Key: $K = 10$, $E = 4$, $Y = 24$.

Binary Representation (5-bit binary):

- $W = 22 \rightarrow 10110$, $E = 4 \rightarrow 00100$, $A = 0 \rightarrow 00000$.
- $K = 10 \rightarrow 01010$, $E = 4 \rightarrow 00100$, $Y = 24 \rightarrow 11000$.

Reverse the Shift (Binary Subtraction Modulo 26):

- Subtract the key number from the ciphertext number, then take mod 26 to get the result within the alphabet range.

Steps:

- First letter: $W (22) - K (10) \rightarrow \text{Binary: } 10110 - 01010 = 01100 (12) \rightarrow M$.
- Second letter: $E (4) - E (4) \rightarrow \text{Binary: } 00100 - 00100 = 00000 (0) \rightarrow A$.
- Third letter: $A (0) - Y (24) \rightarrow \text{Binary: } 00000 - 11000 = -11000 (-24 \bmod 26 = 2) \rightarrow C$.

Text 3: CAT

Encryption process

Converting plaintext number $C=2$, $A=0$, $T=19$ the plain text CAT becomes (2,0,19). Convert the key to numbers $K=10$, $E=4$, $Y=24$

The key becomes (10,4,24). First letter $C=2$ key is K shift 10 shift $2+10=12$ "M" second letter $A=0$ key is E shift 4 shift $0+4=4$ "E" Third letter $T=19$ Key is Y shift 24 shift $19+24=43$, $43 \bmod 26 = 17$ "R"

The cipher text becomes "MER"

Convert Characters to Binary: Each character is first converted into its numerical value ($A=0$, $B=1$, ..., $Z=25$), and then into its binary equivalent.

Example:

- Plaintext: $C = 2$, $A = 0$, $T = 19$.
- Key: $K = 10$, $E = 4$, $Y = 24$.

Binary Encryption Using Addition: Perform bitwise addition (mod 26 if required) in binary format:

- First letter: $C (2) + K (10) \rightarrow \text{Binary: } 00010 + 01010 = 01100 (12) \rightarrow M$.
- Second letter: $A (0) + E (4) \rightarrow \text{Binary: } 00000 + 00100 = 00100 (4) \rightarrow E$.
- Third letter: $T (19) + Y (24) \rightarrow \text{Binary: } 10011 + 11000 = 101011 (43 \bmod 26 = 17) \rightarrow R$.

Decryption process

Converting ciphertext MER and key KEY to number, $M=12$, $E=4$, $R=17$ The ciphertext MER become (12,4,17). Convert the key to numbers. $K=10$, $E=4$, $Y=24$ reverse the shift based on the key $M=12$ key is K shift 10 and reverse shift $12-10=2$ C, $E=4$ key is E shift 4 reverse shift $4-4=0$ A, $R=17$ key is Y shift 24 reverse shift $17-24=-7$, $-7 \bmod 26 = 19$ T

The plain text becomes CAT

Convert Ciphertext and Key to Binary:

- Ciphertext: $M = 12$, $E = 4$, $R = 17 \rightarrow \text{Binary: } 01100, 00100, 10001$.
- Key: $K = 10$, $E = 4$, $Y = 24 \rightarrow \text{Binary: } 01010, 00100, 11000$.

Reverse the Shift (Binary Subtraction):

- Perform binary subtraction and apply mod 26 if the result is negative:
 - First letter: $M (12) - K (10) \rightarrow \text{Binary: } 01100 - 01010 = 00010 (2) \rightarrow C$.

- Second letter: E (4) - E (4) → Binary: 00100 - 00100 = 00000 (0) → A.
- Third letter: R (17) - Y (24) → Binary: 10001 - 11000 = -000111 (-7 mod 26 = 19) → T.

Text 4: DOG

Encryption process

Converting plaintext number D=3, O=14, G=6 the plain text DOG becomes (3,14,6). Convert the key to numbers K=10, E=4, Y=24

The key becomes (10,4,24). First letter D= 3 key is k shift 10 shift 3+10=13 “N” second letter O=14 key is E shift 4 shift 14+4 =18 “S” Third letter G= 6 Key is Y shift 24 shift 6+24=30, 30 mode 26= 4 “E”

The cipher text becomes “NSE”

Convert Plaintext and Key to Numbers:

- Plaintext: D = 3, O = 14, G = 6.
- Key: K = 10, E = 4, Y = 24.

Binary Representation (5-bit binary):

- D = 3 → 00011, O = 14 → 01110, G = 6 → 00110.
- K = 10 → 01010, E = 4 → 00100, Y = 24 → 11000.

Perform Encryption (Binary Addition Modulo 26):

- Add the plaintext number to the key number, then take mod 26 to keep the result within the alphabet range.

Steps:

- First letter: D (3) + K (10) → Binary: 00011 + 01010 = 01101 (13) → N.
- Second letter: O (14) + E (4) → Binary: 01110 + 00100 = 10010 (18) → S.
- Third letter: G (6) + Y (24) → Binary: 00110 + 11000 = 11110 (30 mod 26 = 4) → E.

Decryption process

Converting ciphertext SSQ and key KEY to number, N= 13, S= 18, E= 4 The ciphertext NSE become (13,18,4). Convert the key to numbers. K=10, E=4, Y=24 reverse the shift based on the key N= 13 key is K shift 10 and reverse shift 13-10= 3 D, S= 18 key is E shift 4 reverse shift 18-4=14 O, E=4 key is Y shift 24 reverse shift 4-24= -20, -20 mod 26= 6 G

The plain text becomes DOG

Convert Ciphertext and Key to Numbers:

- Ciphertext: N = 13, S = 18, E = 4.
- Key: K = 10, E = 4, Y = 24.

Binary Representation (5-bit binary):

- N = 13 → 01101, S = 18 → 10010, E = 4 → 00100.
- K = 10 → 01010, E = 4 → 00100, Y = 24 → 11000.

Reverse the Shift (Binary Subtraction Modulo 26):

- Subtract the key number from the ciphertext number, then take mod 26 to keep the result within the alphabet range.

Steps:

- First letter: N (13) - K (10) → Binary: 01101 - 01010 = 00011 (3) → D.
- Second letter: S (18) - E (4) → Binary: 10010 - 00100 = 01110 (14) → O.

- Third letter: E (4) - Y (24) \rightarrow Binary: 00100 - 11000 = -10100 (-20 mod 26 = 6) \rightarrow G.

Text 5: SAD

Encryption process

Converting plaintext number S=18, A=0, D=3 the plain text IOS becomes (18,0,3). Convert the key to numbers K=10, E=4, Y=24

The key becomes (10,4,24). First letter S= 18 key is k shift 10 shift 18+10=28, 28 mode 26 = 2 “C” second letter A=0 key is E shift 4 shift 0+4 =4 “E” Third letter D= 3 Key is Y shift 24 shift 3+24=27, 27 mode 26= 1 “B”

The cipher text becomes “CEB”

Convert Plaintext and Key to Numbers:

- Plaintext: S = 18, A = 0, D = 3.
- Key: K = 10, E = 4, Y = 24.

Binary Representation (5-bit binary):

- S = 18 \rightarrow 10010, A = 0 \rightarrow 00000, D = 3 \rightarrow 00011.
- K = 10 \rightarrow 01010, E = 4 \rightarrow 00100, Y = 24 \rightarrow 11000.

Perform Encryption (Binary Addition Modulo 26):

- Add the plaintext number to the key number, then take mod 26 to keep the result within the alphabet range.

Steps:

- First letter: S (18) + K (10) \rightarrow Binary: 10010 + 01010 = 11100 (28 mod 26 = 2) \rightarrow C.
- Second letter: A (0) + E (4) \rightarrow Binary: 00000 + 00100 = 00100 (4) \rightarrow E.
- Third letter: D (3) + Y (24) \rightarrow Binary: 00011 + 11000 = 11011 (27 mod 26 = 1) \rightarrow B.

Decryption process

Converting ciphertext CEB and key KEY to number, C= 2, E= 4, B= 1 The ciphertext CEB become (2,4,1). Convert the key to numbers. K=10, E=4, Y=24 reverse the shift based on the key C= 2 key is K shift 10 and reverse shift 2-10= -8,-8 mode 26= 18 S, E= 4 key is E shift 4 reverse shift 4-4=0 A, B=1 key is Y shift 24 reverse shift 1-24= -23, -23 mod 26= 3 D

The plain text becomes SAD

Convert Ciphertext and Key to Numbers:

- Ciphertext: C = 2, E = 4, B = 1.
- Key: K = 10, E = 4, Y = 24.

Binary Representation (5-bit binary):

- C = 2 \rightarrow 00010, E = 4 \rightarrow 00100, B = 1 \rightarrow 00001.
- K = 10 \rightarrow 01010, E = 4 \rightarrow 00100, Y = 24 \rightarrow 11000.

Reverse the Shift (Binary Subtraction Modulo 26):

- Subtract the key number from the ciphertext number, then take mod 26 to keep the result within the alphabet range.

Steps:

- First letter: C (2) - K (10) \rightarrow Binary: 00010 - 01010 = -01000 (-8 mod 26 = 18) \rightarrow S.
- Second letter: E (4) - E (4) \rightarrow Binary: 00100 - 00100 = 00000 (0) \rightarrow A.
- Third letter: B (1) - Y (24) \rightarrow Binary: 00001 - 11000 = -10111 (-23 mod 26 = 3) \rightarrow D.

Task 5

5.1 Strengths of the Combined Cipher

- **Simplicity:** It is easy to comprehend, integrate and compute the algorithm of this type, which is relevant for educational and light-weight cryptographic applications
- **Key Dependency:** Encryption solely depends on the key depending on the parameters given. The use of different keys provides for completely different ciphers so that the encryption is not a constant thing.
- **Reversibility:** It help in decrypting the text into normal plaintext.
- **Modular Arithmetic:** By taking modulo of the shifted values the above operation wraps within the alphabet space. This prevents occurrences of what is actually a number being counted as a letter reducing any possibility of an error to deliver only valid results full of pure alphabet.
- **Lightweight and Fast:** This algorithm is computationally efficient and does not consume much computing power; it is good for resource poor environments or can be useful for safe but not very secure information processing.

5.2 Weakness of the Combined Cipher

- **Vulnerability to Known-Plaintext Attacks:** If an attacker has access to both the plaintext and the ciphertext for even a short message, they can easily determine the key by comparing the numerical shifts for each letter.
- **Dependency on key security:** The algorithm's security heavily depends on the secrecy of the key. If the key is short or predictable (e.g., "KEY"), it can be guessed or brute-forced. If the key is exposed, all encrypted messages using that key become vulnerable.
- **Limited keyspace:** The keyspace is limited to 26 possibilities per key character for alphabets, making it weaker compared to modern encryption algorithms like AES that use keys of 128, 192, or 256 bits.
- **Key Repetition weakness:** If the key is shorter than the plaintext, it repeats itself (as in the Vigenère cipher). Repeated patterns in the key can make it vulnerable to cryptanalysis methods like the Kasiski examination or Vigenère key attack, especially for long ciphertexts.
- **No protection against ciphertext manipulation:** An attacker could modify parts of the ciphertext, and the decryption process would not detect tampering. For instance, changing a letter in the ciphertext alters the corresponding plaintext without leaving evidence.

Conclusion

The Combined Cipher, derived from the Caesar cipher and incorporating modular arithmetic with dynamic keys, offers a simple and effective means of encryption for low-security purposes. It addresses some of the vulnerabilities of the basic Caesar cipher by introducing key-based letter

shifts, ensuring that each character in the plaintext is encrypted uniquely based on its corresponding key character.

However, despite its strengths, the algorithm remains unsuitable for modern cryptographic applications due to its inherent weaknesses, such as susceptibility to frequency analysis, brute force, and pattern recognition. The reliance on short keys, lack of diffusion, and absence of integrity checks make it vulnerable to cryptanalysis and ciphertext manipulation.

In conclusion, Combined Cipher provides an accessible, lightweight cryptographic tool, but for modern and secure applications, further development and integration with robust encryption techniques are necessary. It serves as an excellent starting point for understanding cryptography while highlighting the importance of evolving algorithms to meet contemporary security needs.