ACM PROJECT REPORT

ON

OLD CRYPTOGRAPHY TECHNIQUE

Submitted By : Submitted To :

Vipul Kumar Singh **Anuradha Chug Mam**

GIT HUB REPO LINK : https://github.com/vipul-2003/ACM-PROJECT

B TECH – 1st YEAR

ENROLLMENT NO . : 062-1641-2820

UNIVERSITY SCHOOL OF INFORMATION AND

COMMUNICATION TECHNOLOGY

GURU GOBIND SINGH INDRAPRASTHA

UNIVERSITY,NEW DELHI-110078

(2020-2024)

DECLARATION

I certify that

I. The work contained in the thesis/major project is original and has been done by myself under the supervision of my supervisor.

II. The work has not been submitted to any other Institute for any degree or diploma.

III. I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.

IV. Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.

V. Whenever I have quoted written materials from other sources and due credit is given to the sources by citing them.

VI. From the plagiarism test, it is found that the similarity index of whole thesis within 25% and single paper is less than 10 % as per the university guidelines.

Date: 10 September ,2021 **Name of the Student: Vipul Kumar Singh**

Place: New Delhi **Roll. No.: 06216412820**

CERTIFICATE

This is to certify that the paper entitled **“OLD CRYPTOGRAPHY TECHNIQUES IMPLEMENTATION ”** which is being submitted by **Vipul Kumar Singh (06216412820)** in partial fulfilment of the requirement for the award of degree B.Tech in Electronics and communication Engineering to USICT GGSIP University Dwarka Sec-16 , Delhi is a record of the candidate own work carried out by them under my supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree, to the best of my knowledge and belief.

Date: 10 September ,2021

Under the Supervision

Mrs. Anuradha Chug
(Assistant Professor)

ACKNOWLEDGEMENT

I am very grateful to all the people, who gave an excellent opportunity to develop this Project “**OLD CRYPTOGRAPHY TECHNIQUES IMPLEMENTATION** ” which not only enhanced my knowledge but also gave me the opportunity to do something practically useful.

I am heartily thankful to my mentor, **Mrs. Anuradha Chug, Assistant Professor,** Department of Information Technology, USICT, whose encouragement; guidance and support kept me highly motivated from the initial to the final level and enabled me to develop an understanding of the subject.

Lastly, I offer my regards to all of those who directly or indirectly supported me in any respect during the completion of this Project

Name of the Student: Vipul Kumar Singh

Roll. No.: 06216412820

ABSTRACT

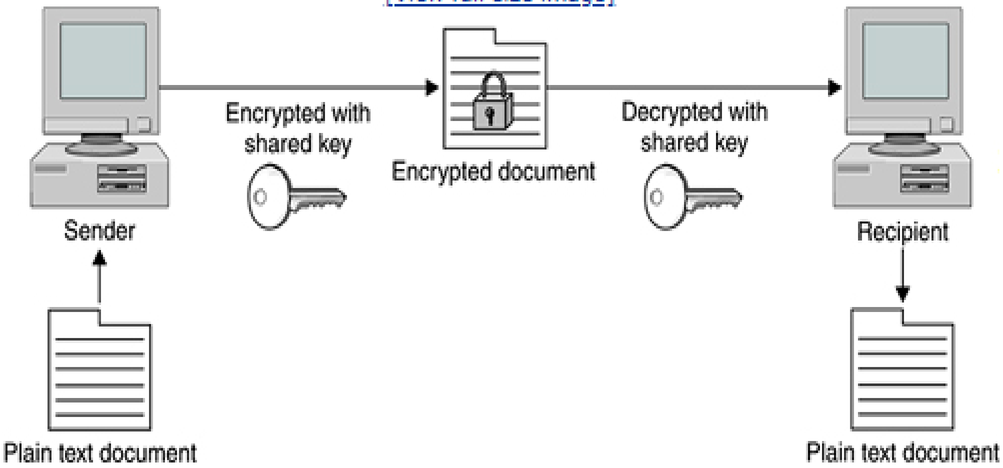
Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix **"crypt-"** means **"hidden"** or **"vault"** and the suffix **"- graphy "** stands for **"writing."**

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

Modern cryptography concerns itself with the following four objectives:

1. **Confidentiality**: the information cannot be understood by anyone for whom it was unintended
2. **Integrity:** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3. **Non-repudiation**: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
4. **Authentication**: the sender and receiver can confirm each other's identity and the origin/destination of the information

[View full size image]



History of cryptography :

The word "cryptography" is derived from the Greek *kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern **cipher** was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

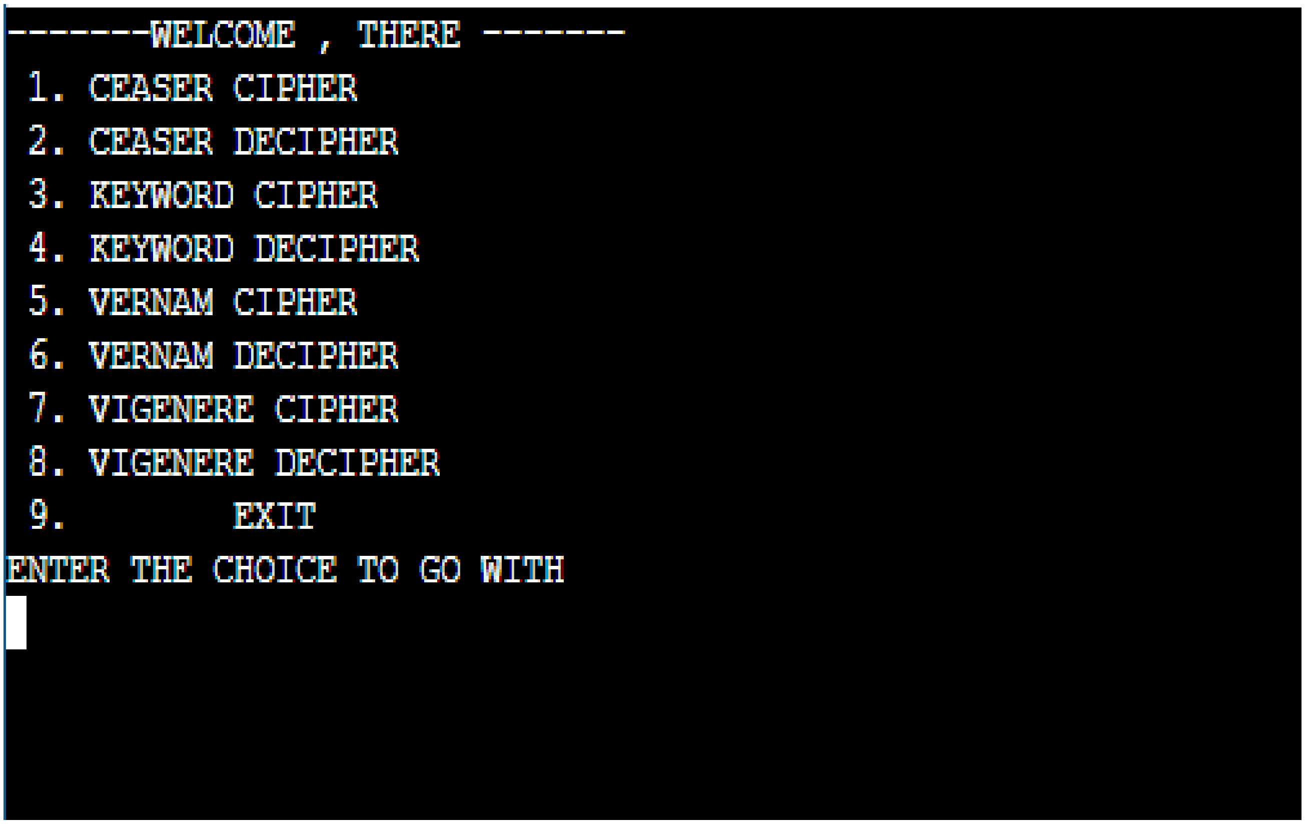
Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

How Does Encryption Work?

Now that we are clear on the concept of encryption, let’s have a look at how exactly it works. In simpler words, encryption uses algorithms to jumble up whatever data you want to encrypt. You need to have a randomly generated key before sending the message or data to the person at the receiving end, through which they can decrypt it. Imagine you have put a lock on the box containing important documents with the help of a key. You send that box to your friend. She has the same key as yours through which she is able to unlock it and get access to those important documents. But in the digital world, all this is done electronically!

So, there are **three encryption levels** that are at work:

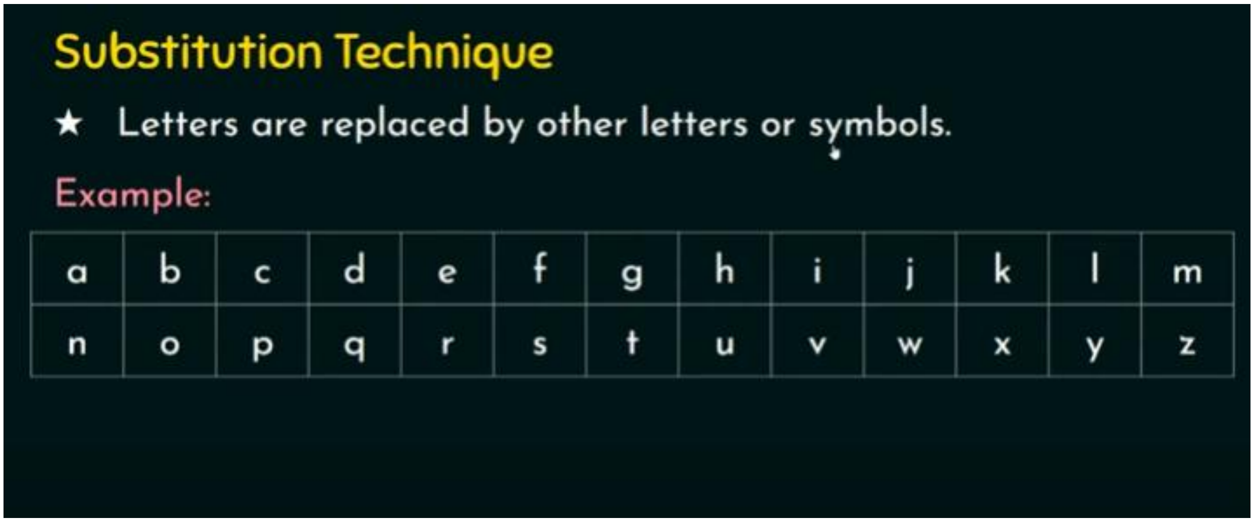
1. **Plain text**
2. **Encrypted text (ciphertext)**
3. **Decrypted text (same as the initial plain text).**



```
-------WELCOME , THERE -------
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9.       EXIT
ENTER THE CHOICE TO GO WITH
```

TYPES OF CLASSICAL TECHNIQUES :

1. **Substitution Technique .**
2. **Transposition Technique.**

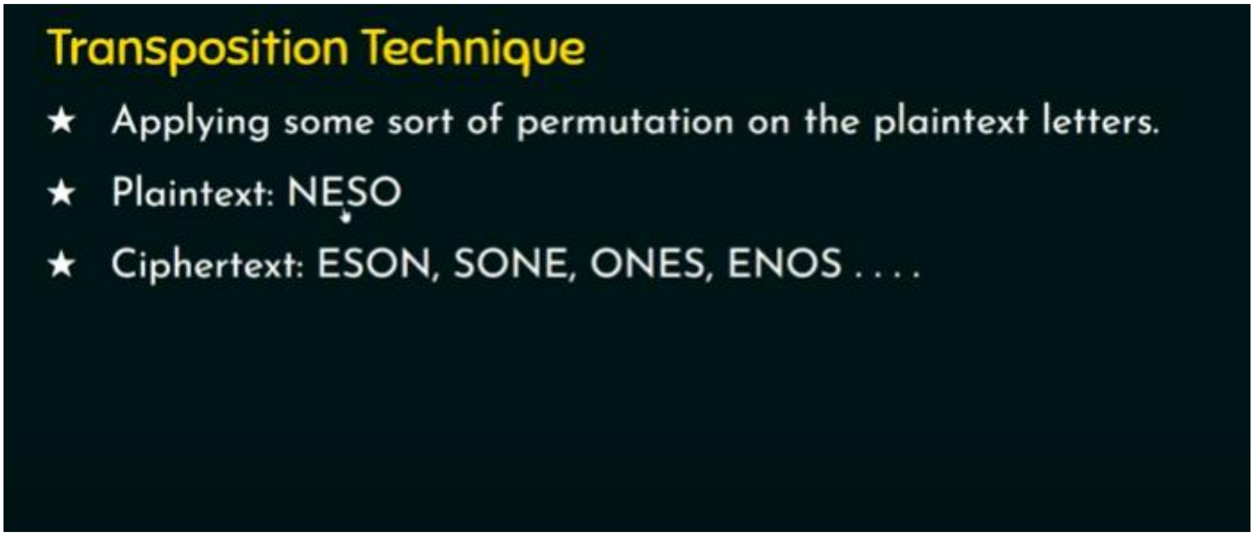


Substitution Technique

★ Letters are replaced by other letters or symbols.

Example:

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



Transposition Technique

★ Applying some sort of permutation on the plaintext letters.

★ Plaintext: NESO

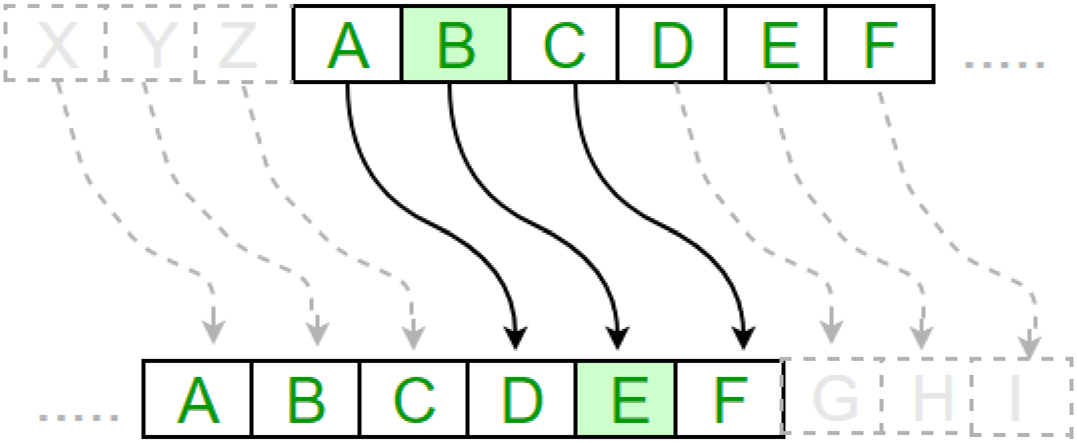
★ Ciphertext: ESON, SONE, ONES, ENOS . . . .

CEASER ENCRYPTION :

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.
Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.
The encryption can 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 by a shift n can be described mathematically as.

(Encryption Phase with shift n)

(Decryption Phase with shift n)



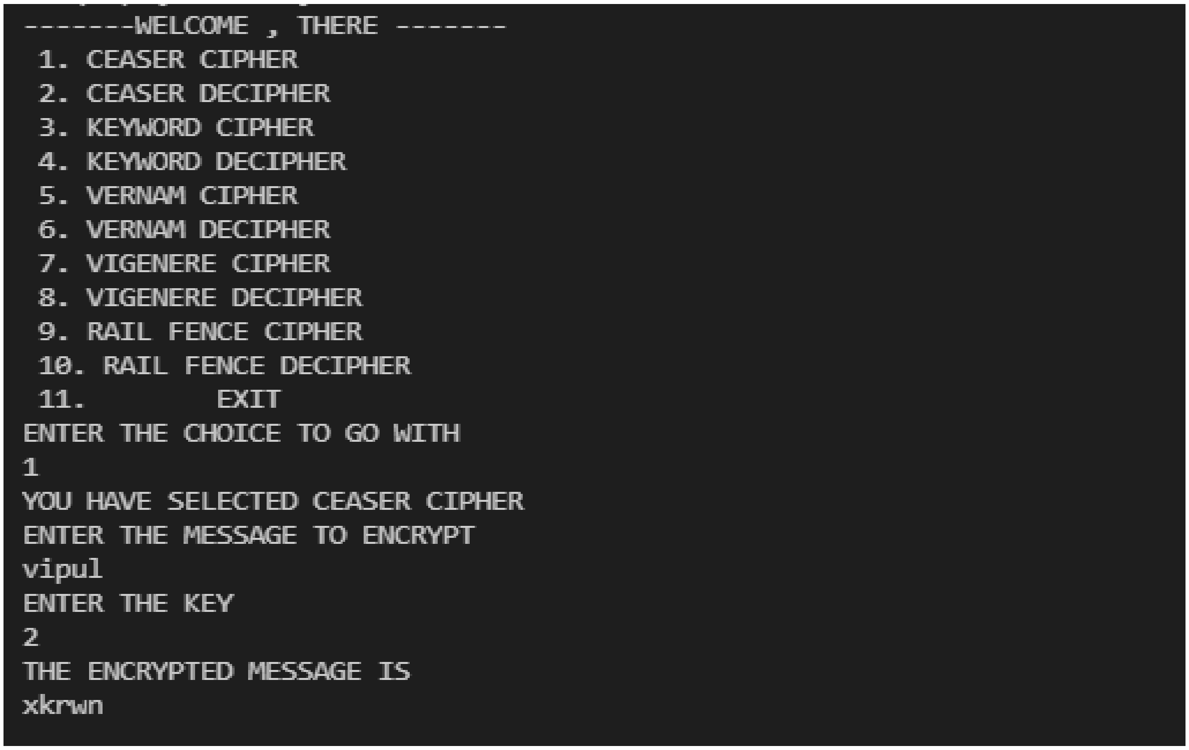
Algorithm for Caesar Cipher:
Input:

1. A String of lower case letters, called Text.
2. An Integer between 0-25 denoting the required shift.

Procedure:

- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
- Return the new string generated.

Program that receives a Text (string) and Shift value(integer) and returns the encrypted text.

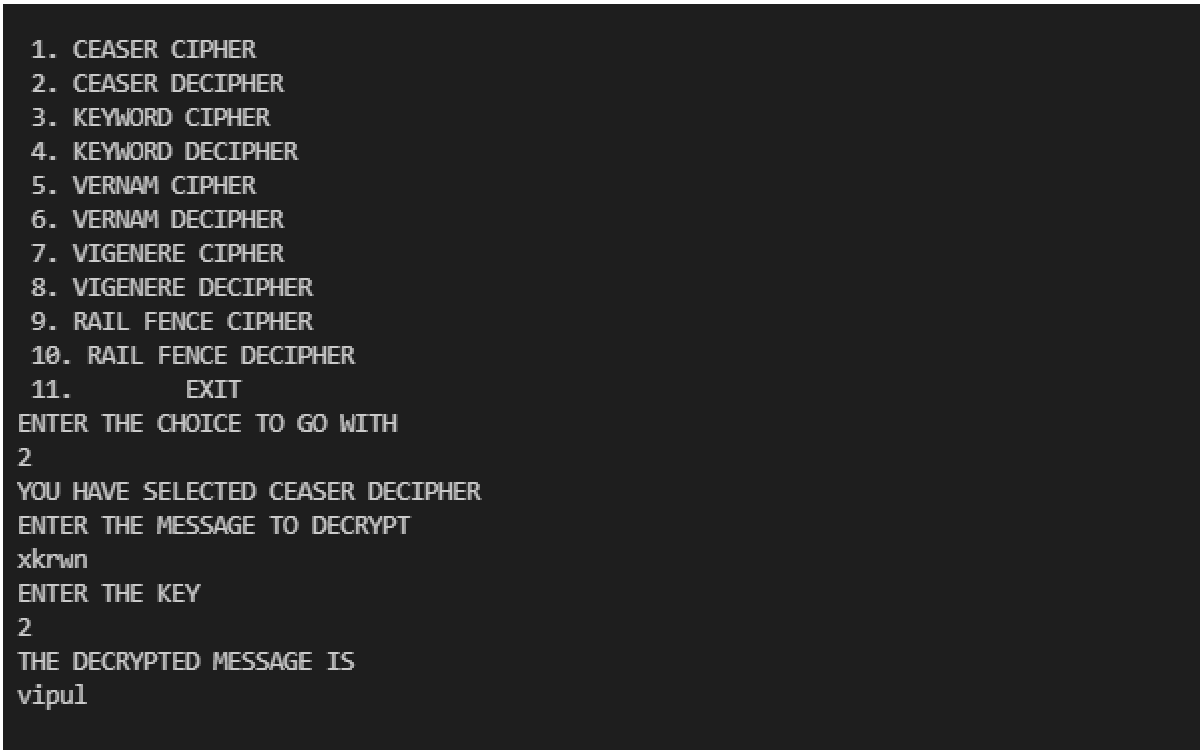


```
-------WELCOME , THERE -------
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9. RAIL FENCE CIPHER
 10. RAIL FENCE DECIPHER
 11.        EXIT
ENTER THE CHOICE TO GO WITH
1
YOU HAVE SELECTED CEASER CIPHER
ENTER THE MESSAGE TO ENCRYPT
vipul
ENTER THE KEY
2
THE ENCRYPTED MESSAGE IS
xkrwn
```

How to decrypt?

We can either write another function decrypt similar to encrypt, that’ll apply the given shift in the opposite direction to decrypt the original text. However we can use the cyclic property of the cipher under modulo , hence we can simply observe

Hence, we can use the same function to decrypt, instead we’ll modify the shift value such that shift = 26-shift



```
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9. RAIL FENCE CIPHER
 10. RAIL FENCE DECIPHER
 11.        EXIT
ENTER THE CHOICE TO GO WITH
2
YOU HAVE SELECTED CEASER DECIPHER
ENTER THE MESSAGE TO DECRYPT
xkrwn
ENTER THE KEY
2
THE DECRYPTED MESSAGE IS
vipul
```

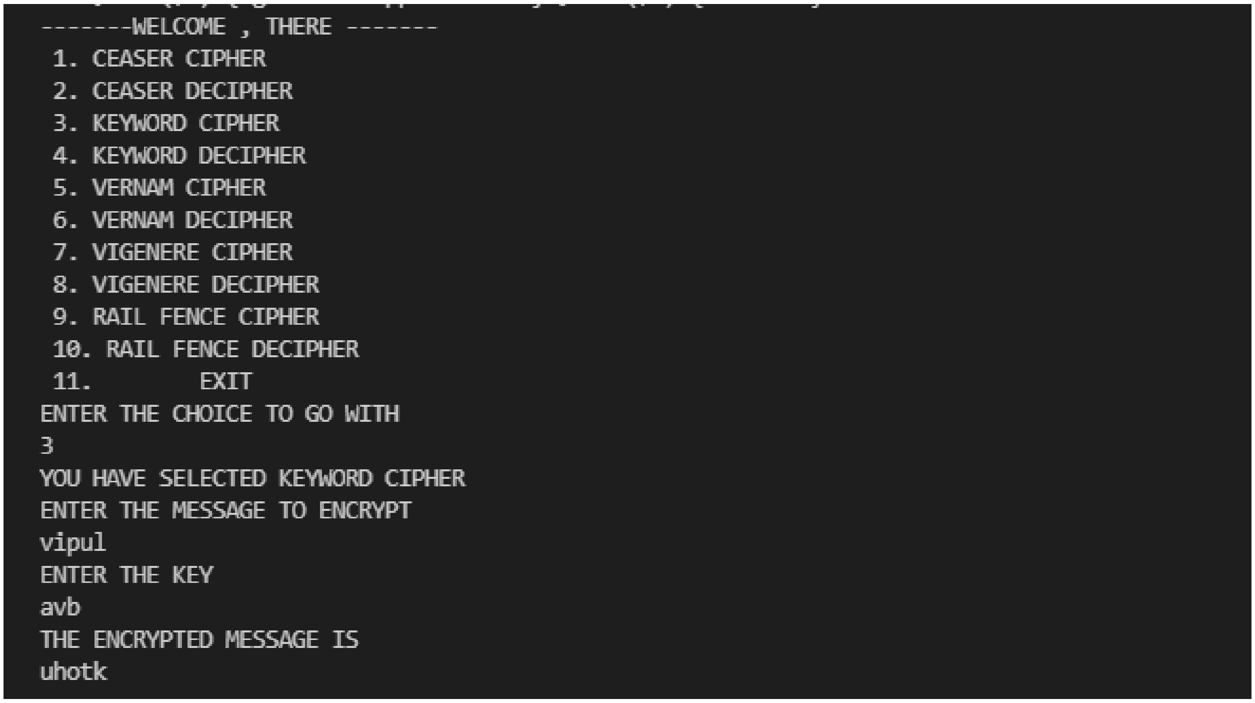
KEYWORD CIPHER :

A keyword cipher is a form of monoalphabetic substitution. A keyword is used as the key, and it determines the letter matchings of the cipher alphabet to the plain alphabet. Repeats of letters in the word are removed, then the cipher alphabet is generated with the keyword matching to A, B, C etc. until the keyword is used up, whereupon the rest of the ciphertext letters are used in alphabetical order, excluding those already used in the key.

Encryption

First line of input contains keyword which you wish to enter. Second line of input contains the string which you have to encrypt.

Plaintext : 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
Encrypted : a v b c d e f g h i j k l m n o p q r s t u w x y z

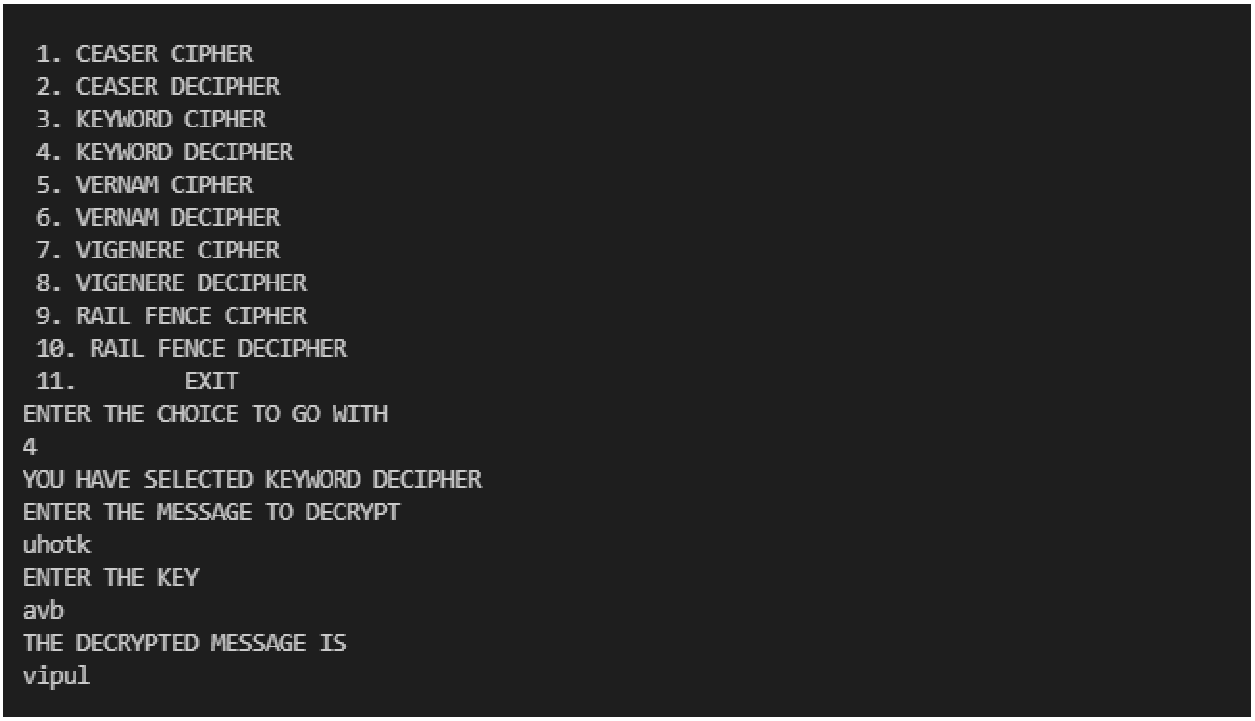


```
-------WELCOME , THERE -------
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9. RAIL FENCE CIPHER
 10. RAIL FENCE DECIPHER
 11.        EXIT
ENTER THE CHOICE TO GO WITH
3
YOU HAVE SELECTED KEYWORD CIPHER
ENTER THE MESSAGE TO ENCRYPT
vipul
ENTER THE KEY
avb
THE ENCRYPTED MESSAGE IS
uhotk
```

Decryption

To decode the message you check the position of given message in encrypting text with the plain text.

Plaintext : 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
Encrypted : a v b c d e f g h i j k l m n o p q r s t u w x y z



```
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9. RAIL FENCE CIPHER
 10. RAIL FENCE DECIPHER
 11.       EXIT
ENTER THE CHOICE TO GO WITH
4
YOU HAVE SELECTED KEYWORD DECIPHER
ENTER THE MESSAGE TO DECRYPT
uhotk
ENTER THE KEY
avb
THE DECRYPTED MESSAGE IS
vipul
```

VERNAM CIPHER :

The Vernam Cipher is an algorithm invented in 1917 to encrypt teletype (TTY) messages.

So named for Gilbert Sandford Vernam, it is a symmetric cipher patented July 22, 1919. The Vernam Cipher combines plaintext (the original message) with pseudo-random series of polyalphabetic characters to form the ciphertext using an "exclusive or" (XOR) function. US Army Captain Joseph Mauborgne soon discovered that the cipher could be made much stronger by using truly random numbers printed on pads of paper. Streams of paper with the random numbers in that fashion became a process known as "one-time pad". The Vernam using one-time pad is regarded as unbreakable.
On background, a teletype is a character printer connected to a telegraph that provides a user interface for people to communicate over various communications protocols such as dedicated or public wires, radio, or microwave.

Method to take key:

In Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.

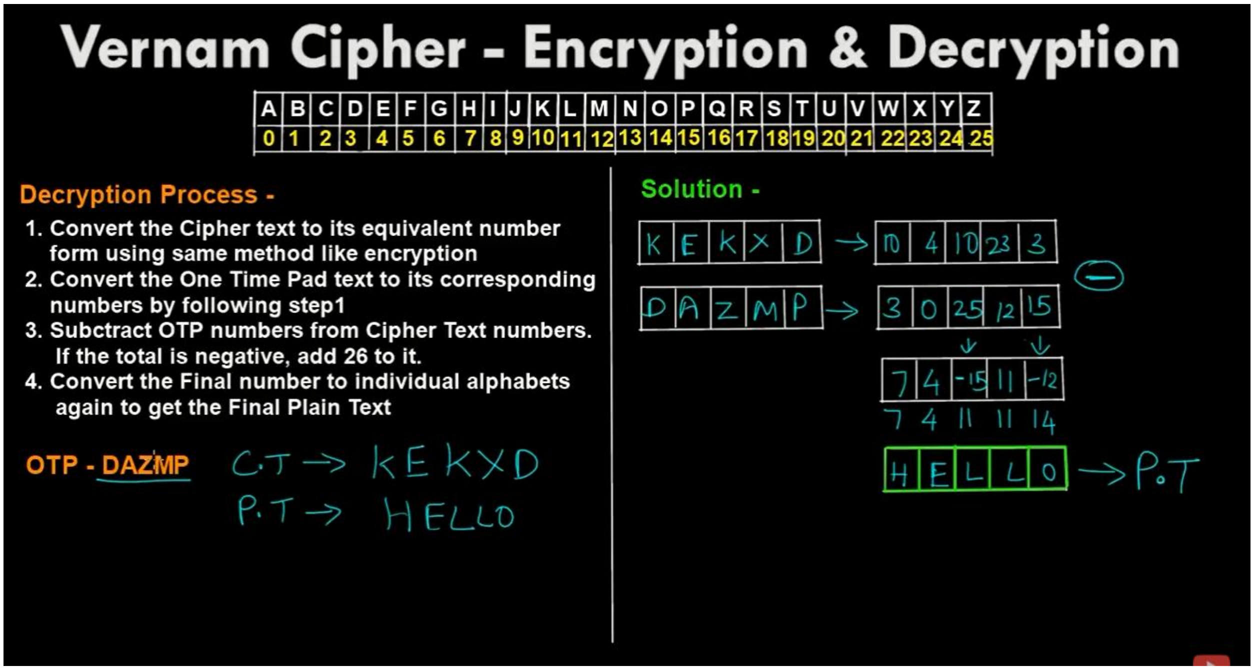
Encryption Algorithm:

1. Assign a number to each character of the plain-text and the key according to alphabetical order.

2. Add both the number (Corresponding plain-text character number and Key character number).

3. Subtract the number from 26 if the added number is greater than 26, if it isn't then leave it.

Now add the number of Plain-Text and Key and after doing the addition and subtraction operation (if required), we will get the corresponding Cipher-Text character number.



Vernam Cipher - Encryption & Decryption

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
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

Decryption Process -

1. Convert the Cipher text to its equivalent number form using same method like encryption
2. Convert the One Time Pad text to its corresponding numbers by following step1
3. Subctract OTP numbers from Cipher Text numbers. If the total is negative, add 26 to it.
4. Convert the Final number to individual alphabets again to get the Final Plain Text

OTP - DAZMP

C.T → KEKXD

P.T → HELLO

Solution -

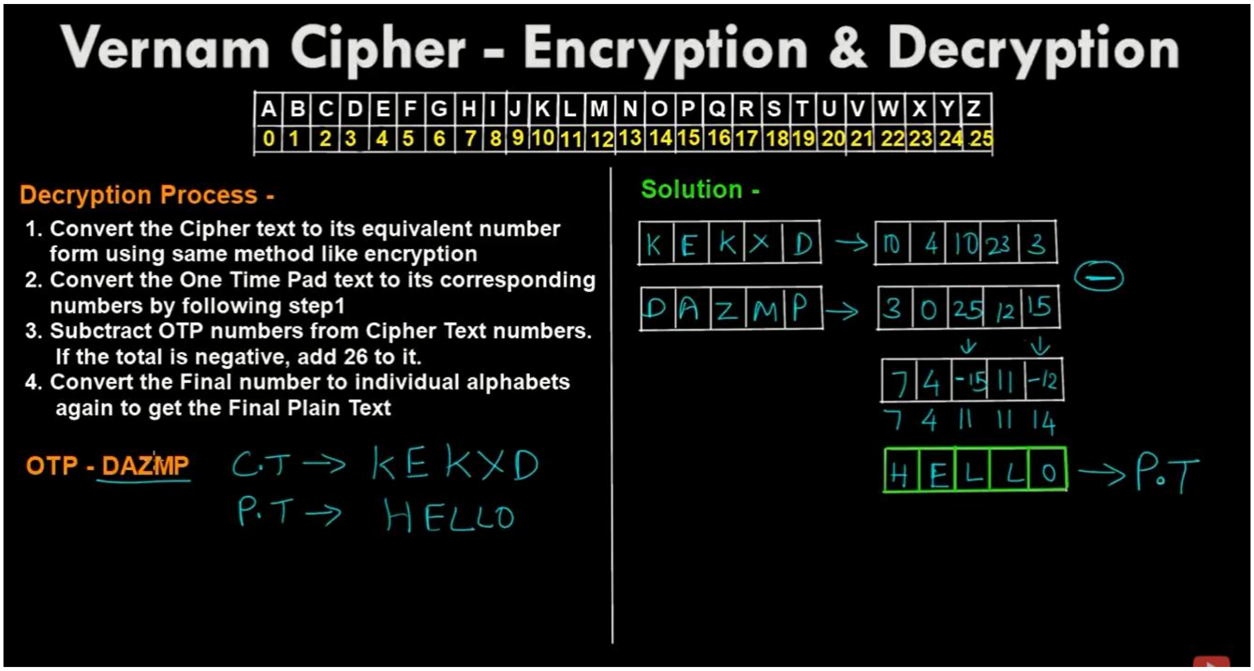
K E K X D → 10 4 10 23 3

D A Z M P → 3 0 25 12 15 ⊖

7 4 -15 11 -12

7 4 11 11 14

H E L L O → P.T



Vernam Cipher - Encryption & Decryption

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
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

Decryption Process -

1. Convert the Cipher text to its equivalent number form using same method like encryption
2. Convert the One Time Pad text to its corresponding numbers by following step1
3. Subctract OTP numbers from Cipher Text numbers. If the total is negative, add 26 to it.
4. Convert the Final number to individual alphabets again to get the Final Plain Text

OTP - DAZMP

C.T → KEKXD

P.T → HELLO

Solution -

K E K X D → 10 4 10 23 3

D A Z M P → 3 0 25 12 15 ⊖

7 4 -15 11 -12

7 4 11 11 14

H E L L O → P.T

VIGENERE CIPHER :

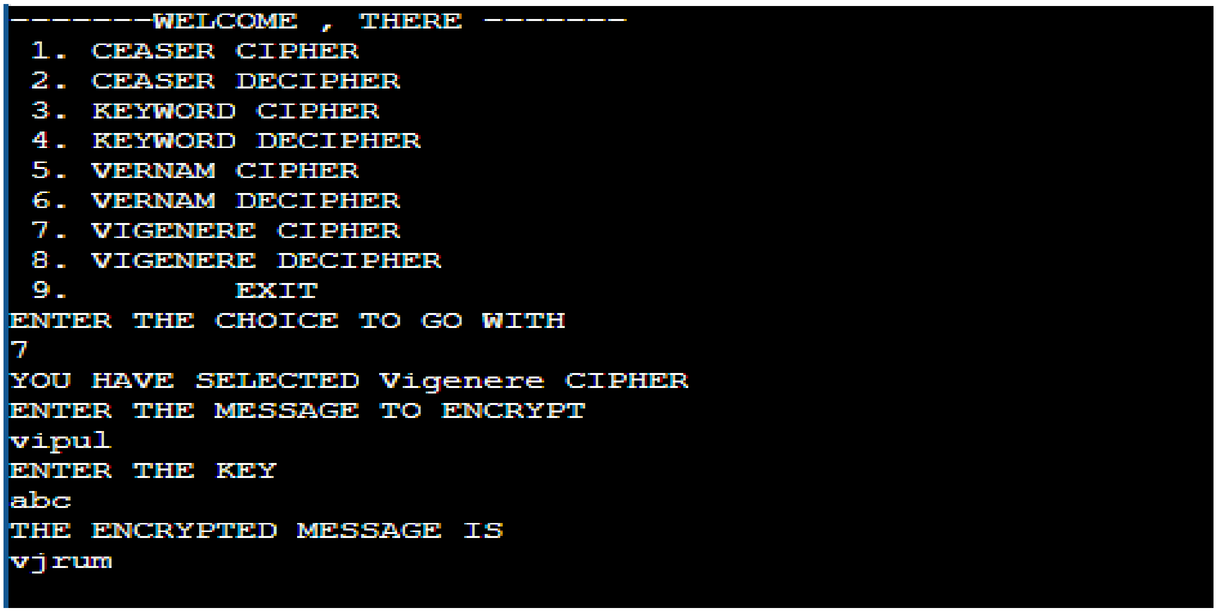
Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .The encryption of the original text is done using the Vigenère square or Vigenère table.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Encryption

The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column Y is C. The rest of the plaintext is enciphered in a similar
fashion.

$$E_i = (P_i + K_i) \bmod 26$$

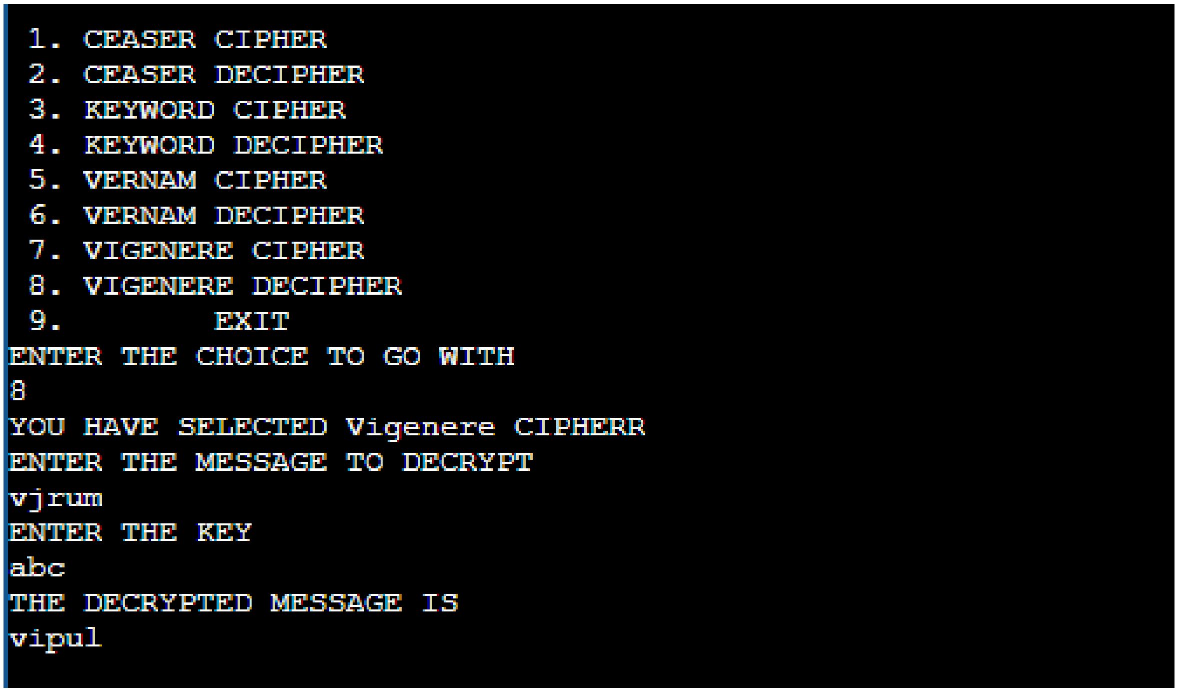


```
-------WELCOME , THERE -------
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9.       EXIT
ENTER THE CHOICE TO GO WITH
7
YOU HAVE SELECTED Vigenere CIPHER
ENTER THE MESSAGE TO ENCRYPT
vipul
ENTER THE KEY
abc
THE ENCRYPTED MESSAGE IS
vjrum
```

Decryption

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.
A more **easy implementation** could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].

$$\mathbf{D_i = (E_i - K_i + 26) \bmod 26}$$



```
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9.        EXIT
ENTER THE CHOICE TO GO WITH
8
YOU HAVE SELECTED Vigenere CIPHERR
ENTER THE MESSAGE TO DECRYPT
vjrum
ENTER THE KEY
abc
THE DECRYPTED MESSAGE IS
vipul
```

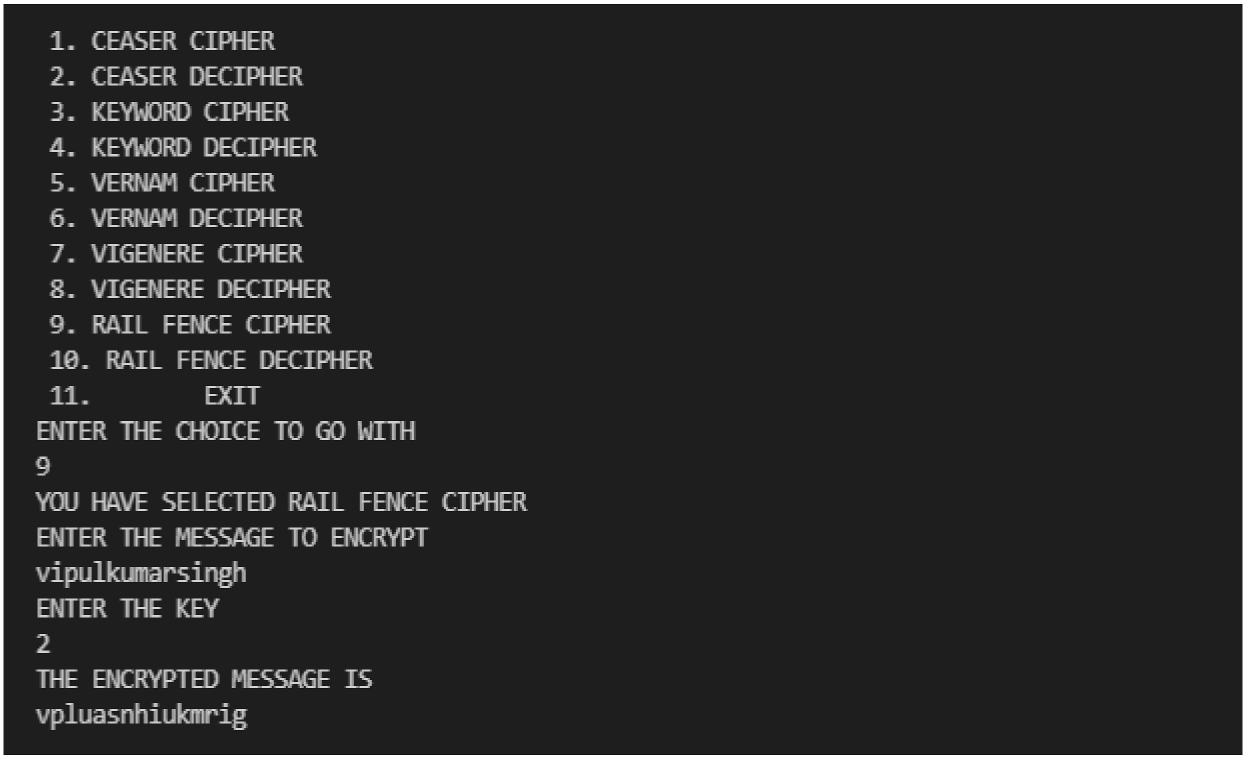
Rail Fence Cipher :

Given a plain-text message and a numeric key, cipher/de-cipher the given text using Rail Fence algorithm.
The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

Encryption

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.



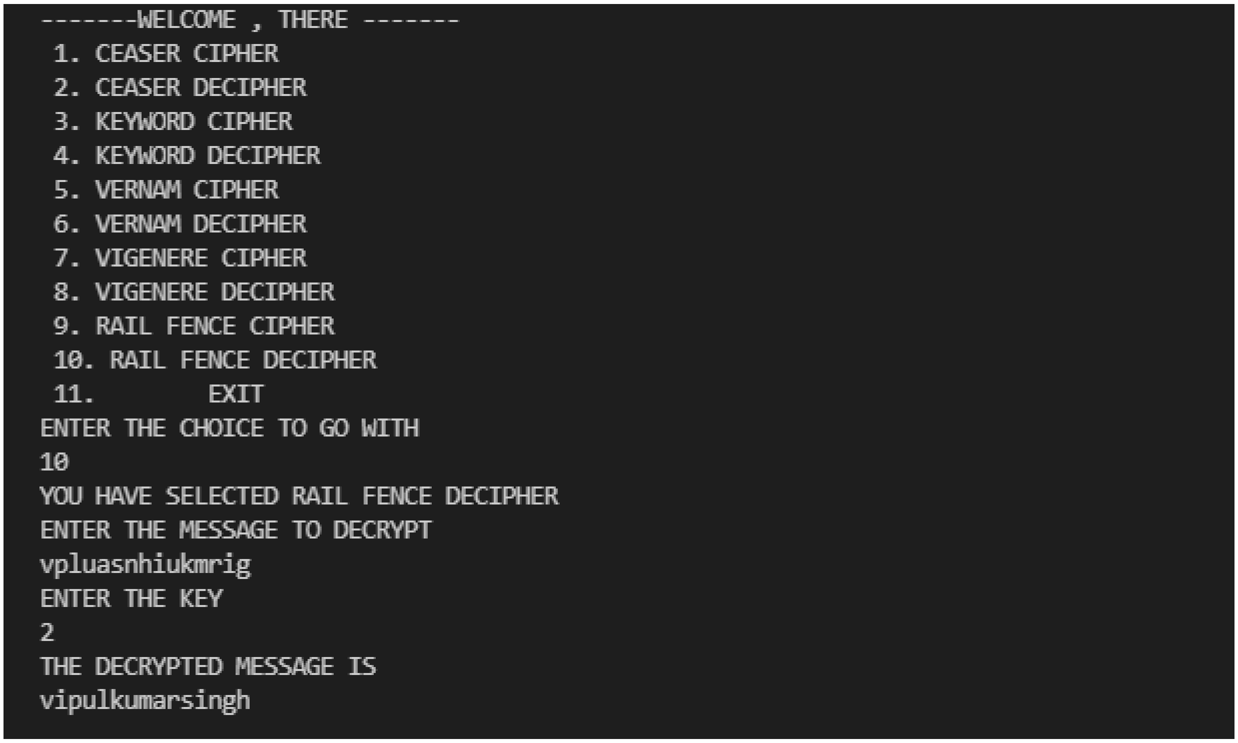
```
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9. RAIL FENCE CIPHER
 10. RAIL FENCE DECIPHER
 11.        EXIT
ENTER THE CHOICE TO GO WITH
9
YOU HAVE SELECTED RAIL FENCE CIPHER
ENTER THE MESSAGE TO ENCRYPT
vipulkumarsingh
ENTER THE KEY
2
THE ENCRYPTED MESSAGE IS
vpluasnhiukmrig
```

Decryption

As we’ve seen earlier, the number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.

- Hence, rail matrix can be constructed accordingly. Once we’ve got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).

- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.



```
-------WELCOME , THERE -------
 1. CEASER CIPHER
 2. CEASER DECIPHER
 3. KEYWORD CIPHER
 4. KEYWORD DECIPHER
 5. VERNAM CIPHER
 6. VERNAM DECIPHER
 7. VIGENERE CIPHER
 8. VIGENERE DECIPHER
 9. RAIL FENCE CIPHER
 10. RAIL FENCE DECIPHER
 11.        EXIT
ENTER THE CHOICE TO GO WITH
10
YOU HAVE SELECTED RAIL FENCE DECIPHER
ENTER THE MESSAGE TO DECRYPT
vpluasnhiukmrig
ENTER THE KEY
2
THE DECRYPTED MESSAGE IS
vipulkumarsingh
```

Related links :

- https://github.com/vipul-2003/ACM-PROJECT [Source Code]
- https://whimsical.com/cryptography-67Gfj8QufPBmgJDHY6fzoC [Flowchart Link]
- https://en.wikipedia.org/wiki/Caesar_cipher
- https://en.wikipedia.org/wiki/Cipher
- https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
- https://isaaccomputerscience.org/concepts/data_encrypt_vernam
- https://www.youtube.com/watch?v=Xb4_VT4y9kQ&list=PLBlnK6fEyqRgJU3EsOYDTW7m6SUmW6kII&index=9