Practical 12

Aim: Perform various Encryption-Decryption Techniques with Cryptool.

Cryptool:

- CrypTool is an open-source project that is a free e-learning softwarefor illustrating cryptographic and cryptanalytic concepts.
- CrypTool implements more than 400 algorithms. Users can adjust these with ownparameters.
- CrypTool is used in schools, universities, companies and agencies for education andawareness training.
- Currently 4 versions of CrypTool are maintained and developed: The CrypTool 1 (CT1)software is available in 6 languages (English, German, Polish, Spanish, Serbian, and French). CrypTool 2 (CT2) is available in 3 languages (English, German, Russian). Allothers, JCrypTool (JCT) and CrypTool-Online (CTO), are available only in English andGerman.

What is Cryptool?

Crytool is a tool often associated with the cryptocurrency and blockchain space, particularly for managing, analyzing, or developing projects related to cryptocurrencies. It can provide functionalities such as wallet management, transaction monitoring, and analytics for cryptoinvestments. The specific features and capabilities can vary depending on the version or developerof Crytool. If you have a particular aspect of Crytool you're curious about, feel free to ask!

- **Cryptocurrency Management**: Crytool helps users manage their cryptocurrency wallets andassets efficiently.

- **Transaction Monitoring**: It allows users to track and analyze transactions in real time.

- **Portfolio Analytics**: Users can monitor the performance of their cryptocurrency investmentsthrough various analytical tools.

- **User-Friendly Interface**: Designed to be accessible for both beginners and experienced users.

- **Multi-Currency Support**: Typically supports a wide range of cryptocurrencies for versatilemanagement.

- **Security Features**: Emphasizes the security of user funds, often incorporating encryption andtwo-factor authentication.

- **Market Insights**: Provides market data and trends to help users make informed investmentdecisions.

- **Community Features**: May include forums or social features for users to share tips andstrategies.

- **Customization**: Offers options to tailor the user experience to individual preferences.

- **Updates and Support**: Regular updates and customer support to address user needs andimprove functionality.

Substituion Cipher:

⍰ In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key.For example with a shift of 1, A would be replaced by B, B would become C, and so on.

<u>Algorithm for Substitution Cipher:</u>

Input:

⍰ A String of both lower and upper case letters, called PlainText.
⍰ An Integer denoting the required key.

Procedure:

⍰ Create a list of all the characters.
⍰ Create a dictionary to store the substitution for all characters.
⍰ For each character, transform the given character as per the rule,

depending onwhether we’re encrypting or decrypting the text.

 Print the new string generated.

Types:

a) Caser Ciper

The Caesar cipher is the simplest and oldest method of cryptography.

The Caesar cipher method is based on a mono-alphabetic cipher and is also called a shiftcipher or additive cipher.

Julius Caesar used the shift cipher (additive cipher) technique to communicate with hisofficers.

For this reason, the shift cipher technique is called the Caesar cipher. The Caesar cipheris a kind of replacement (substitution) cipher, where all letter of plain text is replacedby another letter.

The formula of encryption

is: En (x) = (x + n) mod

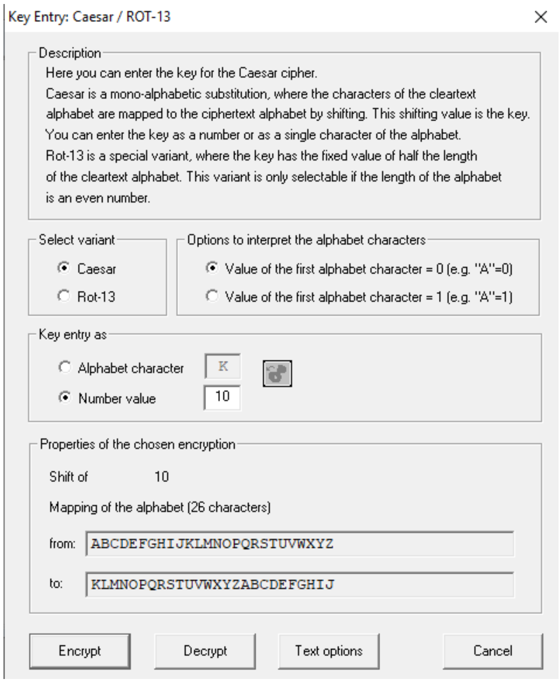
26

The formula of decryption

is: Dn (x) = (xi - n) mod

26

Output:



Key Entry: Caesar / ROT-13

Description

Here you can enter the key for the Caesar cipher.
Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key.
You can enter the key as a number or as a single character of the alphabet.
Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.

Select variant
● Caesar
○ Rot-13

Options to interpret the alphabet characters
● Value of the first alphabet character = 0 (e.g. "A"=0)
○ Value of the first alphabet character = 1 (e.g. "A"=1)

Key entry as
○ Alphabet character K
● Number value 10

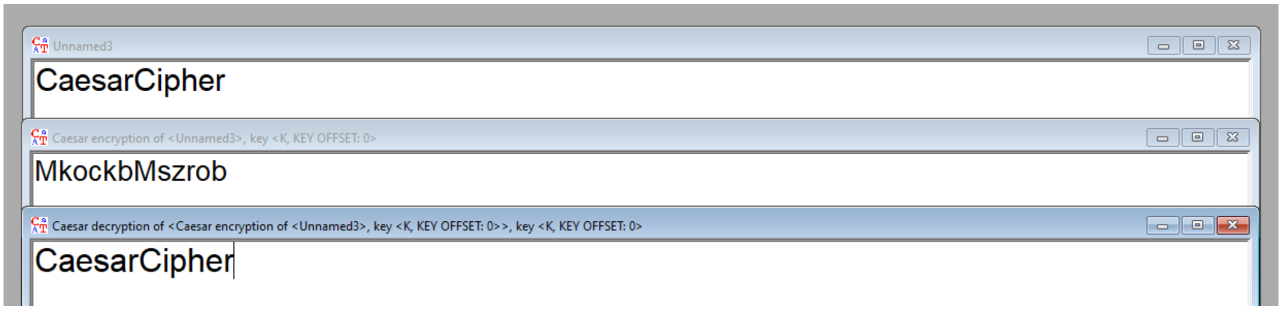
Properties of the chosen encryption

Shift of 10

Mapping of the alphabet (26 characters)

from: ABCDEFGHIJKLMNOPQRSTUVWXYZ

to: KLMNOPQRSTUVWXYZABCDEFGHIJ



Unnamed3

CaesarCipher

Caesar encryption of <Unnamed3>, key <K, KEY OFFSET: 0>

MkockbMszrob

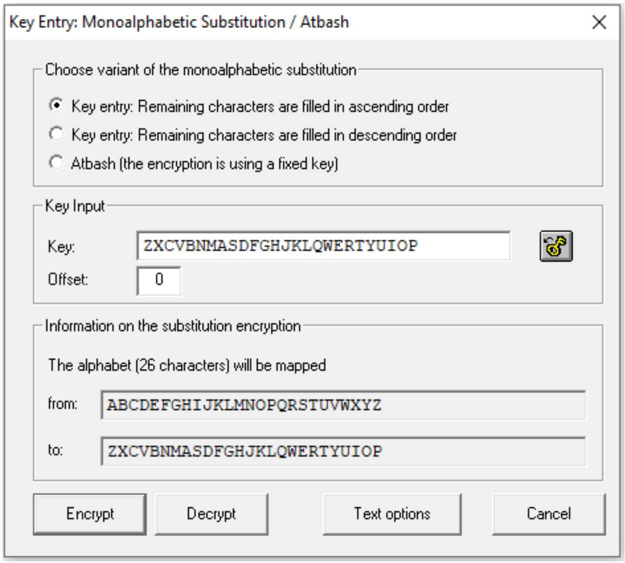
Caesar decryption of <Caesar encryption of <Unnamed3>, key <K, KEY OFFSET: 0> >, key <K, KEY OFFSET: 0>

CaesarCipher

b) Monoalphabatic

- Mono-alphabetic cipher (aka simple substitution cipher) is a substitution cipher where each letter of the plain text is replaced with another letter of the alphabet. Ituses a fixed key which consist of the 26 letters of a “shuffled alphabet”.
- This type of cipher is a form of symmetric encryption as the same key can be used to bothencrypt and decrypt a message.

Output :


Key Entry: Monoalphabetic Substitution / Atbash

Choose variant of the monoalphabetic substitution

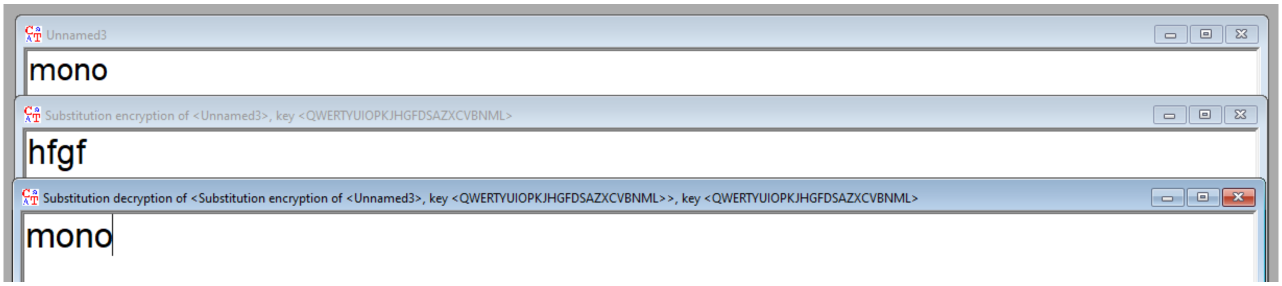
● Key entry: Remaining characters are filled in ascending order
○ Key entry: Remaining characters are filled in descending order
○ Atbash (the encryption is using a fixed key)

Key Input

Key: ZXCVBNMASDFGHJKLQWERTYUIOP
Offset: 0

Information on the substitution encryption

The alphabet (26 characters) will be mapped
from: ABCDEFGHIJKLMNOPQRSTUVWXYZ
to: ZXCVBNMASDFGHJKLQWERTYUIOP


Unnamed3

mono

Substitution encryption of <Unnamed3>, key <QWERTYUIOPKJHGFDSAZXCVBNML>

hfgf

Substitution decryption of <Substitution encryption of <Unnamed3>, key <QWERTYUIOPKJHGFDSAZXCVBNML>>, key <QWERTYUIOPKJHGFDSAZXCVBNML>

mono

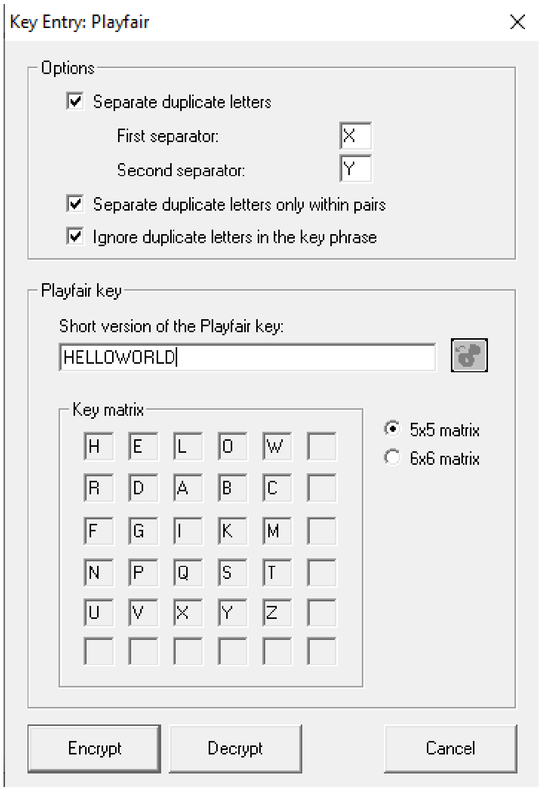
c) Playfair Cipher

- The Playfair cipher encryption technique can be used to encrypt or encode a message. It operates exactly like typical encryption. The only difference is that it encrypts a digraph, or a pair of two letters, as opposed to a single letter.
- An initial 5×5 matrix key table is created. The plaintext encryption key is made out of the matrix's alphabetic characters. Be mindful that you shouldn't repeat the letters.

  There are 26 alphabets, however, there are only 25 spaces in which we can place aletter. The matrix will delete the extra letter because there is an excess of one letter(typically J).

  Despite this, J is there in the plaintext before being changed to I.

Output :



Key Entry: Playfair

Options

☑ Separate duplicate letters

First separator: X

Second separator: Y

☑ Separate duplicate letters only within pairs

☑ Ignore duplicate letters in the key phrase

Playfair key

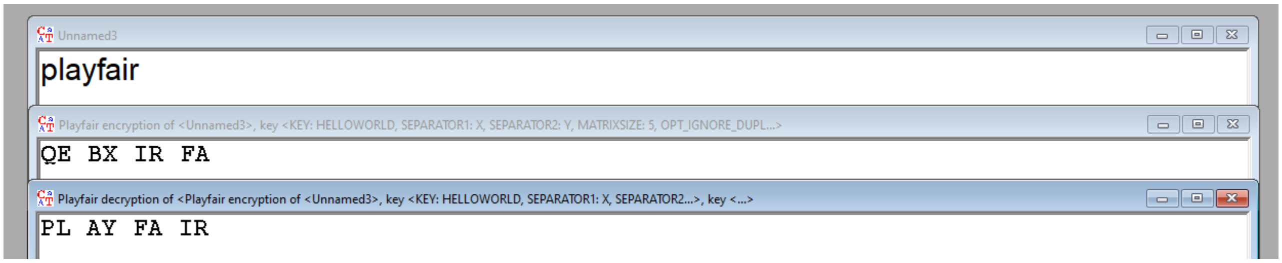
Short version of the Playfair key: HELLOWORLD

Key matrix

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

● 5x5 matrix

○ 6x6 matrix



Unnamed3

```
playfair
```

Playfair encryption of <Unnamed3>, key <KEY: HELLOWORLD, SEPARATOR1: X, SEPARATOR2: Y, MATRIXSIZE: 5, OPT_IGNORE_DUPL...>

```
QE BX IR FA
```

Playfair decryption of <Playfair encryption of <Unnamed3>, key <KEY: HELLOWORLD, SEPARATOR1: X, SEPARATOR2...>, key <...>

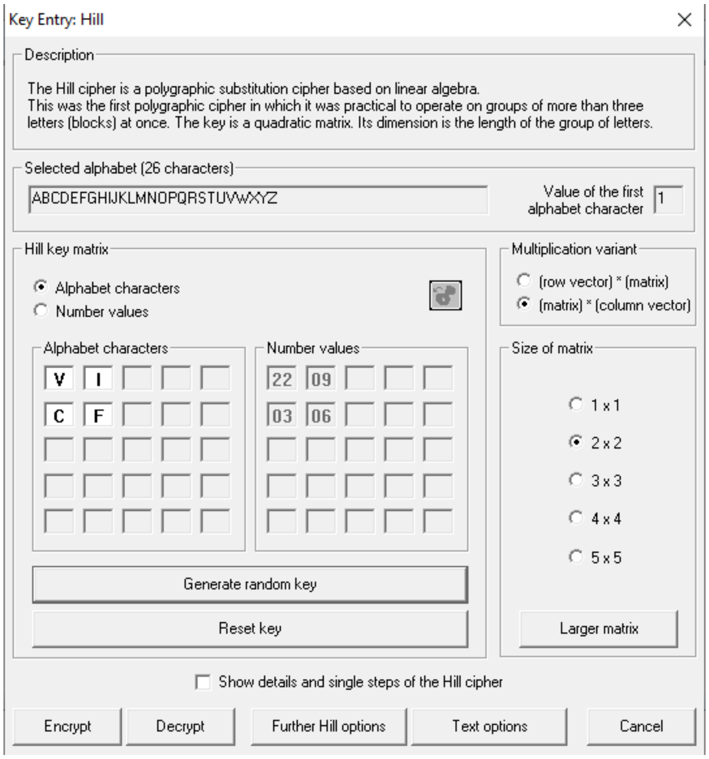
```
PL AY FA IR
```

d) Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher. 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 thematrix used for encryption.

- The matrix used for encryption is the cipher key, and it should be chosen randomlyfrom the set of invertible n × n matrices (modulo 26).

Output :



Key Entry: Hill

Description

The Hill cipher is a polygraphic substitution cipher based on linear algebra.
This was the first polygraphic cipher in which it was practical to operate on groups of more than three letters (blocks) at once. The key is a quadratic matrix. Its dimension is the length of the group of letters.

Selected alphabet (26 characters)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Value of the first alphabet character: 1

Hill key matrix

● Alphabet characters
○ Number values

Multiplication variant

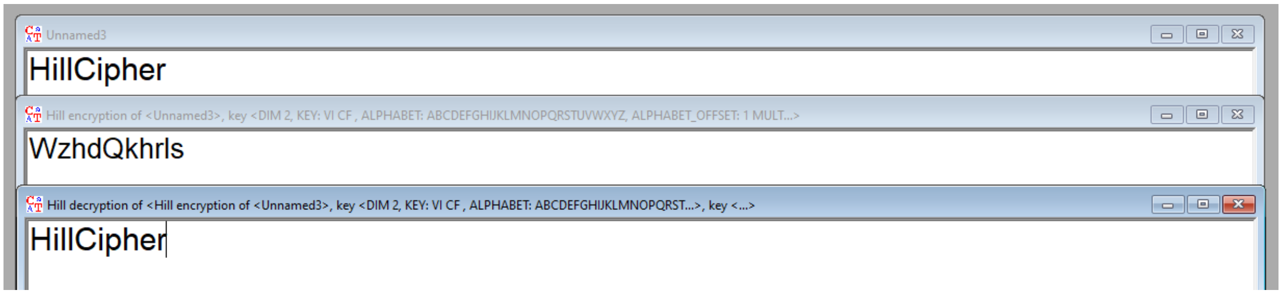
○ (row vector) * (matrix)
● (matrix) * (column vector)

Alphabet characters		Number values	
V	I	22	09
C	F	03	06

Size of matrix

○ 1 x 1
● 2 x 2
○ 3 x 3
○ 4 x 4
○ 5 x 5

□ Show details and single steps of the Hill cipher



Unnamed3

HillCipher

Hill encryption of <Unnamed3>, key <DIM 2, KEY: VI CF , ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFFSET: 1 MULT...>

WzhdQkhrls

Hill decryption of <Hill encryption of <Unnamed3>, key <DIM 2, KEY: VI CF , ALPHABET: ABCDEFGHIJKLMNOPQRST...>, key <...>

HillCipher

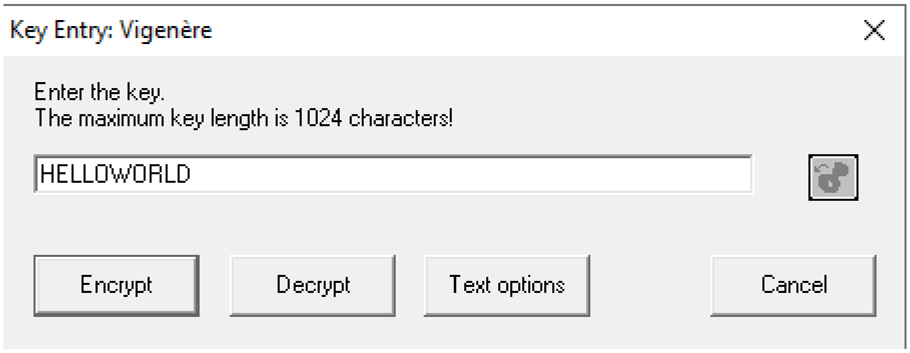
e) Polyalphabetic Cipher:

- A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters areenciphered differently based upon their installation in the text. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.

- There are two types of it.

1) ***Vigenere Cipher***

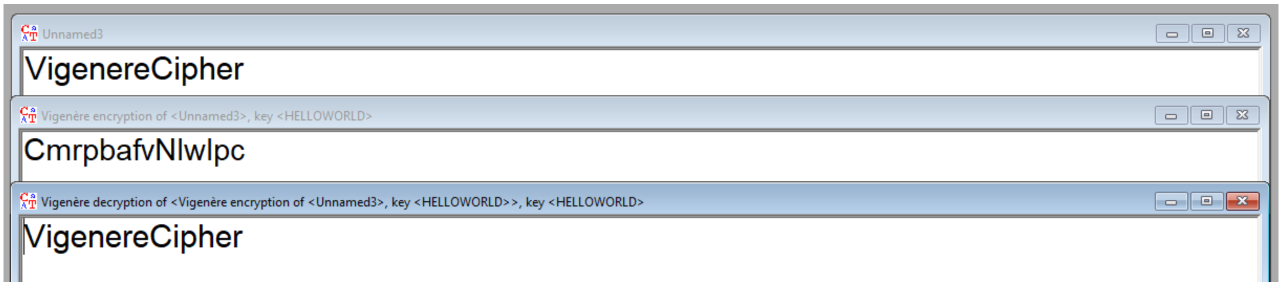
- The encryption of the original text is done using the Vigenère square or Vigenère table.
- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the26 possible Caesar Ciphers.
- At 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.



Key Entry: Vigenère

Enter the key.
The maximum key length is 1024 characters!

HELLOWORLD



Unnamed3

VigenereCipher

Vigenère encryption of <Unnamed3>, key <HELLOWORLD>

CmrpbafvNlwlpc

Vigenère decryption of <Vigenère encryption of <Unnamed3>, key <HELLOWORLD>>, key <HELLOWORLD>

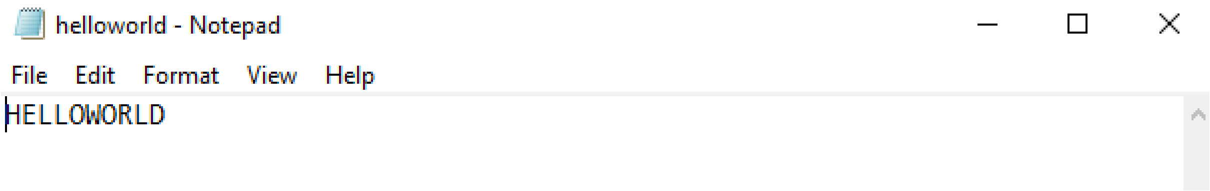
VigenereCipher

2) ***Vernam Cipher***

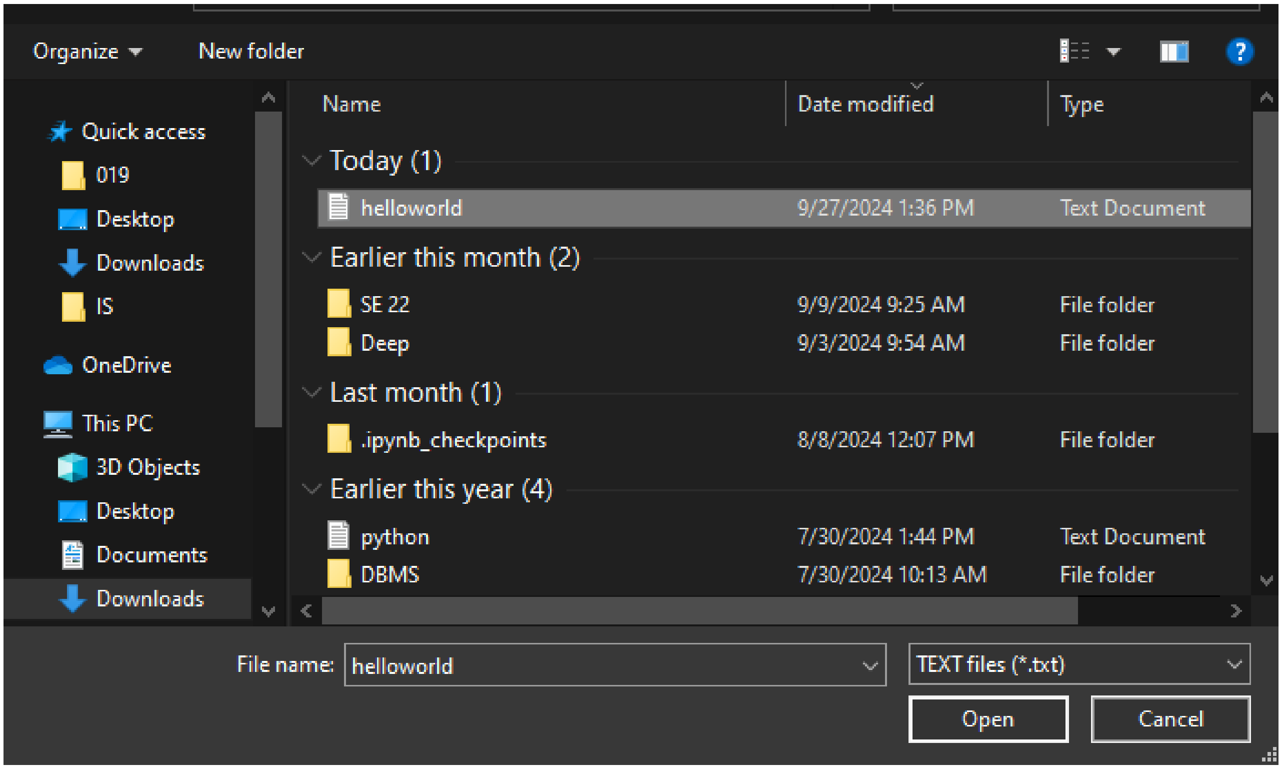
- Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitutiontechniques for converting plain text into cipher text. In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, ... z = 25).
- Method to take key**:** In the Vernam cipher algorithm, we take a key to encrypt theplain text whose 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 toalphabetical order.
2. Bitwise XOR both the number (Corresponding plain-text character number andKey character number).
3. Subtract the number from 26 if the resulting number is greater than or equal to 26,if it isn't then leave it.



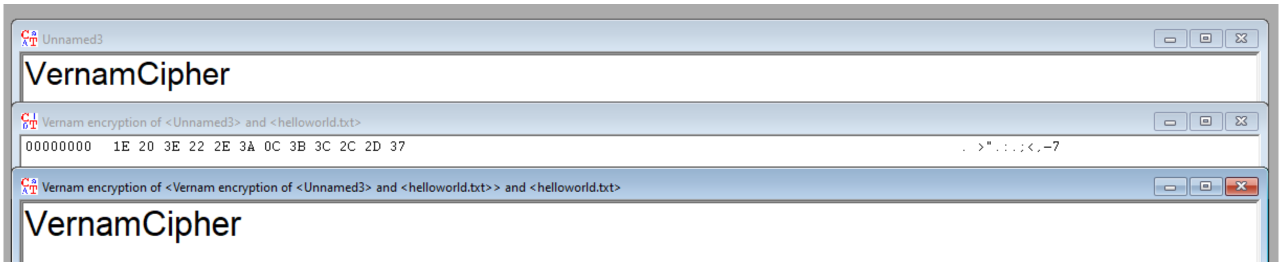
```
HELLOWORLD
```



Name	Date modified	Type
Today (1)		
helloworld	9/27/2024 1:36 PM	Text Document
Earlier this month (2)		
SE 22	9/9/2024 9:25 AM	File folder
Deep	9/3/2024 9:54 AM	File folder
Last month (1)		
.ipynb_checkpoints	8/8/2024 12:07 PM	File folder
Earlier this year (4)		
python	7/30/2024 1:44 PM	Text Document
DBMS	7/30/2024 10:13 AM	File folder

File name: helloworld

TEXT files (*.txt)



Unnamed3

VernamCipher

Vernam encryption of <Unnamed3> and <helloworld.txt>

```
00000000   1E 20 3E 22 2E 3A 0C 3B 3C 2C 2D 37        . >".:.;<,-7
```

Vernam encryption of <Vernam encryption of <Unnamed3> and <helloworld.txt>> and <helloworld.txt>

VernamCipher

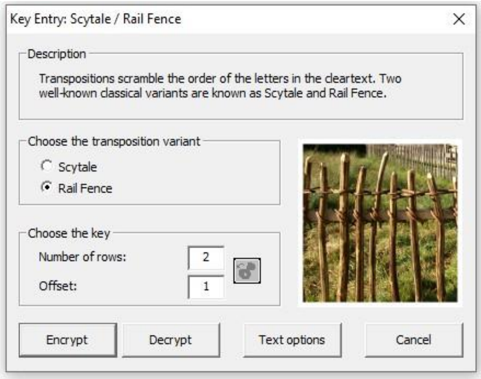
Transposition Cipher:

 In cryptography, a transposition cipher is a method of encryption which scrambles thepositions of characters (transposition) without changing the characters themselves.

Transposition ciphers reorder units of plaintext (typically characters or groups ofcharacters) according to a regular system to produce a ciphertext which is a permutation of the plaintext.

1) Rail Fence Transposition

The Rail Fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded. in the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we get tothe bottom. The message is then read off in rows.



Key Entry: Scytale / Rail Fence

Description

Transpositions scramble the order of the letters in the cleartext. Two well-known classical variants are known as Scytale and Rail Fence.

Choose the transposition variant

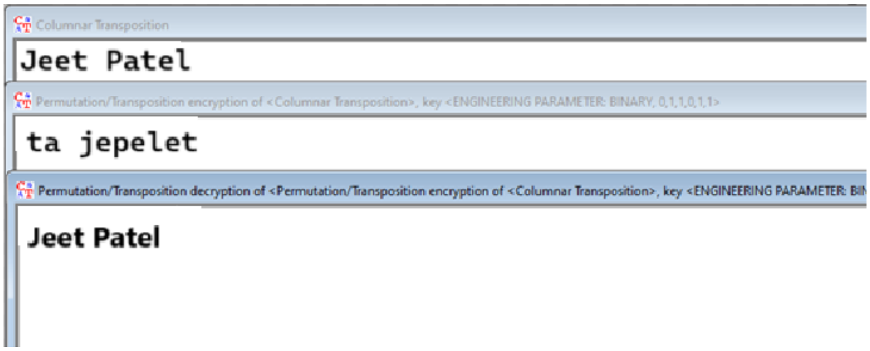
○ Scytale

● Rail Fence

Choose the key

Number of rows: 2

Offset: 1



Columnar Transposition

Jeet Patel

Permutation/Transposition encryption of <Columnar Transposition>, key <ENGINEERING PARAMETER: BINARY, 0,1,1,0,1,1>

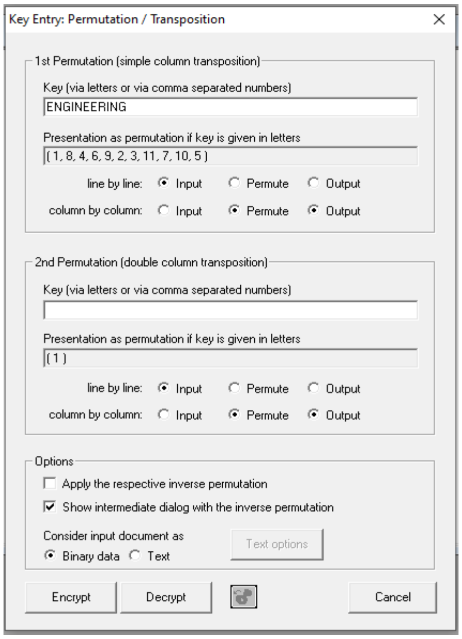
ta jepelet

Permutation/Transposition decryption of <Permutation/Transposition encryption of <Columnar Transposition>, key <ENGINEERING PARAMETER: BI

Jeet Patel

2) Columnar Transposition

- In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambledorder. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the keyword ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".



Key Entry: Permutation / Transposition

1st Permutation (simple column transposition)

Key (via letters or via comma separated numbers): ENGINEERING

Presentation as permutation if key is given in letters: (1, 8, 4, 6, 9, 2, 3, 11, 7, 10, 5)

line by line: ● Input ○ Permute ○ Output

column by column: ○ Input ● Permute ● Output

2nd Permutation (double column transposition)

Key (via letters or via comma separated numbers):

Presentation as permutation if key is given in letters: (1)

line by line: ● Input ○ Permute ○ Output

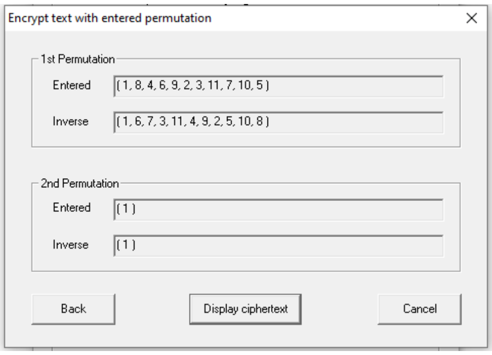
column by column: ○ Input ● Permute ● Output

Options

☐ Apply the respective inverse permutation

☑ Show intermediate dialog with the inverse permutation

Consider input document as ● Binary data ○ Text



Encrypt text with entered permutation

1st Permutation

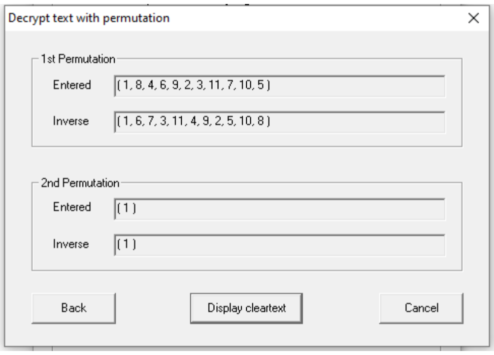
Entered: (1, 8, 4, 6, 9, 2, 3, 11, 7, 10, 5)

Inverse: (1, 6, 7, 3, 11, 4, 9, 2, 5, 10, 8)

2nd Permutation

Entered: (1)

Inverse: (1)



Decrypt text with permutation

1st Permutation

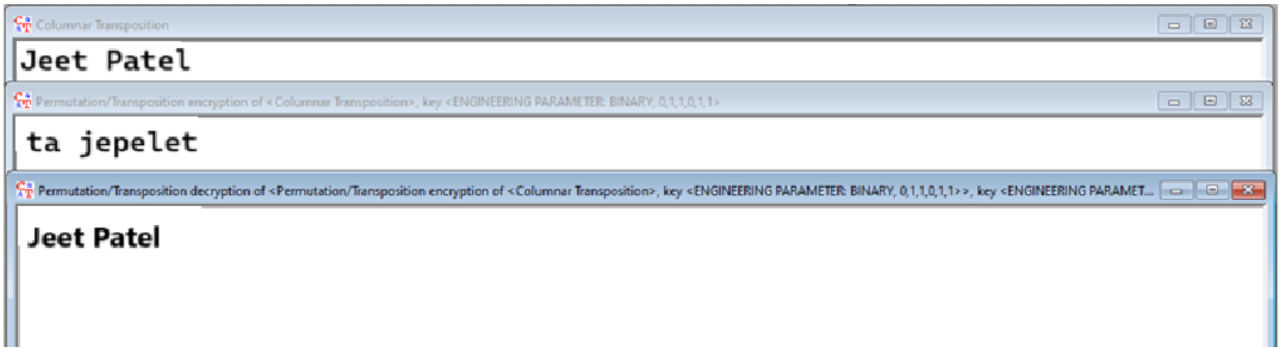
Entered: (1, 8, 4, 6, 9, 2, 3, 11, 7, 10, 5)

Inverse: (1, 6, 7, 3, 11, 4, 9, 2, 5, 10, 8)

2nd Permutation

Entered: (1)

Inverse: (1)



Columnar Transposition

```
Jeet Patel
```

Permutation/Transposition encryption of <Columnar Transposition>, key <ENGINEERING PARAMETER: BINARY, 0,1,1,0,1,1>

```
ta jepelet
```

Permutation/Transposition decryption of <Permutation/Transposition encryption of <Columnar Transposition>, key <ENGINEERING PARAMETER: BINARY, 0,1,1,0,1,1> >, key <ENGINEERING PARAMET...

```
Jeet Patel
```