**PRACTICAL: 11**

**AIM:** **Perform various Encryption-Decryption techniques with the Cryptool**.

**INTRODUCTION**:

* CrypTool is an [open source](https://findwords.info/term/open%20source) [e-learning](https://findwords.info/term/e-learning) tool illustrating cryptographic and cryptanalytic concepts.
* CrypTool implements more than 300 [algorithms](https://findwords.info/term/algorithm). Users can adjust these with own parameters.
* The graphical interface, online documentation, analytic tools and algorithms of CrypTool introduce users to the field of [cryptography](https://findwords.info/term/cryptography).
* Classical ciphers are available alongside asymmetric cryptography including RSA, elliptic curve cryptography, [digital signatures](https://findwords.info/term/digital%20signature), homomorphic encryption, and Diffie–Hellman key exchange, many of which are visualized by animations.
* CrypTool also contains some didactical games, and an animated tutorial about [primes](https://findwords.info/term/prime%20number) and elementary [number theory](https://findwords.info/term/number%20theory).

**Encryption – Decryption** :

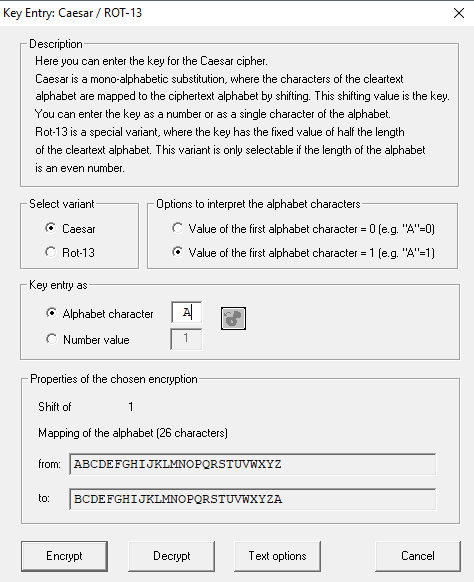
1. **Caesar Cipher**

* The Caesar cipheris named so, as it was first implemented by Julius Caesar. It also goes by the name of shift cipher and belongs to the family of substitution ciphers. With this cipher each character is represented by another character in the alphabet, more specifically the whole alphabet is shifted by a set amount to encrypt the data.
* The set amount that the alphabet is shifted by becomes the key, anyone with knowledge of this key should be able to reveal the true contents of the ciphertext and Cryptographic Techniques for Network Security -25- conversely anyone without knowledge of the key should not be able to interpret the ciphertext as the original plaintext.

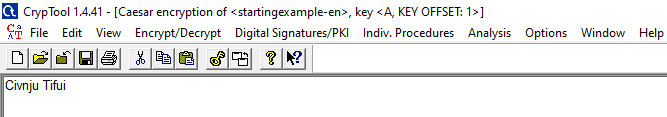
Encryption:



* Open a new cryptool file for the plaintext, Choose Encrypt/Decrypt/Symmetric (classic)/Caesar/Rot-13/

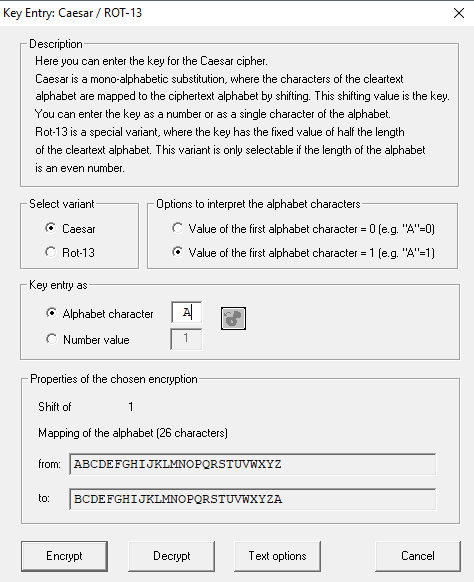


* Then apply the type of encryption to perform on plaintext. And click the Encrypt button.

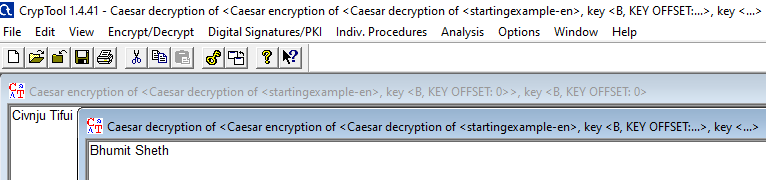


Decryption:

* Open a new cryptool file for the ciphertext, Choose Encrypt/Decrypt/Symmetric (classic)/Caesar/Rot-13/



* After applying the type of decryption, click the Decrypt button.

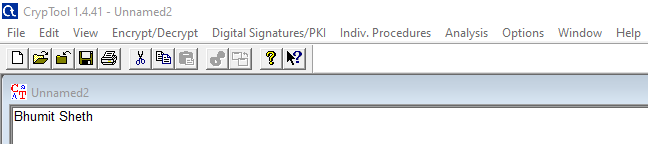


1. **Vigenere Cipher**

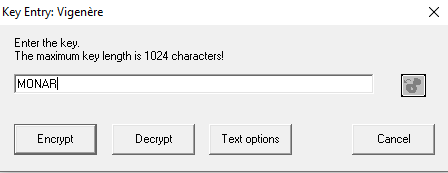
* The Vigenère cipher bares much resemblance to the Modified Caesar cipher, discussed above, but using a key phrase instead of the numbers in the shift vector. The encryption process for this cipher takes each individual letter of a plaintext message and combines it with a letter from the key, together these two letters act as coordinates for a position on the Vigenère squareTo decipher a message, reverse the process, starting by finding the character of the key, and then find the ciphertext letter along the same row and then find what column it is on to reveal the plaintext.

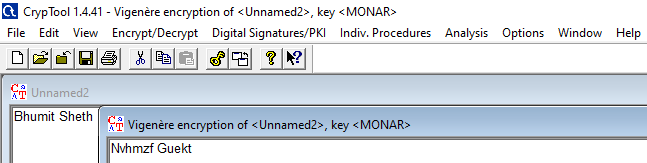
Encryption:

* Open a new cryptool file for the plaintext, Choose Encrypt/Decrypt/Symmetric (classic)/Vignere/



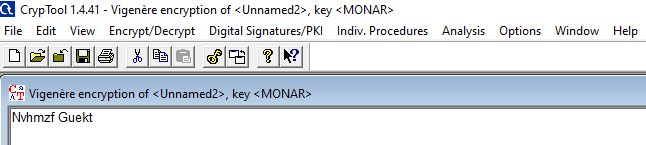
* Enter the key for the encryption, Then click the Encrypt button.



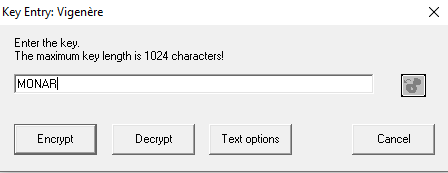
.

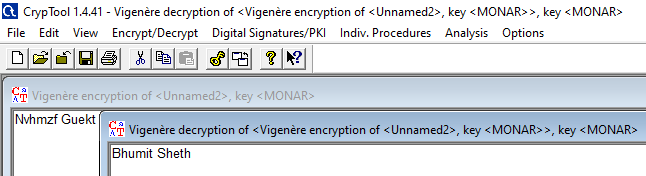
Decryption:

* Open a new cryptool file for the cipherntext, Choose Encrypt/Decrypt/Symmetric (classic)/Vignere/



* Enter the key for the decryption, Then click the Decrypt button.



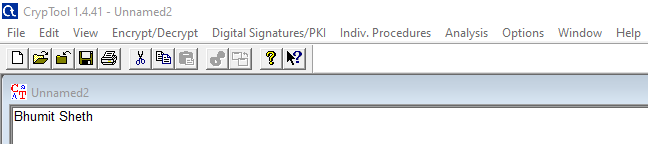


1. **Playfair Cipher**

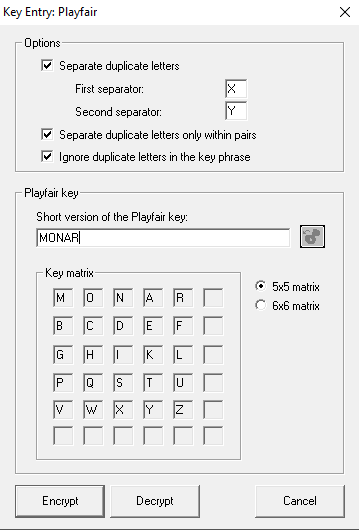
* The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.
* It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

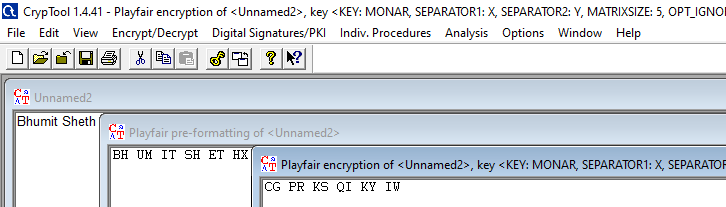
Encryption:

* Open a new cryptool file for the plaintext, Choose Encrypt/Decrypt/Symmetric (classic)/Playfair



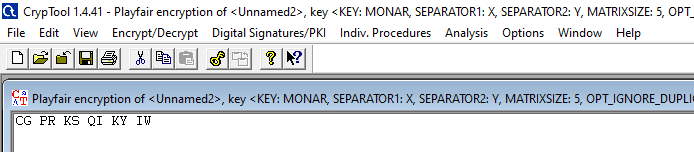
* Enter the key for the encryption, Then click the Encrypt button.





Decryption:

* Open a new cryptool file for the cipherntext, Choose Encrypt/Decrypt/Symmetric (classic)/Playfair



* Enter the key for the decryption, Then click the Decrypt button.

