iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: XI Month of publication: November 2021

DOI: https://doi.org/10.22214/ijraset.2021.38732

# Different Methods of Encryption and Decryption

Pratiksha Satapure[1], Divya Sawant[2], Rutuja Tallapalli[3], Ruchi Thakkar[4], Prof. Sujata Bhamare[5]
[1, 2, 3, 4]*Computer Engineering, Pimpri Chinchwad, College of Engineering*
[5]*Engineering Mathematics, Pimpri Chinchwad, College of Engineering*

***Abstract: Data is any type of stored digital information. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, personal databases and websites. Cryptography is evergreen and developments. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. Compression is the process of reducing the number of bits or bytes needed to represent a given set of data. It allows saving more data. Cryptography is a popular ways of sending vital information in a secret way. There are many cryptographic techniques available and among them AES is one of the most powerful techniques. The scenario of present day of information security system includes confidentiality, authenticity, integrity, nonrepudiation. The security of communication is a crucial issue on World Wide Web. It is about confidentiality, integrity, authentication during access or editing of confidential internal documents.***

***Keywords: Cryptography, Hill Cipher, Homophonic Substitution Cipher, Monoalphabetic Cipher, Ceaser Cipher.***

## I. INTRODUCTION

To secure the data, compression is used because it use less disk space (saves money), more Computer Engineering, data can be transfer via internet. It increase speed of data transfer from disk to memory. Security goals for data security are Confidential, Authentication, Integrity, and Non-repudiation. Data security delivers data protection across enterprise. Information security is a growing issue among IT organizations of all sizes. To tackle this growing concern, more and more IT firms are moving towards cryptography to protect their valuable information. In addition to above concerns over securing stored data, IT organizations are also facing challenges with everincreasing costs of storage required to make sure that there is enough storage capacity to meet the organization’s current and future demands. Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller sized format called code word. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, called plaintext, to another format, called cipher text, using an encryption key. Currently compression and encryption methods are done separately. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.

It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.

## II. CRYPTOGRAPHY

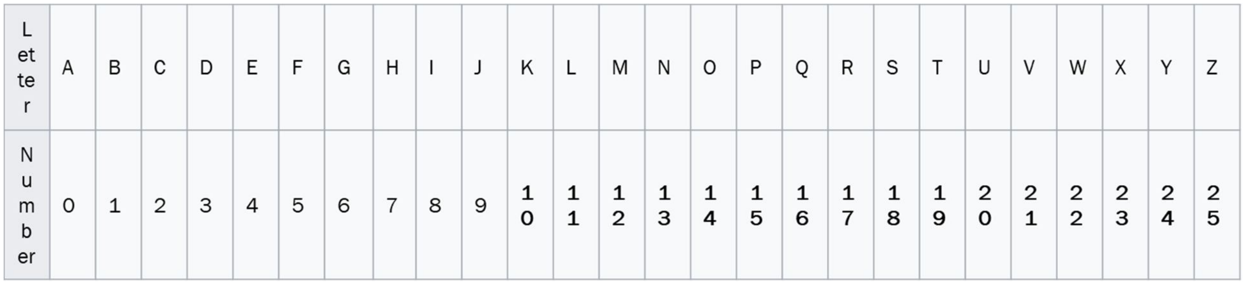
The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.
The information that we need to hide, is called plaintext , It’s the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the sending of a message in the sender before encryption, or it is the text at the receiver after decryption.

Types of Cipher
*1)* Hill Cipher Method
*2)* Homophonic Substitution Cipher
*3)* Monoalphabetic Cipher
*4)* Ceaser Cipher

### *A. Hill Cipher Method*

The Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once.

*1) Encryption:* Each letter is represented by a number modulo 26. Though this is not an essential feature of the cipher, this simple scheme is often used:



| Letter | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Number | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

Consider the message 'ACT’ (n=3) which we need to encrypt and the key (GYBNQKURP in letters):

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to cipher text of 'POH'

2) *Decryption:* To decrypt the message, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters).The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Ciphertext 'POH':

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

**KEYWORD** **POH** **ACT**

which gives us back 'ACT'.

### B. *Homophonic Substitution Cipher*

Homophonic Substitution was an early attempt to make Frequency Analysis a less powerful method of cryptanalysis.

The basic idea behind homophonic substitution is to allocate more than one letter or symbol to the higher frequency letters.

For example, you might use 6 different symbols to represent "e" and "t", 2 symbols for "m" and 1 symbol for "z".

Clearly, this cipher will require an alphabet of more than 26 letters, as each letter needs at least one ciphertext letter, and many need more than this.

The standard way to do this is to include the numbers in the ciphertext alphabet, but you can also use a mixture of uppercase, lowercase and upside down letters.

Some people even design artistic symbols to use.

We need to use a key of some form to order the letters of the ciphertext alphabet, and we shall use a keyword like for the Mixed Alphabet Cipher.

In a similar way, we use the letters from the keyword first, without repeats, then use the rest of the alphabet.

Examples:

1) Using the keyphrase "18 fresh tomatoes and 29 cucumbers“phrase "18 fresh tomatoes and 29 cucumbers" is used with the alpha-numeric alphabet, assigning multiple symbols to the most common letters.

| Plaintext Alphabet | a | | b | c | d | e | | | | f | g | h | i | | j | k | l | m | n | | o | | p | q | r | s | | t | | | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext Alphabet | 1 | 8 | F | R | E | S | H | T | O | M | A | N | D | 2 | 9 | C | U | B | G | I | J | K | L | P | Q | V | W | X | Y | Z | 0 | 3 | 4 | 5 | 6 | 7 |

2) Using the keyphrase "run away, the enemy are coming" We start as if it was a normal Mixed Alphabet Cipher, getting "Q" for "r" and "0" for "u", but then we get to "n" and we could choose either "G" or "I" to represent "n".

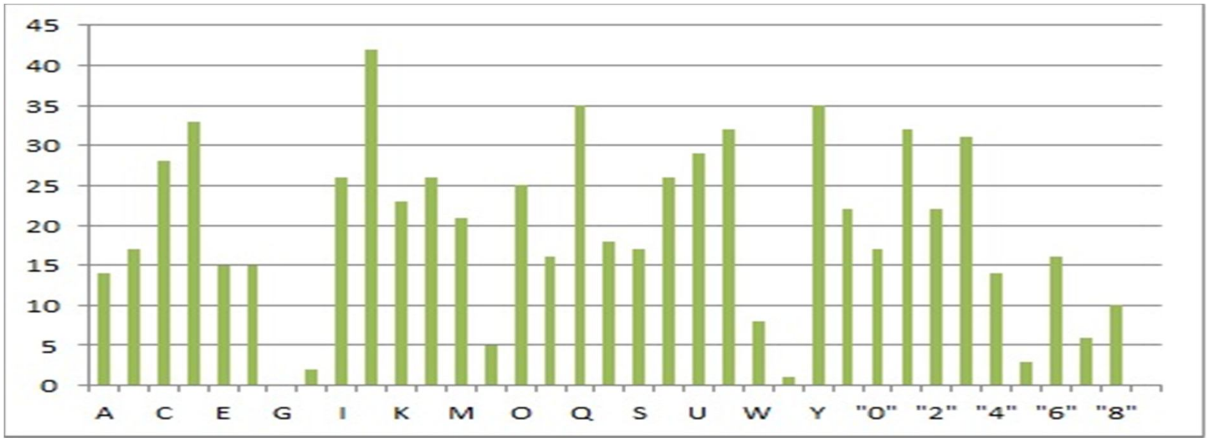
Continuing like this, and choosing randomly which symbol to use we could get the ciphertext "Q0I 1486, YNH OGSB6 1QH RKB2GA".

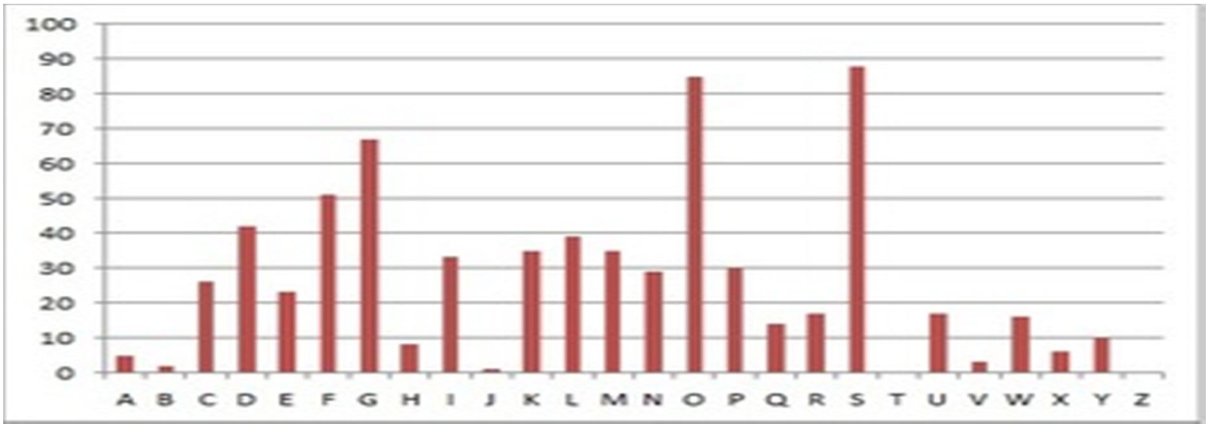
Homophonic Substitution is a simple way to make monoalphabetic substitution more secure, by levelling out the frequencies with which the ciphertext letters appear.

There are many approaches to the homonphonic substitution cipher, and it can be adapted in many ways.

Using the text we decrypted in Frequency Analysis, with the same keyword *manuscript*, we get the frequency distributions below.

We notice much more clumping of the letters in the homophonic example, and also the extra symbols to represent the 26 letters.





The letter frequencies after a Mixed Alphabet Cipher

One special type of homophonic substitution cipher is a *nomenclator*. This combines a codebook with a large homophonic substitution cipher.

Originally used in France, it is named after the people who announced the arrival of dignitaries, and started with a small codebook consisting of the names of dignitaries.

This however expanded rapidly, to include many common words, phrases and places. When written, the code and cipher parts are not distinguished.

Nomenclators were a hugely successful cipher, and many remained unbroken for hundreds of years.

In fact, there are still some articles in achives that have not been broken, and provide interesting insights into historical accounts.

### *C. Monoalphabetic Cipher*

As Caesar cipher and a modified version of Caesar cipher is easy to break, monoalphabetic cipher comes into the picture. In monoalphabetic, each alphabet in plain text can be replaced by any other alphabet except the original alphabet. That is, A can be replaced by any other alphabet from B to Z. B can be replaced by A or C to Z. C can be replaced by A, B, and D to z, etc. Mono alphabetic cipher causes difficulty to crack the message as there are random substitutions and a large number of permutation and combination are available.

Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.The relationship between a character in the plain text and the characters in the cipher text is one-to-one.

Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.

A stream cipher is a monoalphabetic cipher if the value of key does not depend on the position of the plain text character in the plain text stream

It is a simple substitution cipher which is simple to understand and Implement.

We have 26! possible keys. So brute force attack won't work here.

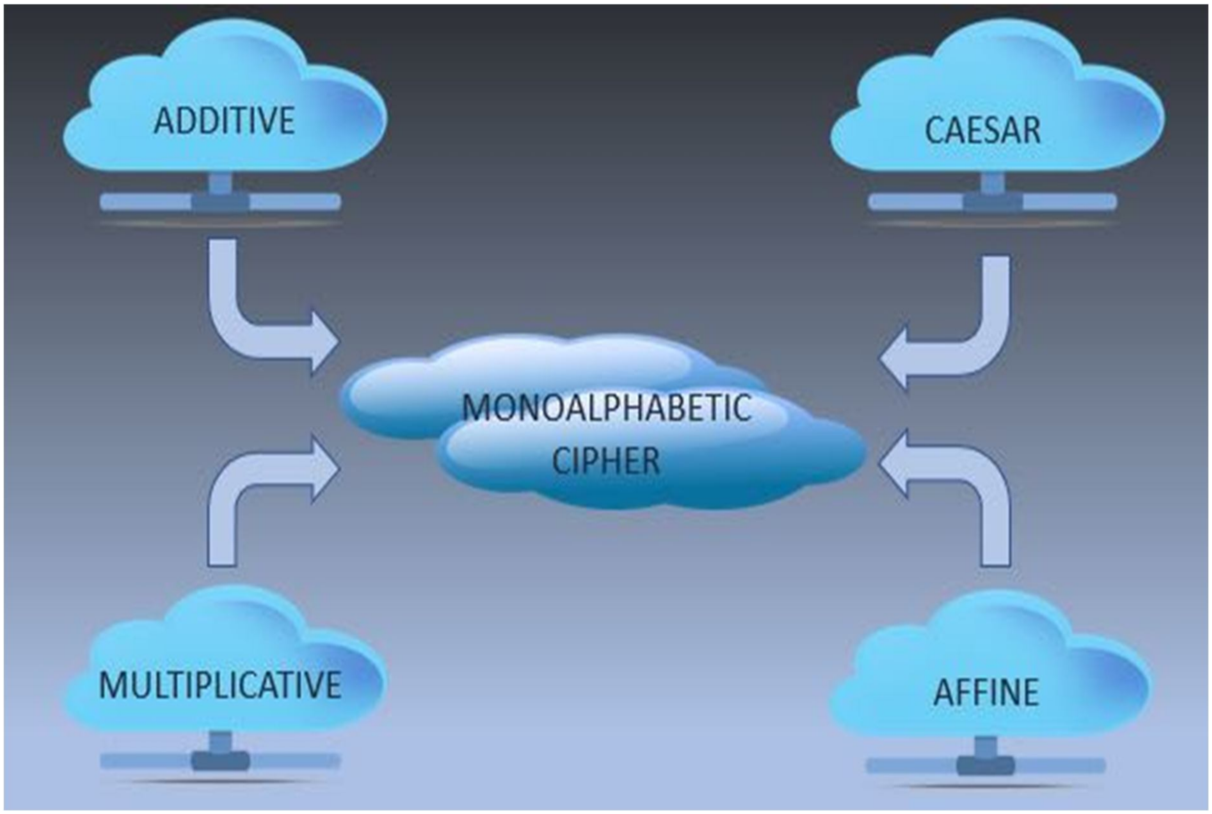
Monoalphabetic Cipher is described as a substitution cipher in which the same fixed mappings from plain text to cipher letters across the entire text are used.

Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.

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

Here, the word HOME is encrypted as CPYM.

Since a key is a generic substitution which can be represented as a permutation of the alphabet, the number of keys is the number of permutations of 26 elements, i.e., 26! which is approximately 4 x $10^{26}$, a number bigger than $2^{88}$ which makes it very heavy to brute force even using powerful parallel computers.



Types of monoalphabetic cipher are

1) *Additive Cipher:* Additive cipher is the type of monoalphabetic substitution cipher, in which the each character of a plain text is mapped by some other character depending upon the value of key.

Example: If the plain text contain alphabet 'B' and the value of key is '4', then the alphabet 'B' will be replaced by the alphabet 'F' i.e the 4th alphabet after 'B' .
Mathematical Representation is
Encryption process :
C=( P + k) mod 26
where, 'P' is the character in plain text, 'K' is the key and 'C' is the required cipher

Decryption process :
P=( C - k) mod 26

2) Ceasar cipher: Caesar cipher is the most simplest form of cipher, it is similar to additive cipher. In caesar cipher the value of key is always '3'.

Mathematical Representation is
Encryption process :
C=(P + K) mod 26
where, 'P' is the character in plain text, 'K' is the key (k=3) and 'C' is the required cipher

Decryption process :
P=( C - k) mod 26

3) *Multiplicative Cipher:* In multiplicative cipher, character of a plain text is multiplied with the key and then modulus function is applied on it. It is a type of monoalphabetic substitution cipher hence it is not a stronger cipher.

Mathematical Representation is
Encryption process :
C=(P * K) mod 26
where, 'P' is the character in plain text, 'K' is the key and 'C' is the required cipher

Decryption process :
P=(9*C) mod 26

4) *Affine cipher:* Affine cipher is the stronger cipher among the additive and multiplicative cipher. Affine cipher consists of two keys as it a combination of additive and multiplicative cipher .

Mathematical Representation is
Encryption process :
C=( P *k1 + k2) mod 26
where, P is the character in plain text, K1 is multiplicative key ,K2 is additive key ,C is the character in cipher.

Decryption process :
P=( (C- k2 ) / k1 ) mod 26

### D. *Ceaser Cipher*

It is type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabets.
In cryptography, a ceaser cipher is also known as ceaser’s cipher, the shift cipher, ceaser’s code or ceaser shift.
It is one of the simplest and most widely known encryption techniques.
For caesar ciphers, the key is the number oc characters to shift the cipher alphabets.

1) *Uses of Ceasar Cipher:* Caesar ciphers can be found today in children's toys such as secret decoder rings. A Caesar shift of thirteen is also performed in the ROT13 algorithm, a simple method of obfuscating text used in some Internet forums to obscure text (such as joke punchlines and story spoilers), but not used as a method of encryption. Julius caesar used an additive cipher to communicate with his officer. For this reason, additive cipher are sometimes called as caesar ciphers.

Examples:

*a)* With left shift of 3 , d would be replaced by a , e would become b, and do on.....

*b)* Attack at dawn" encrypts to "dwwdfn dw gdzq" using the caesar cipher. .

Encryption

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A → 0, B → 1, ..., Z → 25.

Encryption of a letter x by a shift n can be described mathematically as,

Encryption(x)=(x+n)\mod {26}

Decryption

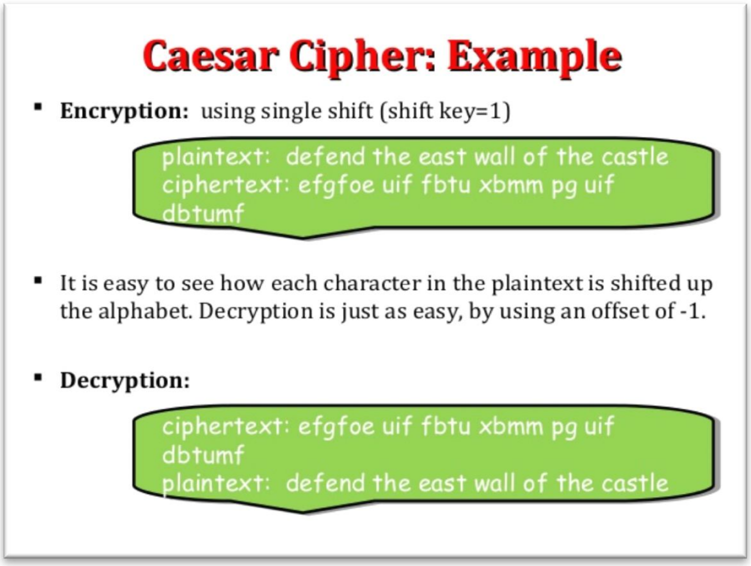
Caesar code decryption replaces a letter another with an inverse alphabet shift: a previous letter in the alphabet.

Example: Decrypt GFRGHA with a shift of 3. To decrypt G, take the alphabet and look 3 letters before: D. So G is decrypted with D. To decrypt X, loop the alphabet: before A: Z, before Z: Y, before Y: X.

Decryption is performed similarly,

Decryption(x)=(x-n)\mod {26}

| | | | | |
|---|---|---|---|---|
| A=0 | G=6 | M=12 | | X=23 |
| B=1 | H=7 | N=13 | S =18 | Y=24 |
| C=2 | I=8 | O=14 | t=19 | Z=25 |
| D=3 | J=9 | P=15 | U=20 | |
| E=4 | K=10 | Q=16 | V=21 | |
| F=5 | L=11 | R=17 | W=22 | |



Caesar Cipher: Example

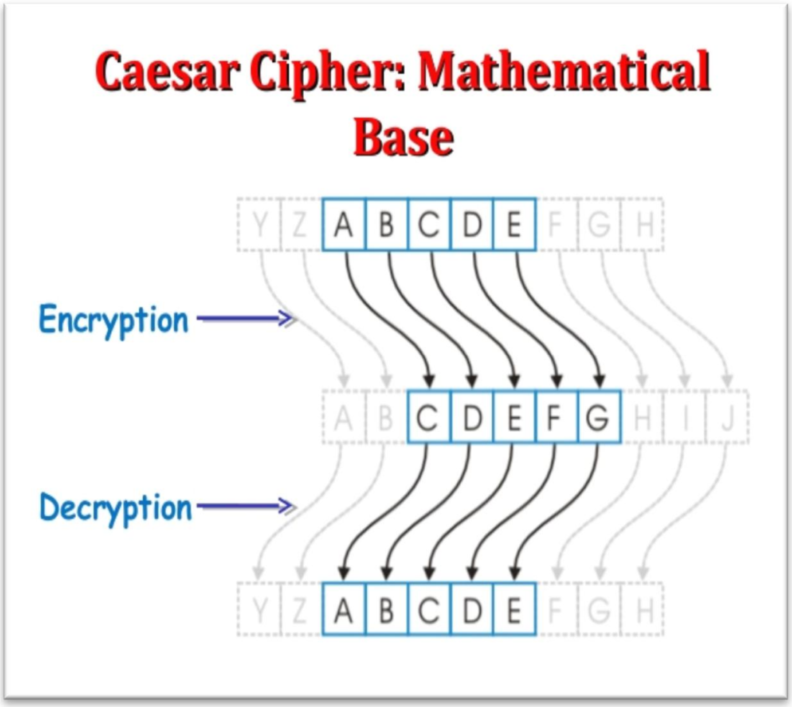
- **Encryption:** using single shift (shift key=1)

plaintext: defend the east wall of the castle
ciphertext: efgfoe uif fbtu xbmm pg uif dbtumf

- It is easy to see how each character in the plaintext is shifted up the alphabet. Decryption is just as easy, by using an offset of -1.

- **Decryption:**

ciphertext: efgfoe uif fbtu xbmm pg uif dbtumf
plaintext: defend the east wall of the castle

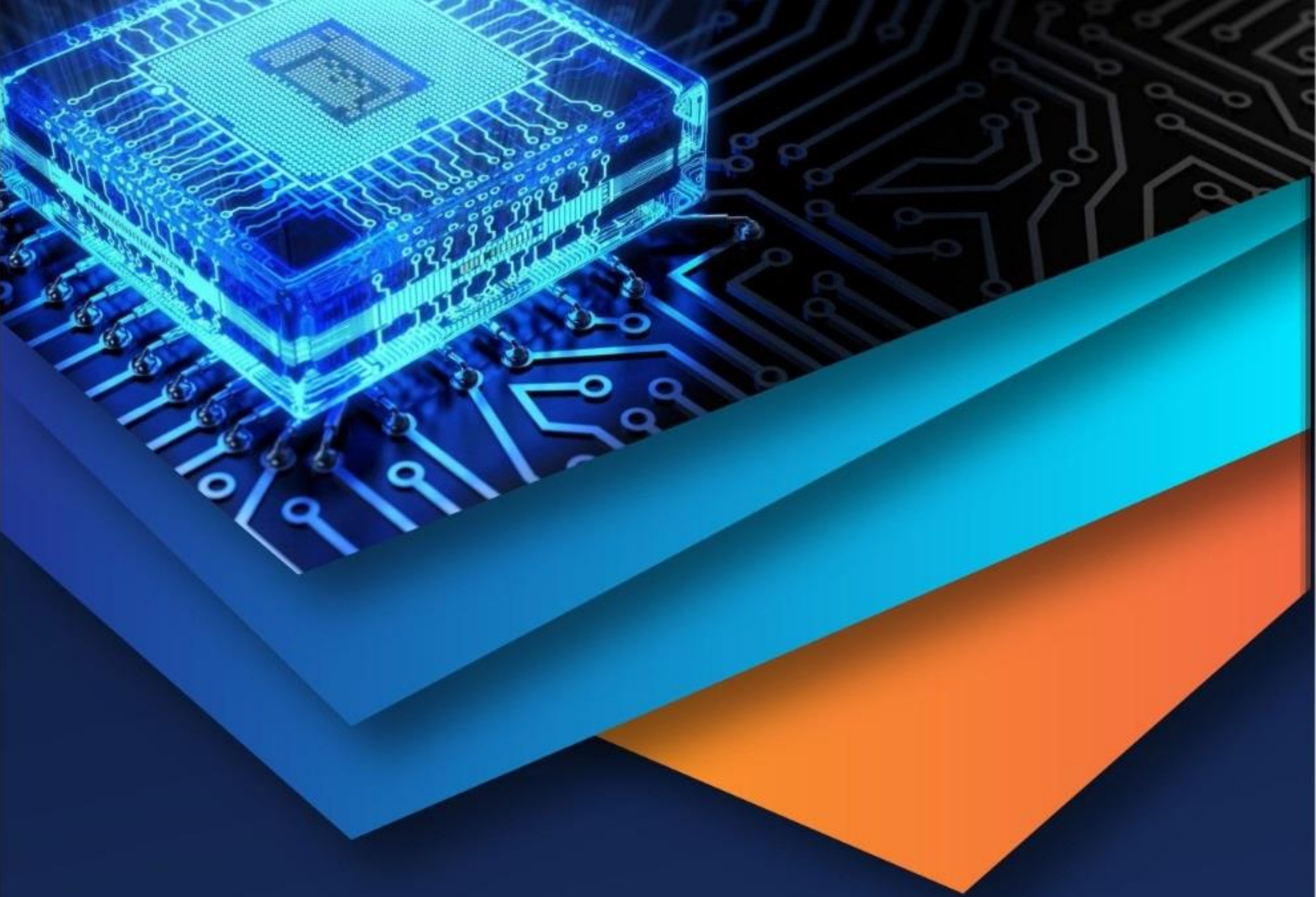


## III. SUMMARY

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified.

## REFERENCES

[1] https://www.researchgate.net/publication/328693056
[2] https://en.m.wikipedia.org/wiki/Caesar_cipher
[3] https://www.educba.com/types-of-cipher/
[4] https://crypto.interactive-maths.com/homophonic-substitution.html
[5] https://github.com/enRaved/Homophonic-Substitution-Cipher



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429