Practical 12

# Aim: Perform various Encryption-Decryption Techniques with Cryptool.

**Cryptool:**

 CrypTool is an open-source project that is a free e-learning software for illustrating cryptographic and cryptanalytic concepts.

 CrypTool implements more than 400 algorithms. Users can adjust these with own parameters.

 CrypTool is used in schools, universities, companies and agencies for education and awareness 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). All others, JCrypTool (JCT) and CrypTool-Online (CTO), are available only in English and German.

# 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 crypto investments. The specific features and capabilities can vary depending on the version or developer of 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 and assets efficiently.
* **Transaction Monitoring**: It allows users to track and analyze transactions in real time.
* **Portfolio Analytics**: Users can monitor the performance of their cryptocurrency investments through 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 versatile management.
* **Security Features**: Emphasizes the security of user funds, often incorporating encryption and two-factor authentication.
* **Market Insights**: Provides market data and trends to help users make informed investment decisions.
* **Community Features**: May include forums or social features for users to share tips and strategies.
* **Customization**: Offers options to tailor the user experience to individual preferences.
* **Updates and Support**: Regular updates and customer support to address user needs and improve 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.

Algorithm for Substitution Cipher:

*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 on whether we’re encrypting or decrypting the text.

 Print the new string generated.

# Types:

1. **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 shift cipher or additive cipher.

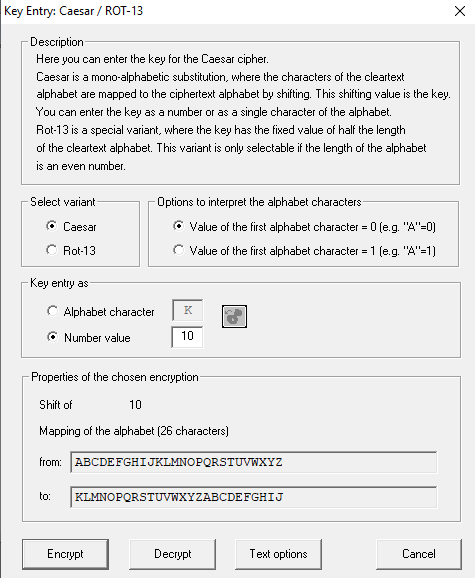
Julius Caesar used the shift cipher (additive cipher) technique to communicate with his officers.

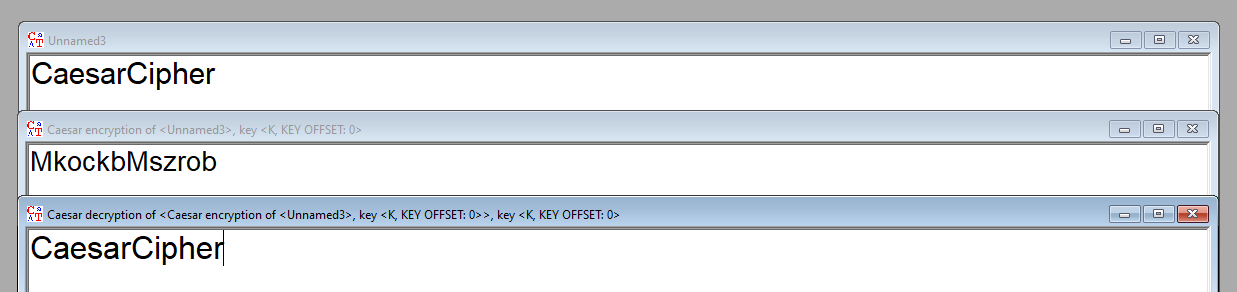
For this reason, the shift cipher technique is called the Caesar cipher. The Caesar cipher is a kind of replacement (substitution) cipher, where all letter of plain text is replaced by another letter.

The formula of encryption is: En (x) = (x + n) mod 26

The formula of decryption is: Dn (x) = (xi - n) mod 26

### Output:



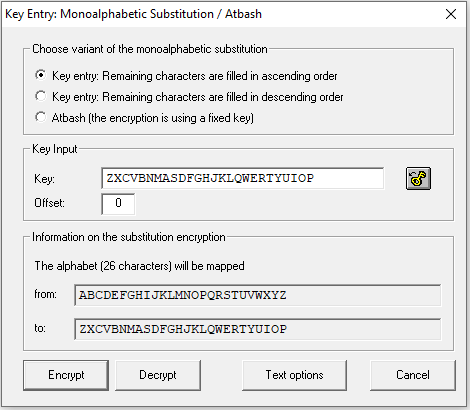


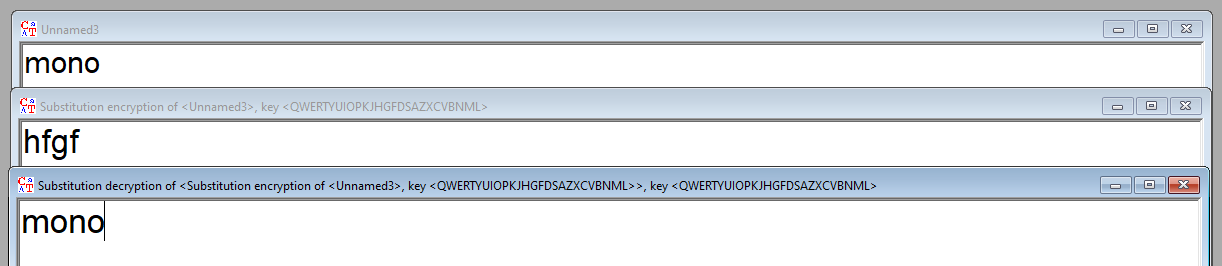
# Monoalphabatic

 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. It uses 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 both encrypt and decrypt a message.

## Output :





# Playfair Cipher

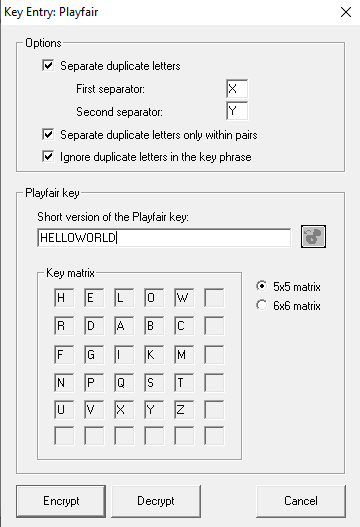
 The Playfair cipher encryption technique can be used to encrypt or encode a message. It operates exactly like typical encryption. The only difference is that it encrypts a digraph, or a pair of two letters, as opposed to a single letter.

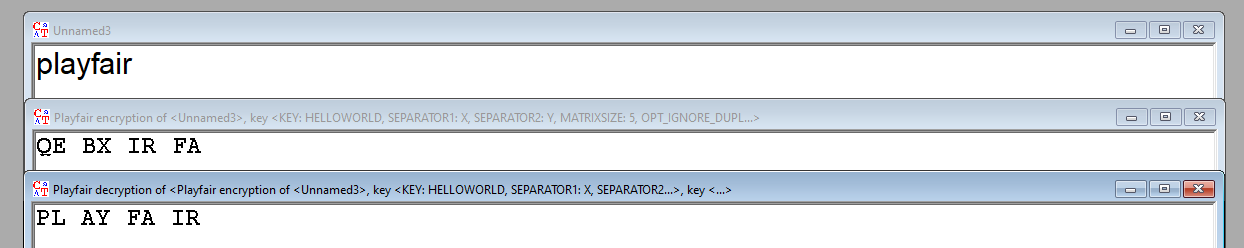
 An initial 5×5 matrix key table is created. The plaintext encryption key is made out of the matrix’s alphabetic characters. Be mindful that you shouldn’t repeat the letters.

There are 26 alphabets, however, there are only 25 spaces in which we can place a letter. 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 :



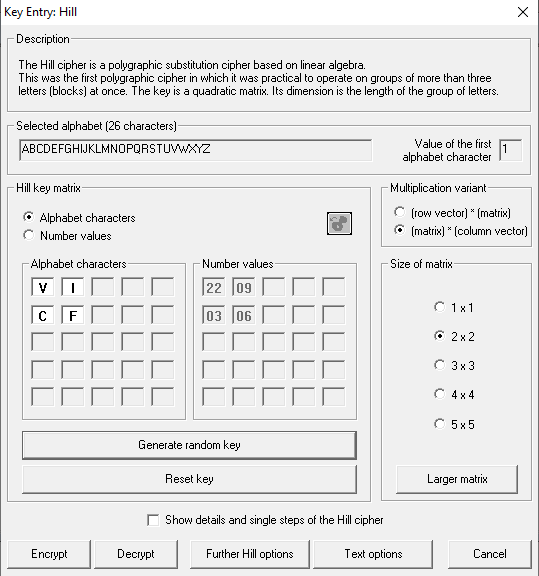
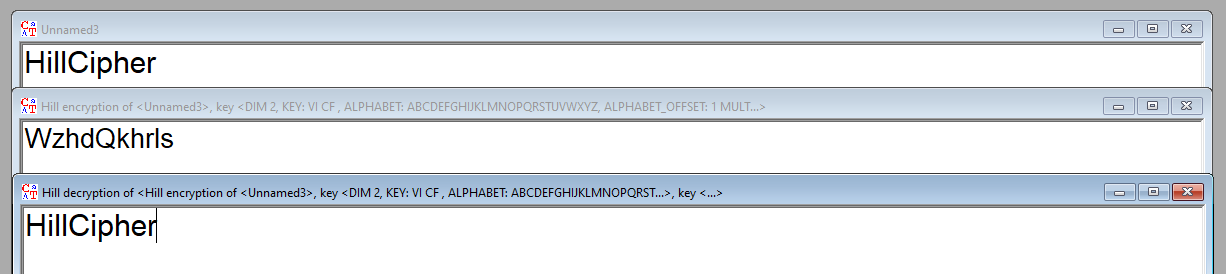


# Hill Cipher

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 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).

## Output :



# Polyalphabetic Cipher:

 A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered 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.

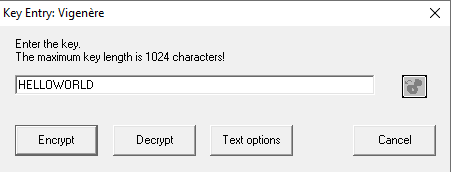
There are two types of it.

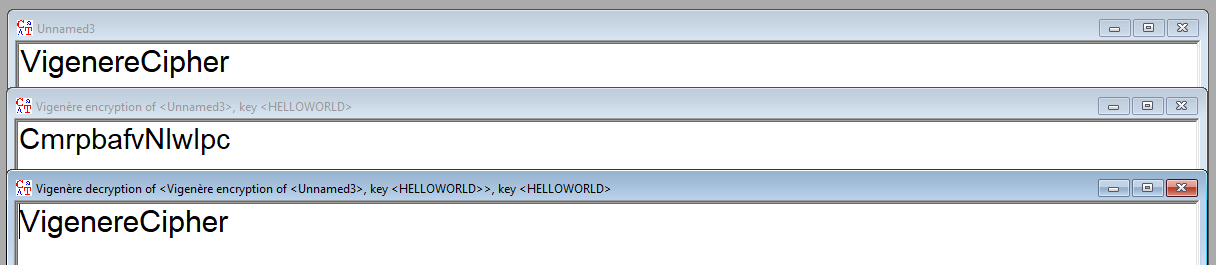
* 1. ***Vigenere Cipher***

 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 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.



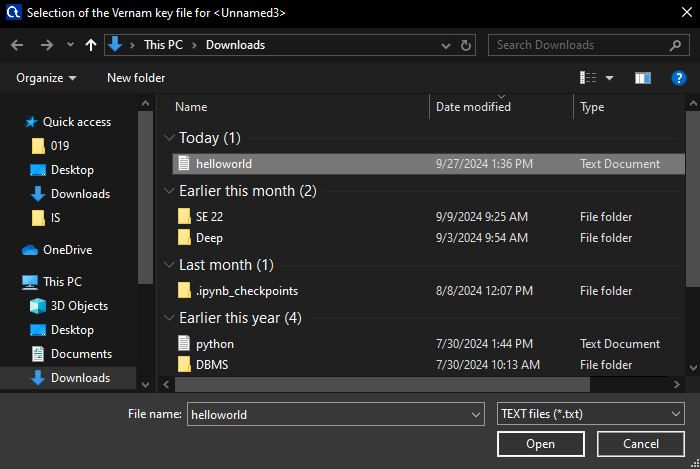


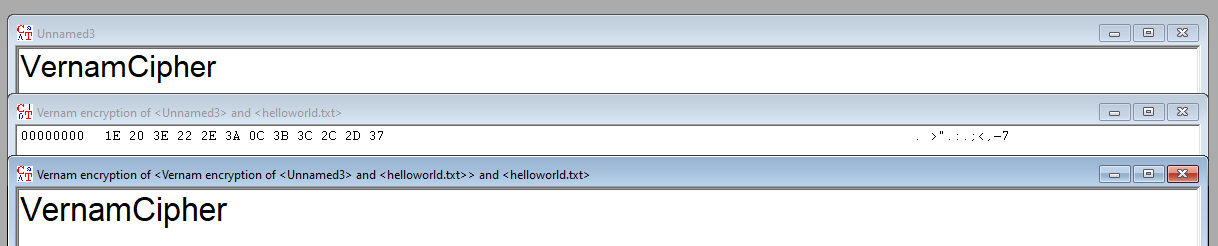
* 1. ***Vernam Cipher***

 Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques 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 the plain 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 to alphabetical order.
    2. Bitwise XOR both the number (Corresponding plain-text character number and Key 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.

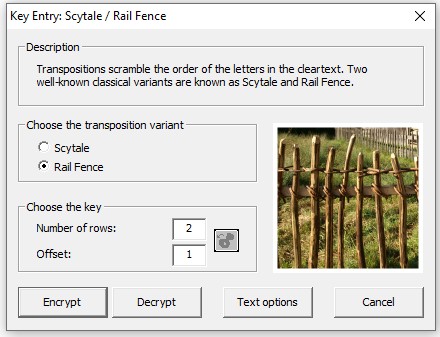
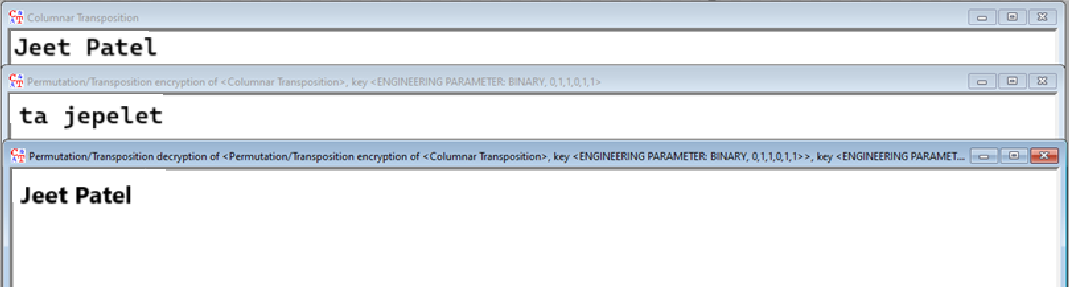


**Transposition Cipher:**

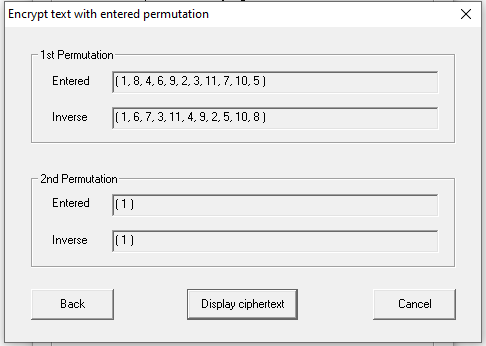
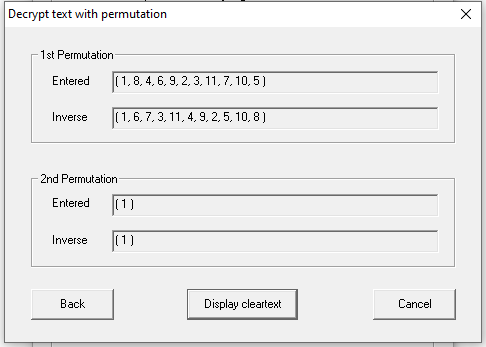
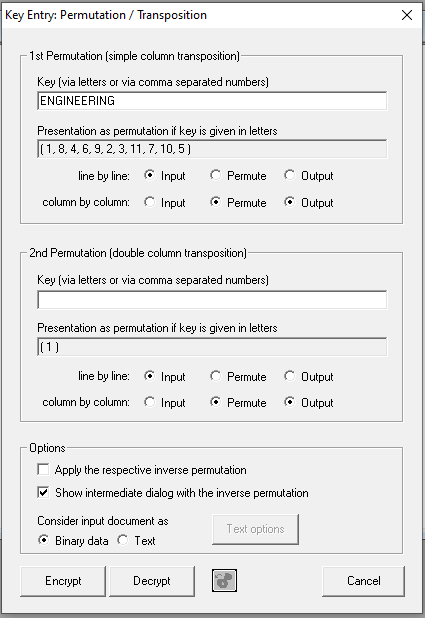
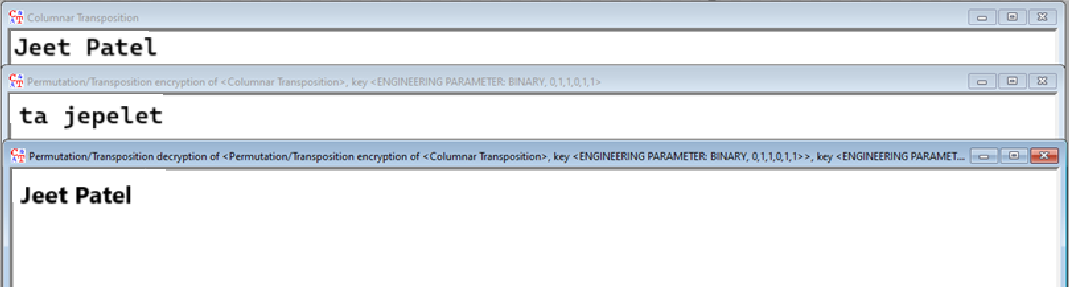
 In cryptography, a transposition cipher is a method of encryption which scrambles the positions of characters (transposition) without changing the characters themselves.

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

### 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 to the bottom. The message is then read off in rows.

### 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 scrambled order. 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".