PRACTICAL: 11

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

INTRODUCTION:

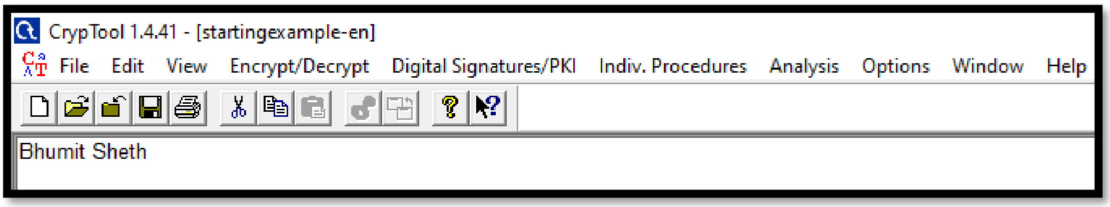
- CrypTool is an open source e-learning tool illustrating cryptographic and cryptanalytic concepts.
- CrypTool implements more than 300 algorithms. Users can adjust these with own parameters.
- The graphical interface, online documentation, analytic tools and algorithms of CrypTool introduce users to the field of cryptography.
- Classical ciphers are available alongside asymmetric cryptography including RSA, elliptic curve cryptography, digital signatures, 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 and elementary number theory.

Encryption – Decryption :

1. Caesar Cipher

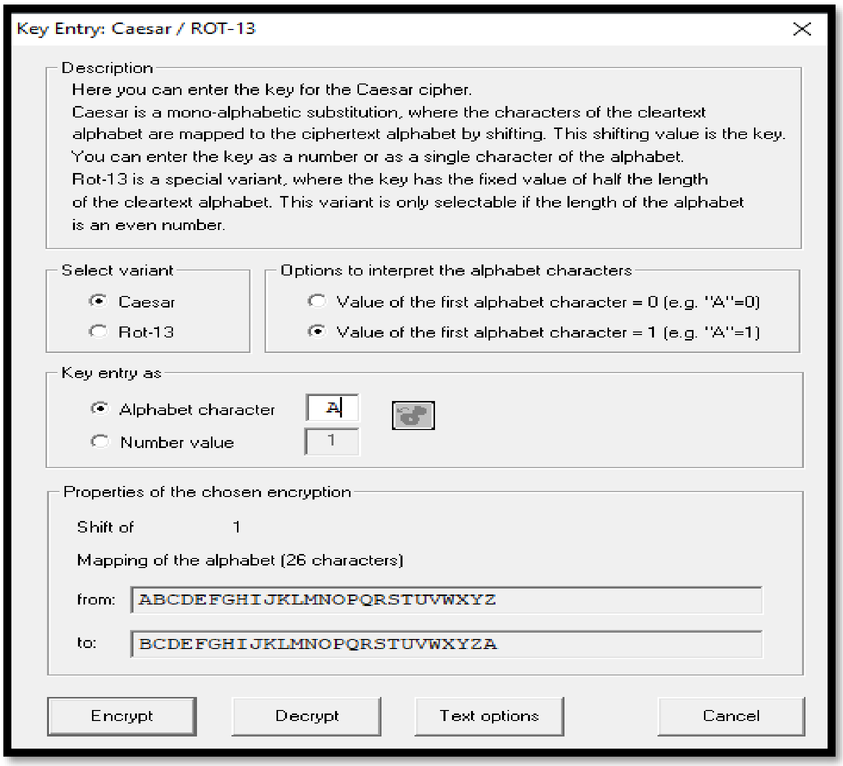
- The Caesar cipher is named so, as it was first implemented by Julius Caesar. It also goes by the name of shift cipher and belongs to the family of substitution ciphers. With this cipher each character is represented by another character in the alphabet, more specifically the whole alphabet is shifted 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:



Bhumit Sheth

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



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.

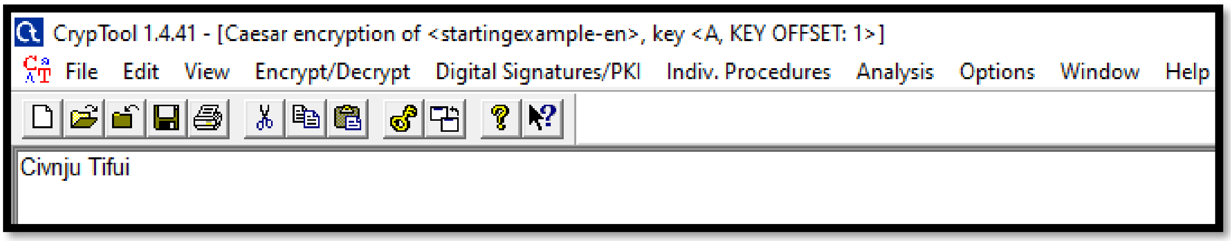
Select variant
● Caesar
○ Rot-13

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: A
○ Number value: 1

Properties of the chosen encryption
Shift of 1
Mapping of the alphabet (26 characters)
from: ABCDEFGHIJKLMNOPQRSTUVWXYZ
to: BCDEFGHIJKLMNOPQRSTUVWXYZA

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

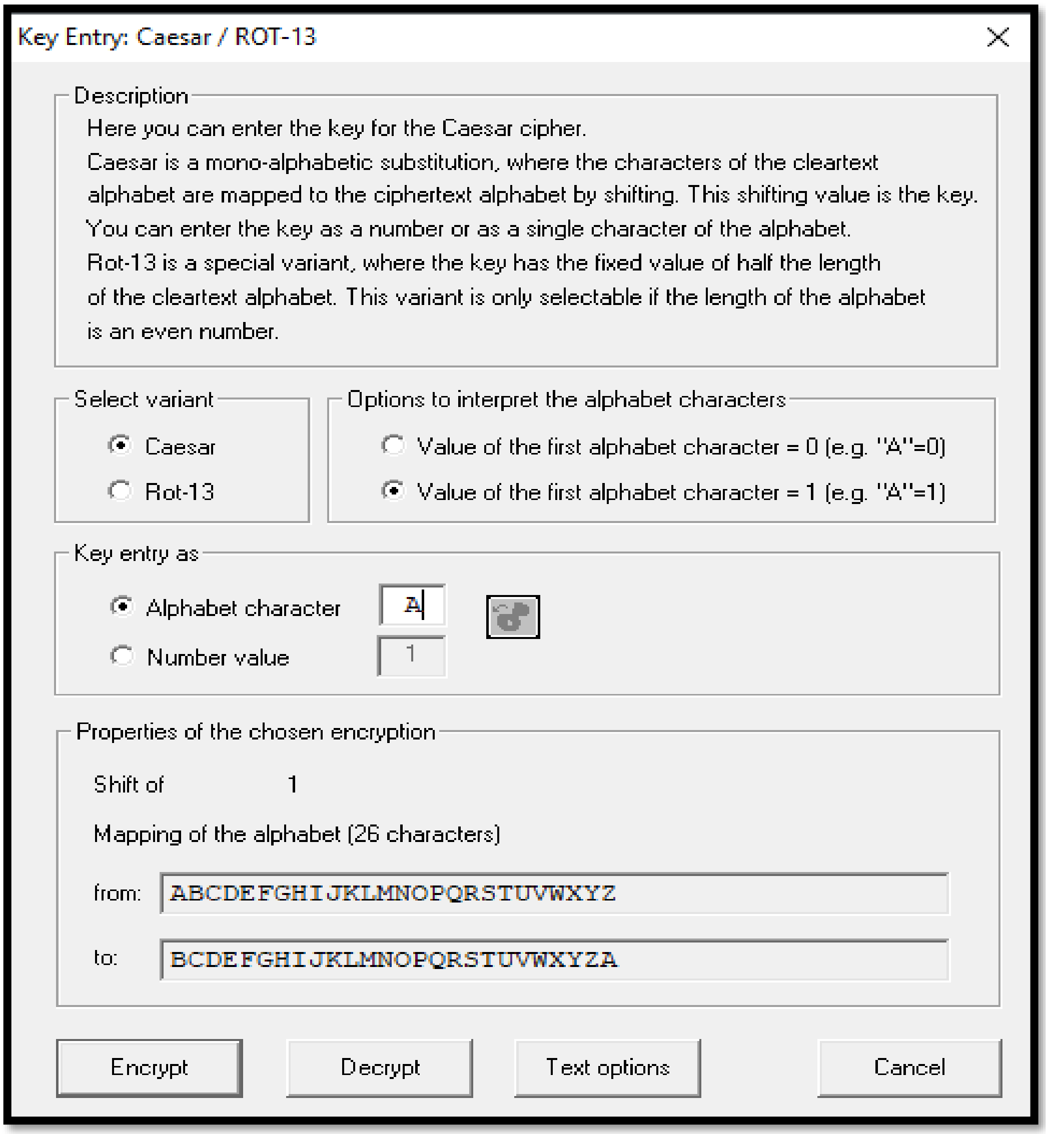


CrypTool 1.4.41 - [Caesar encryption of <startingexample-en>, key <A, KEY OFFSET: 1>]

Civnju Tifui

Decryption:

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



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: A
○ Number value: 1

Properties of the chosen encryption

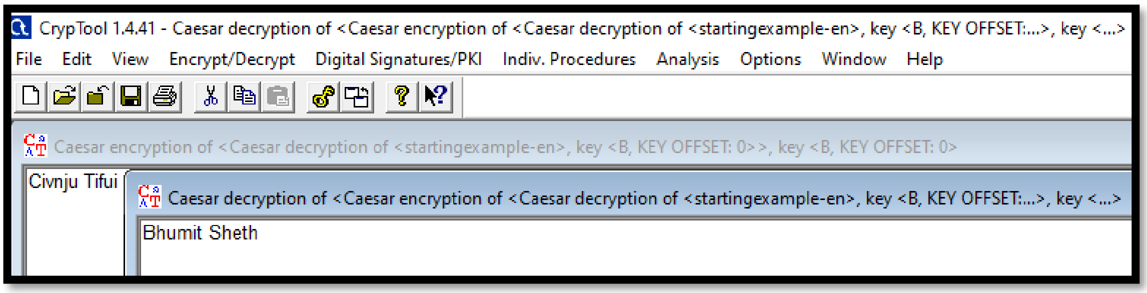
Shift of 1

Mapping of the alphabet (26 characters)

from: ABCDEFGHIJKLMNOPQRSTUVWXYZ

to: BCDEFGHIJKLMNOPQRSTUVWXYZA

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



CrypTool 1.4.41 - Caesar decryption of <Caesar encryption of <Caesar decryption of <startingexample-en>, key <B, KEY OFFSET:...>, key <...>

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

Caesar encryption of <Caesar decryption of <startingexample-en>, key <B, KEY OFFSET: 0>>, key <B, KEY OFFSET: 0>

Civnju Tifui

Caesar decryption of <Caesar encryption of <Caesar decryption of <startingexample-en>, key <B, KEY OFFSET:...>, key <...>

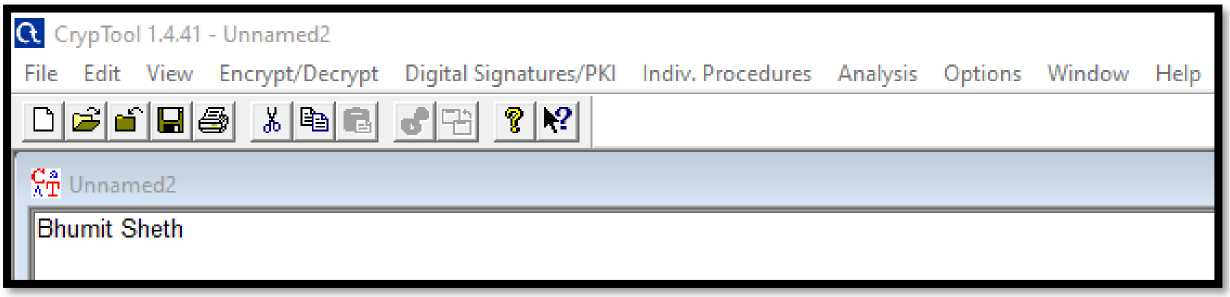
Bhumit Sheth

2. 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.

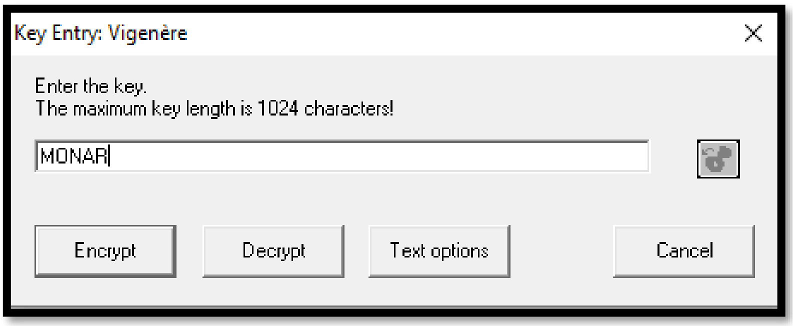
Encryption:

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


CrypTool 1.4.41 - Unnamed2
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2

Bhumit Sheth

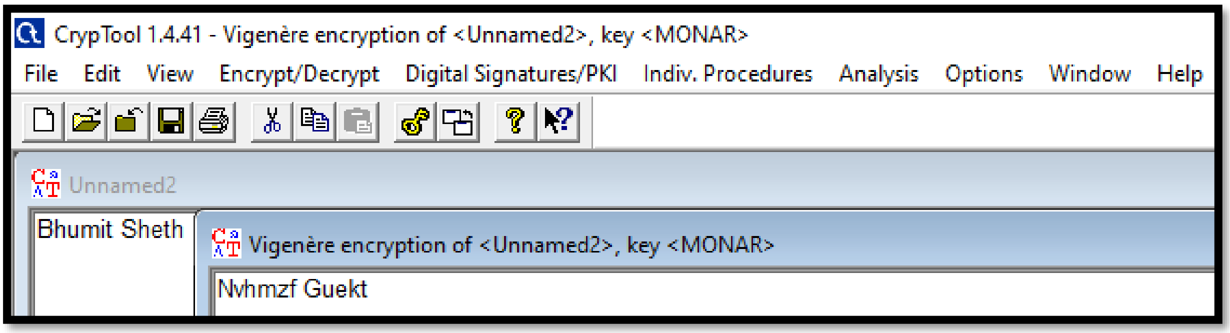
- Enter the key for the encryption, Then click the Encrypt button.



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

MONAR

.

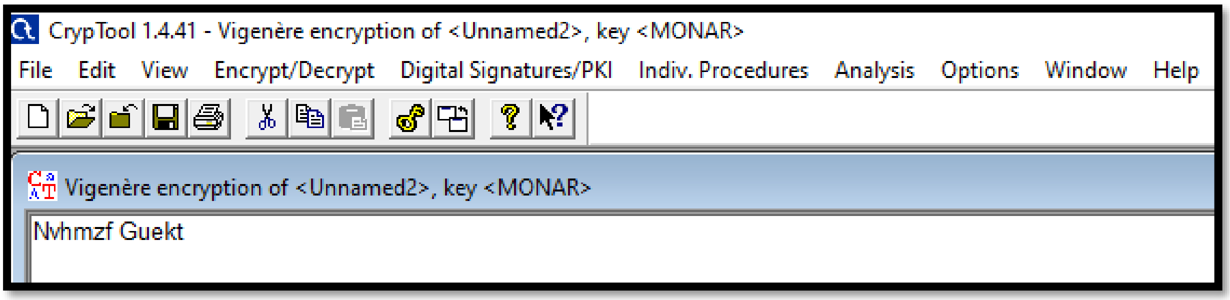

CrypTool 1.4.41 - Vigenère encryption of <Unnamed2>, key <MONAR>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2
Vigenère encryption of <Unnamed2>, key <MONAR>

Bhumit Sheth

Nvhmzf Guekt

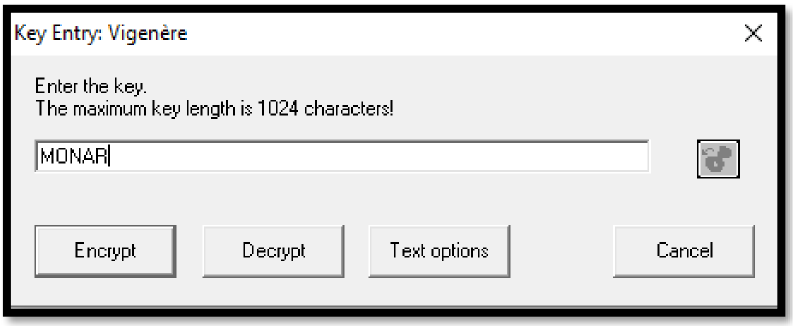
Decryption:

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


CrypTool 1.4.41 - Vigenère encryption of <Unnamed2>, key <MONAR>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Vigenère encryption of <Unnamed2>, key <MONAR>

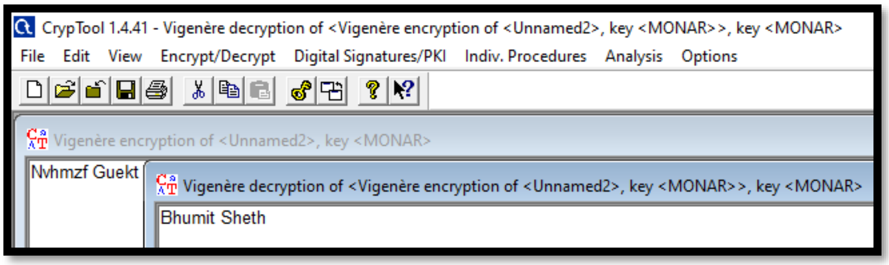
Nvhmzf Guekt

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



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

MONAR


CrypTool 1.4.41 - Vigenère decryption of <Vigenère encryption of <Unnamed2>, key <MONAR>>, key <MONAR>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options
Vigenère encryption of <Unnamed2>, key <MONAR>
Vigenère decryption of <Vigenère encryption of <Unnamed2>, key <MONAR>>, key <MONAR>

Nvhmzf Guekt

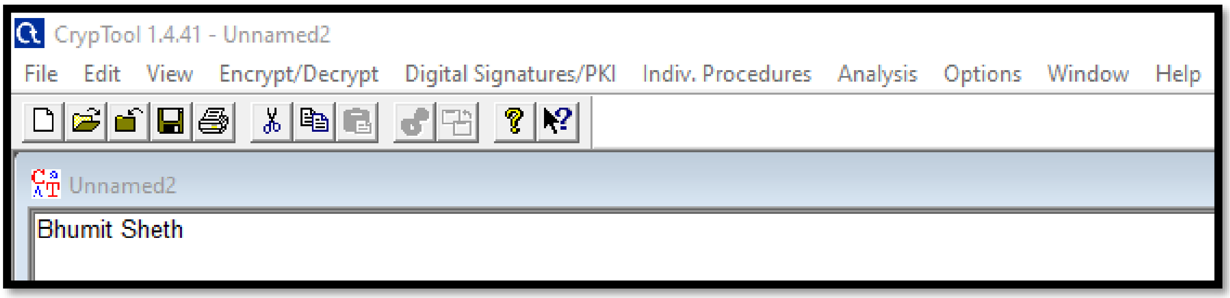
Bhumit Sheth

3. 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.

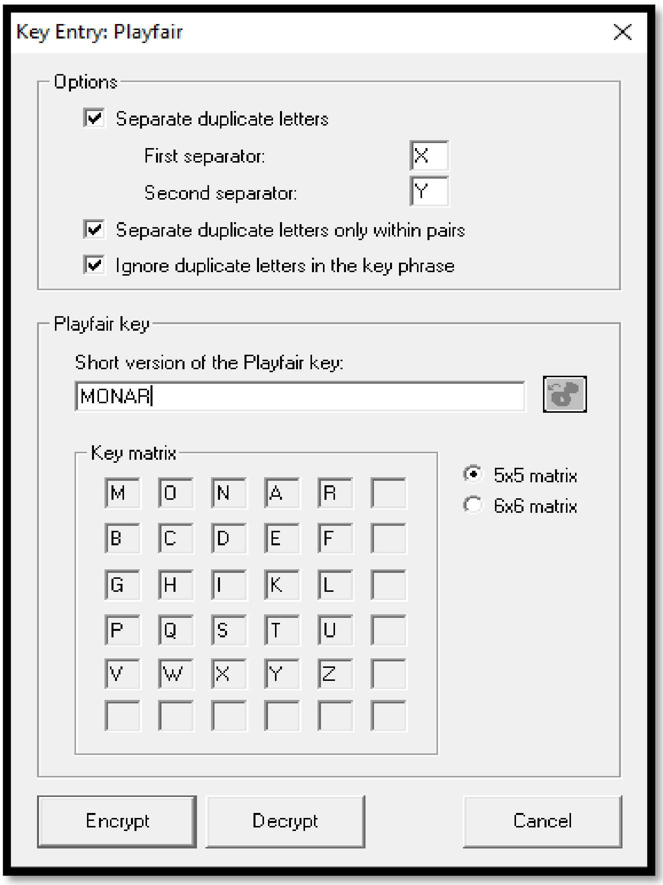
Encryption:

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


CrypTool 1.4.41 - Unnamed2
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2

Bhumit Sheth

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



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

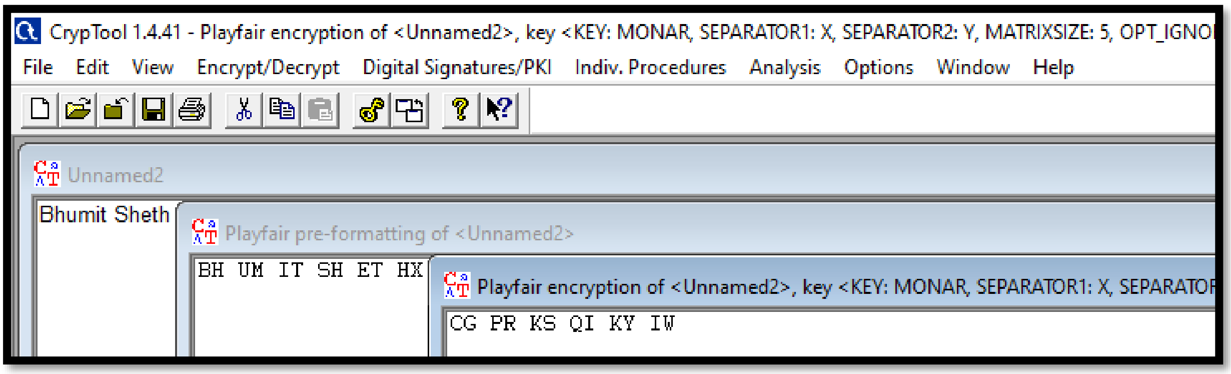
Playfair key

Short version of the Playfair key: MONAR

Key matrix

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

● 5x5 matrix
○ 6x6 matrix



CrypTool 1.4.41 - Playfair encryption of <Unnamed2>, key <KEY: MONAR, SEPARATOR1: X, SEPARATOR2: Y, MATRIXSIZE: 5, OPT_IGNO

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

Unnamed2

```
Bhumit Sheth
```

Playfair pre-formatting of <Unnamed2>

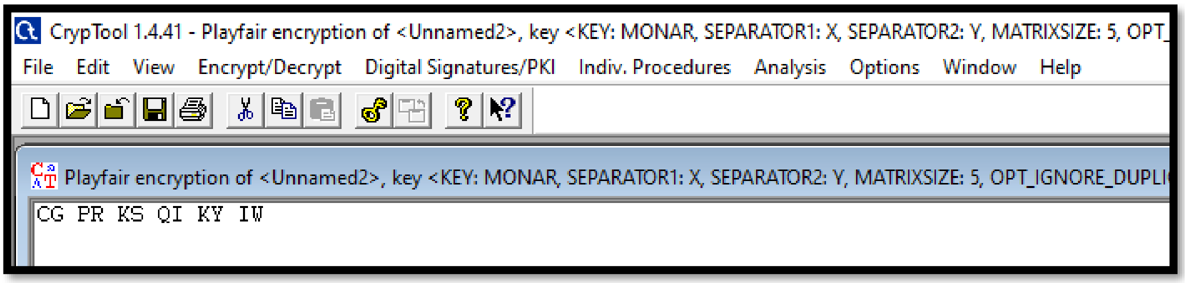
```
BH UM IT SH ET HX
```

Playfair encryption of <Unnamed2>, key <KEY: MONAR, SEPARATOR1: X, SEPARATOF

```
CG PR KS QI KY IW
```

Decryption:

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



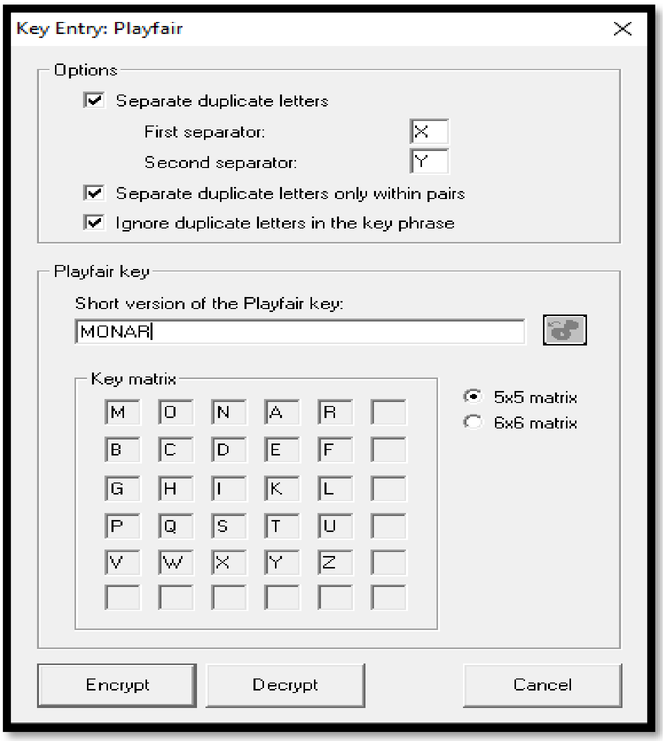
CrypTool 1.4.41 - Playfair encryption of <Unnamed2>, key <KEY: MONAR, SEPARATOR1: X, SEPARATOR2: Y, MATRIXSIZE: 5, OPT_

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

Playfair encryption of <Unnamed2>, key <KEY: MONAR, SEPARATOR1: X, SEPARATOR2: Y, MATRIXSIZE: 5, OPT_IGNORE_DUPLI

```
CG PR KS QI KY IW
```

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



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

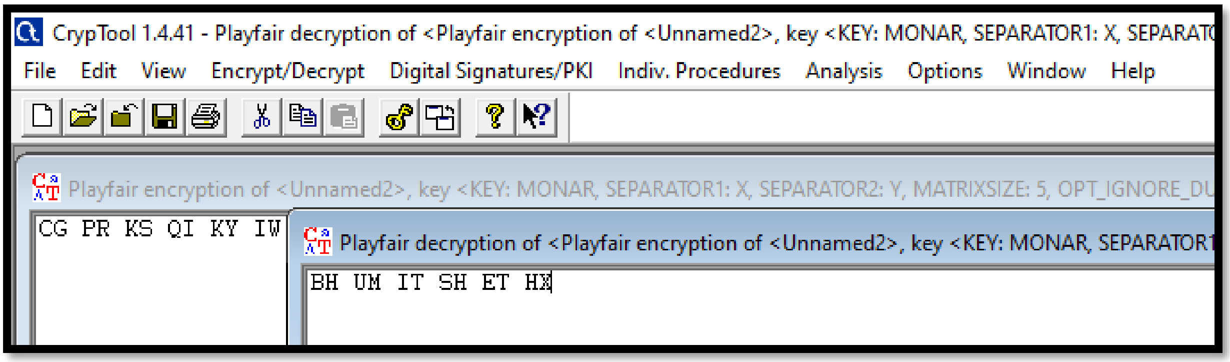
Playfair key

Short version of the Playfair key: MONAR

Key matrix

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

● 5x5 matrix
○ 6x6 matrix



CrypTool 1.4.41 - Playfair decryption of <Playfair encryption of <Unnamed2>, key <KEY: MONAR, SEPARATOR1: X, SEPARATO

Playfair encryption of <Unnamed2>, key <KEY: MONAR, SEPARATOR1: X, SEPARATOR2: Y, MATRIXSIZE: 5, OPT_IGNORE_DU

```
CG PR KS QI KY IW
```

Playfair decryption of <Playfair encryption of <Unnamed2>, key <KEY: MONAR, SEPARATOR1

```
BH UM IT SH ET HX
```