

CrypTool 1.4.42 - Unnamed1

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



Unnamed1

Hello Good Morning

CT Unnamed1

Hello Good Morning

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

☐ Number value

19

Properties of the chosen encryption

Shift of

19

Mapping of the alphabet (26 characters)

from:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

to:

TUVWXYZABCDEFGHIJKLMNOPS

Encrypt

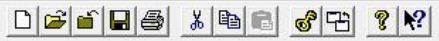
Decrypt

Text options

Cancel

CrypTool 1.4.42 - Caesar encryption of <Unnamed1>, key <T, KEY OFFSET: 0>

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

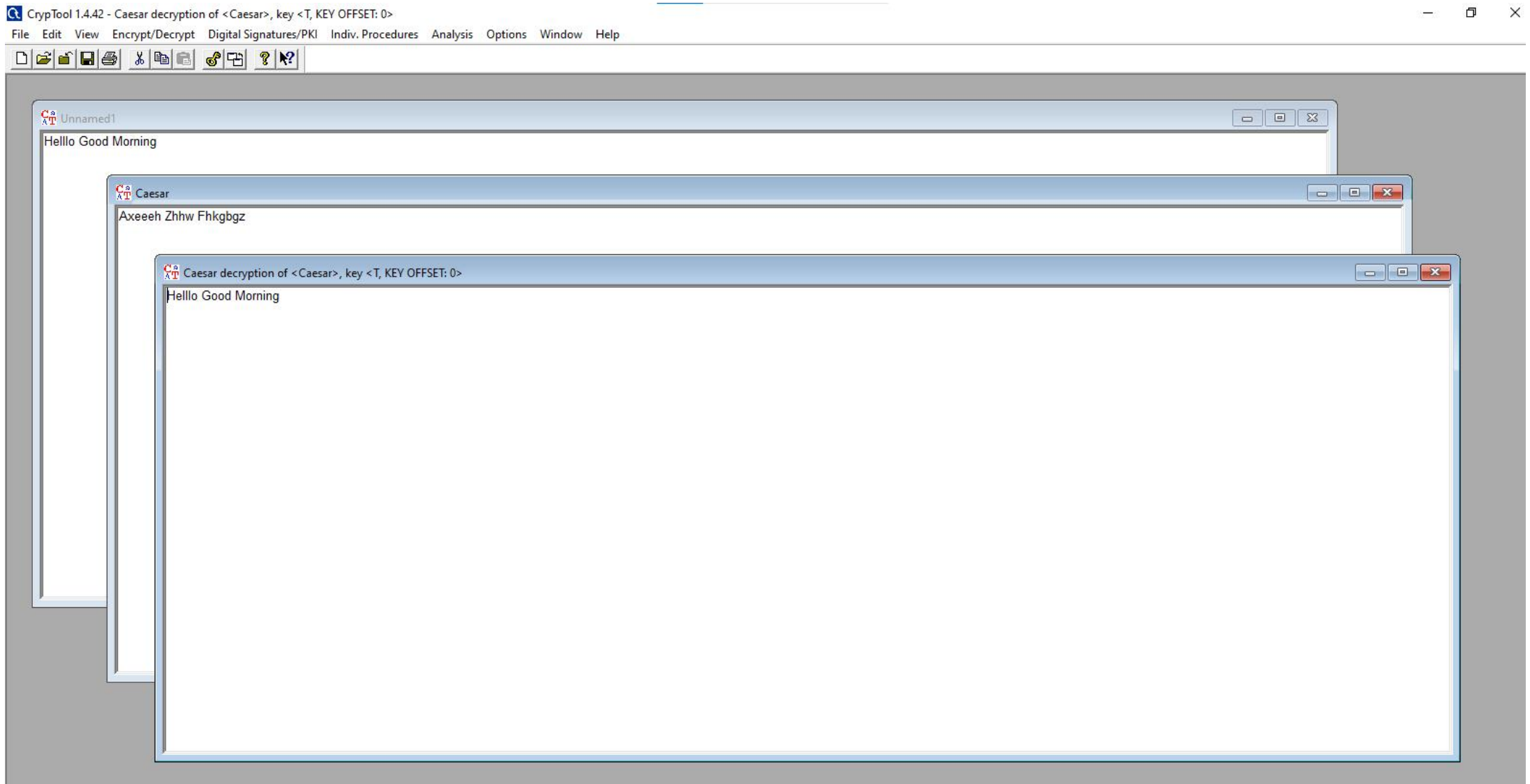


Ca Unnamed1

Hello Good Morning

Ca Caesar encryption of <Unnamed1>, key <T, KEY OFFSET: 0>

Axeeeh Zhhw Fhkgbgz





Unnamed1

Hello Good Morning

Key Entry: Vigenère

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

WHITE

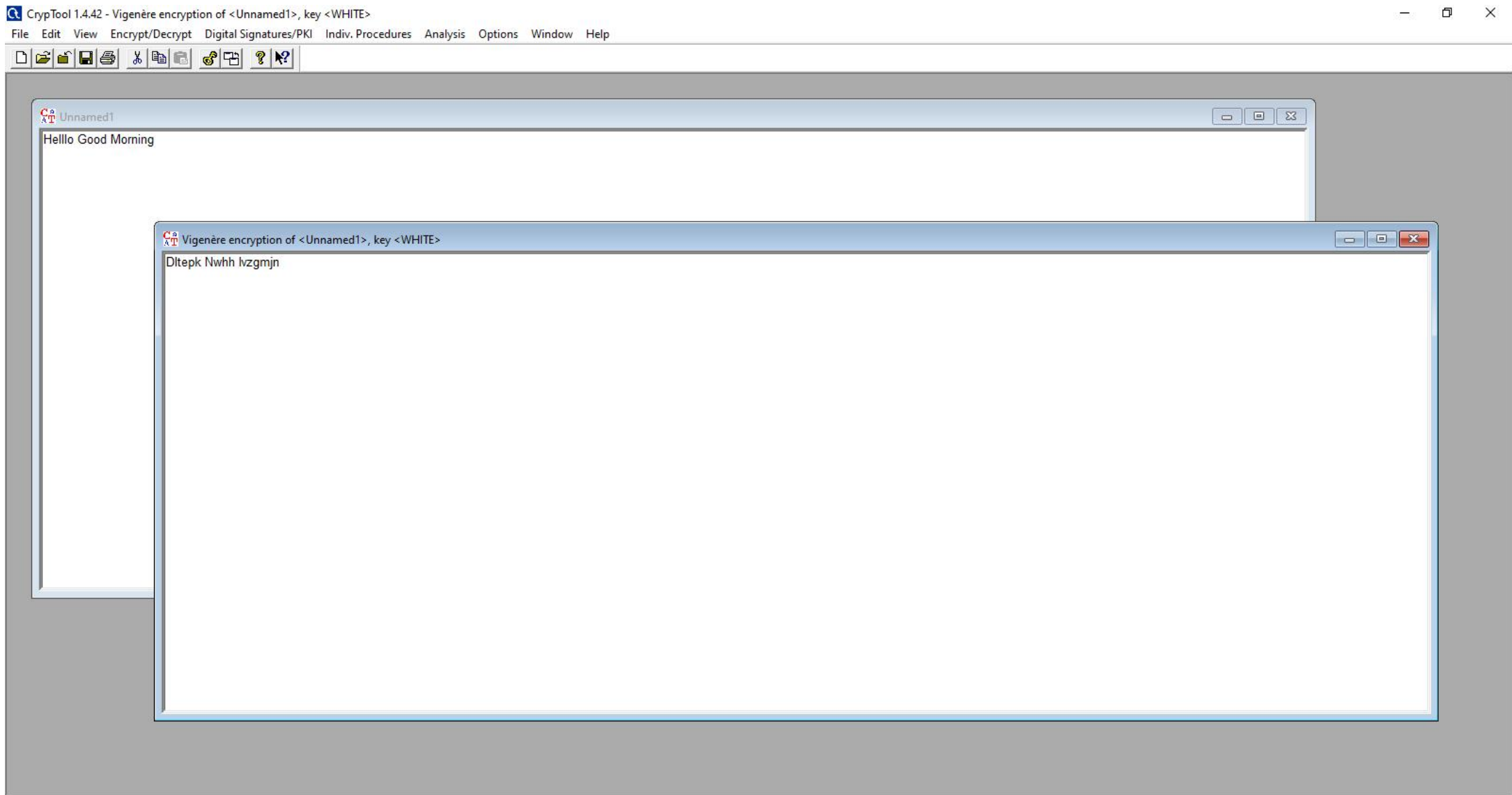


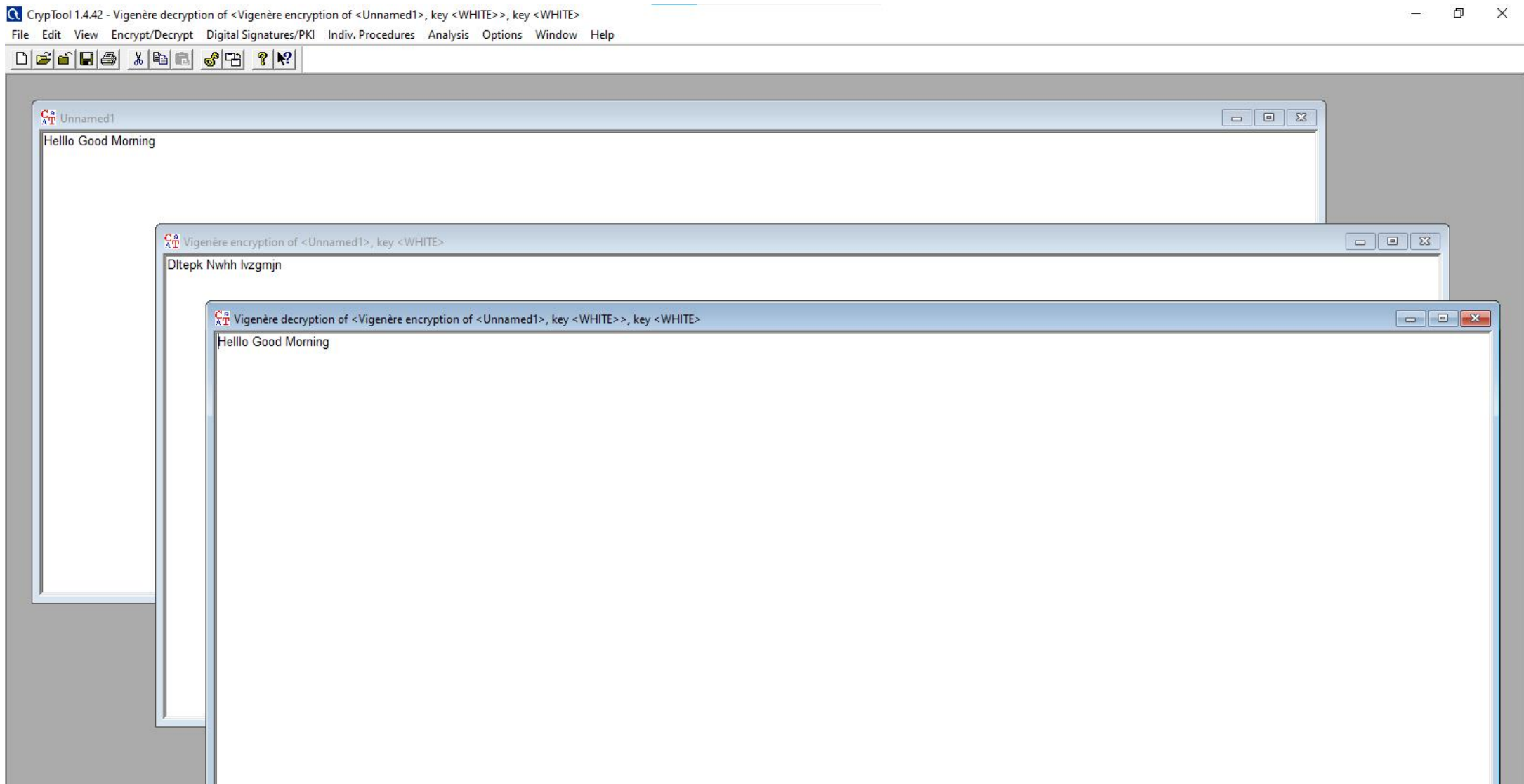
Encrypt

Decrypt

Text options

Cancel







CrypTool Unnamed1

Hello Good Morning

CrypTool Hill encryption of <Unnamed1>, key <DIM 2, KEY: AF FF, ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFFSET: 0 MULT...>

Ymhpwe Wftq Wjdrkzl

CrypTool Details of Hill encryption of <Unnamed1>, key <DIM 2, KEY: AF FF, ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFF...>

Hill En-/Decryption:

This detailed description of the Hill encryption / decryption consists of the following parts:

1. Encoding the alphabet characters to numbers
2. Encryption parameters and properties
3. Hill encryption
4. Hill decryption

This log file text shows all calculations done with the current Hill key matrix and the beginning characters of the used message.

1. Encoding the Alphabet Characters to Numbers

The actually selected alphabet and it's encoding to numbers as of Menu "Options / Textoptions" is:

A --> 01	H --> 08	O --> 15	U --> 21
B --> 02	I --> 09	P --> 16	V --> 22
C --> 03	J --> 10	Q --> 17	W --> 23
D --> 04	K --> 11	R --> 18	X --> 24
E --> 05	L --> 12	S --> 19	Y --> 25
F --> 06	M --> 13	T --> 20	Z --> 26
G --> 07	N --> 14		

The actual alphabet consists of 26 characters. The first alphabet character is encoded to the number 1.

2. Encryption Parameters and Properties

This example describes the Hill encryption of the 2 first characters of the input plaintext. Only characters from the current alphabet are encrypted.

Here are the required parameter information for the selected Hill encryption:

- o For the Hill encryption and decryption the Hill matrix is multiplied by a column vector from right.
- o The selected Hill matrix is of dimension 2x2.
- o The plaintext consists of 0 characters. Thereof are 0 non-alphabet characters (non-alphabet characters are ignored.) In case the selected alphabet consists only of capital characters non capital characters are encrypted too but this is not true for the other direction. Below the Hill encryption and decryption is demonstrated on the example of the 2 first alphabet characters from the given plaintext.