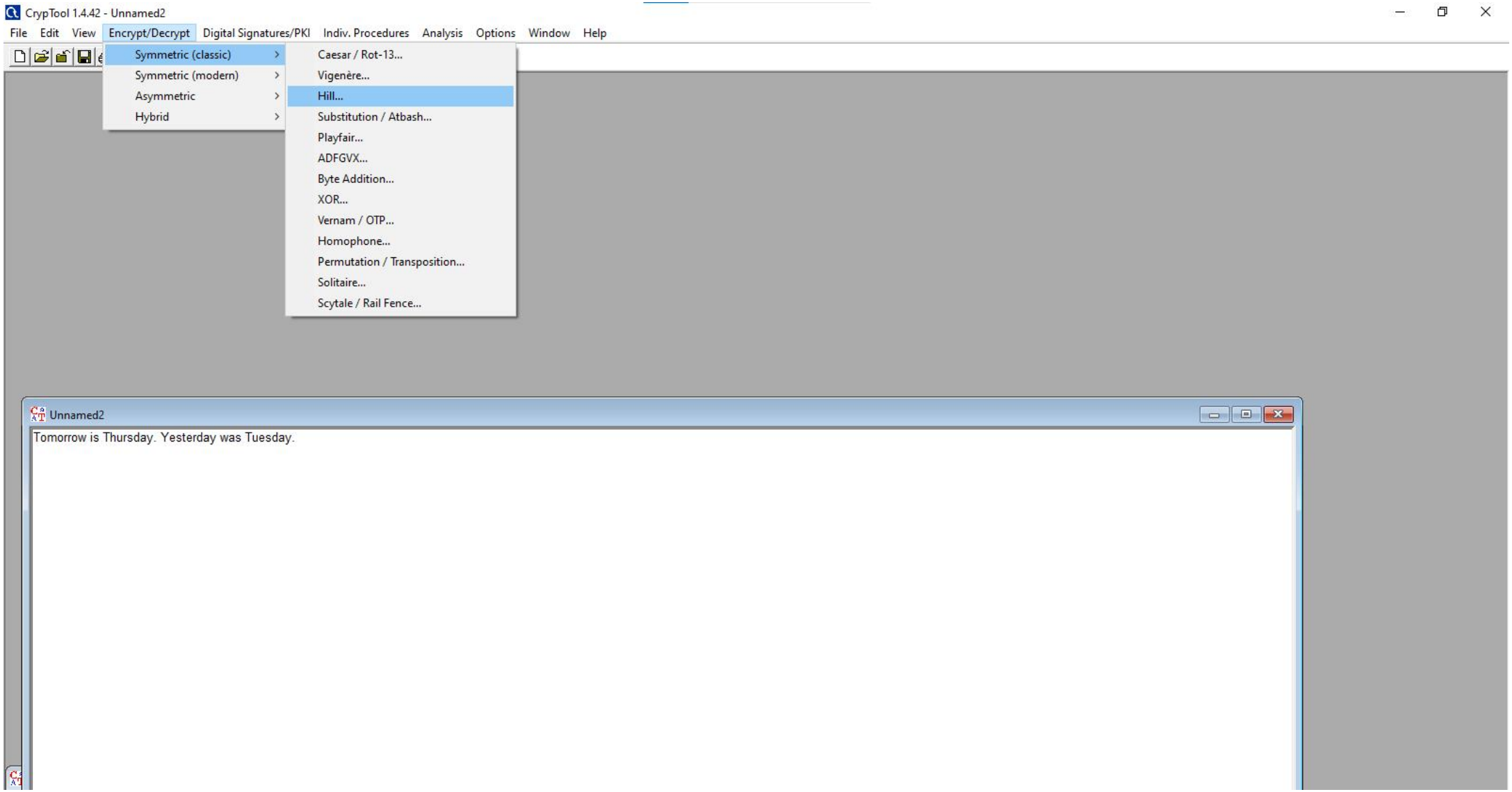
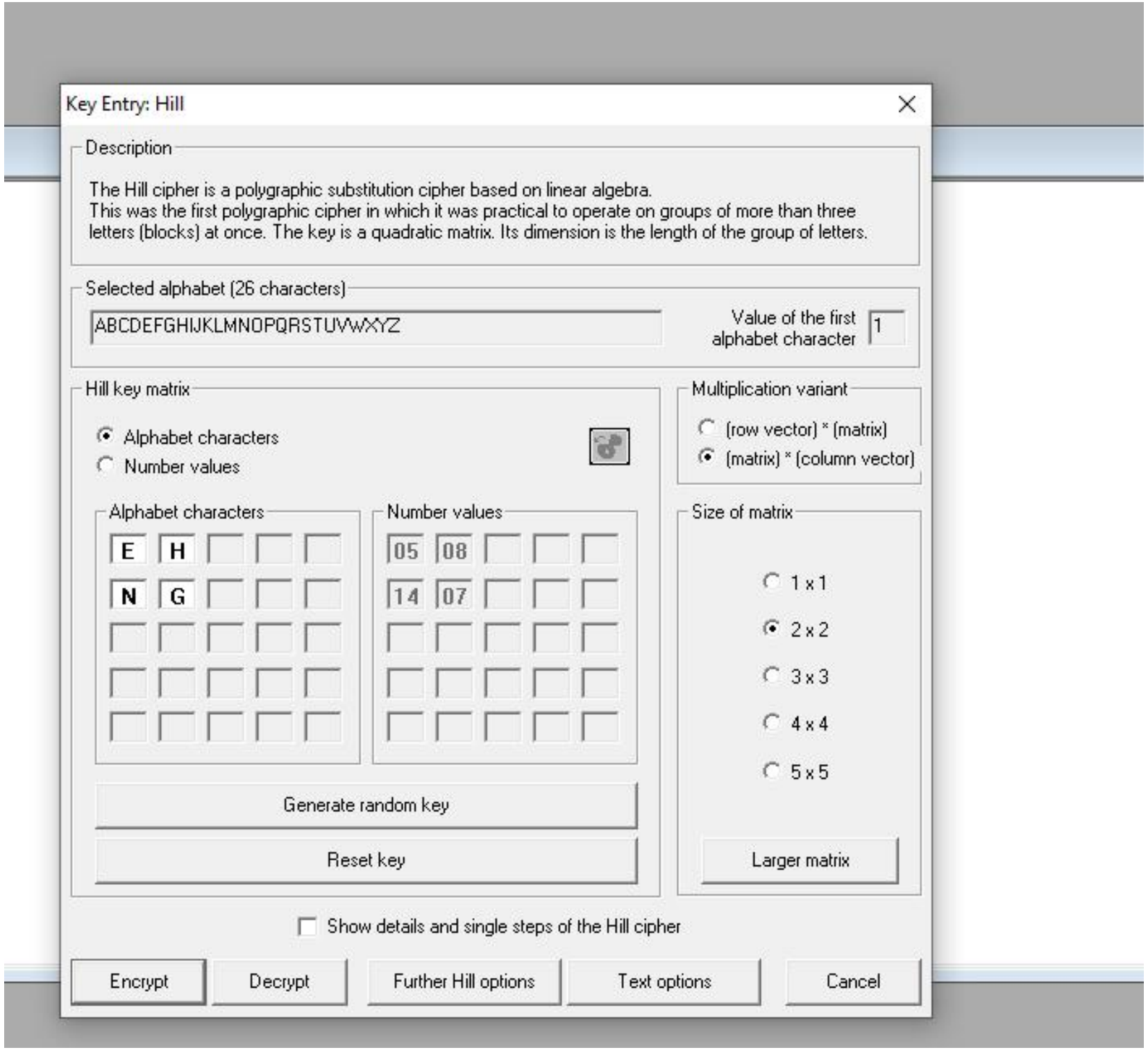
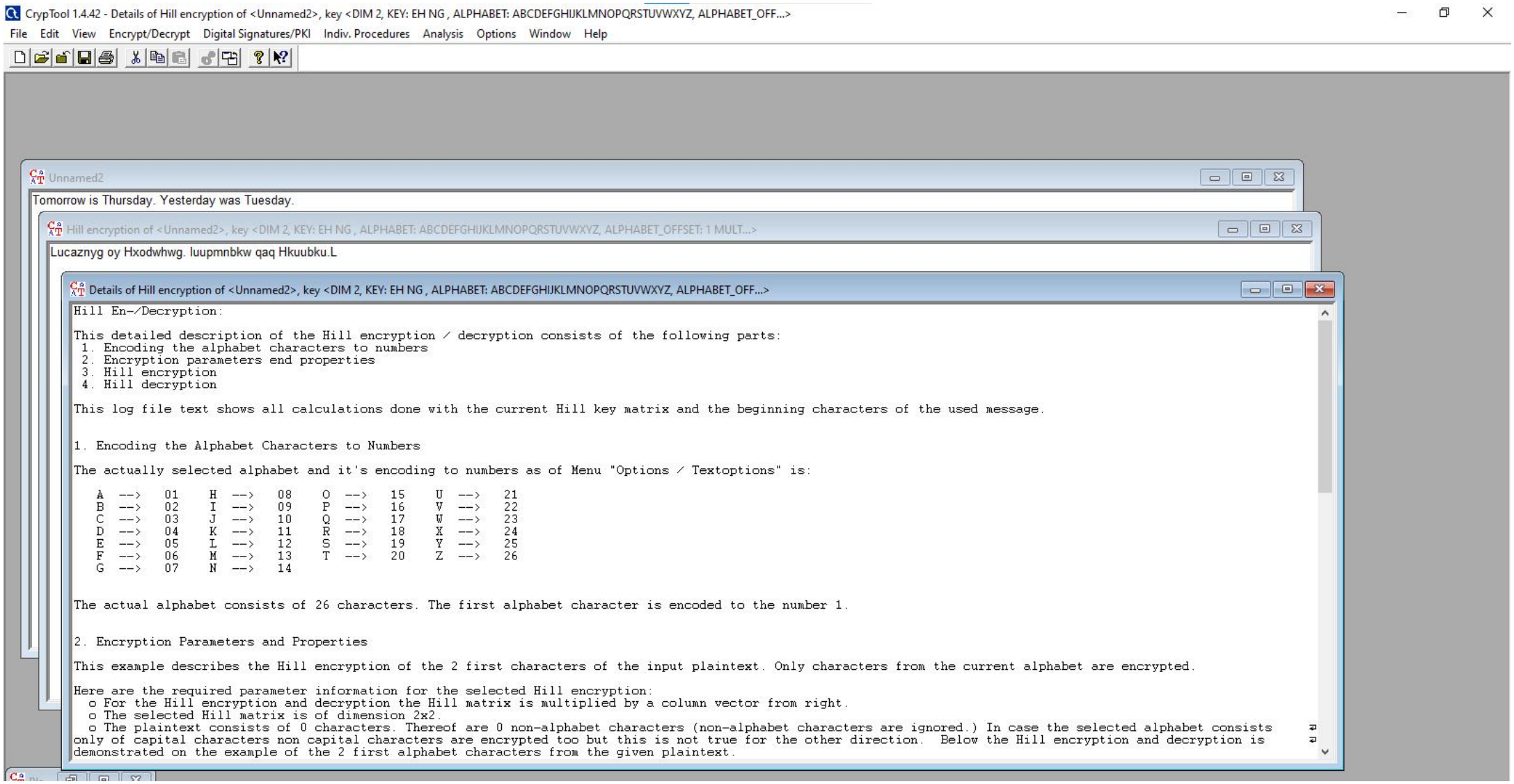
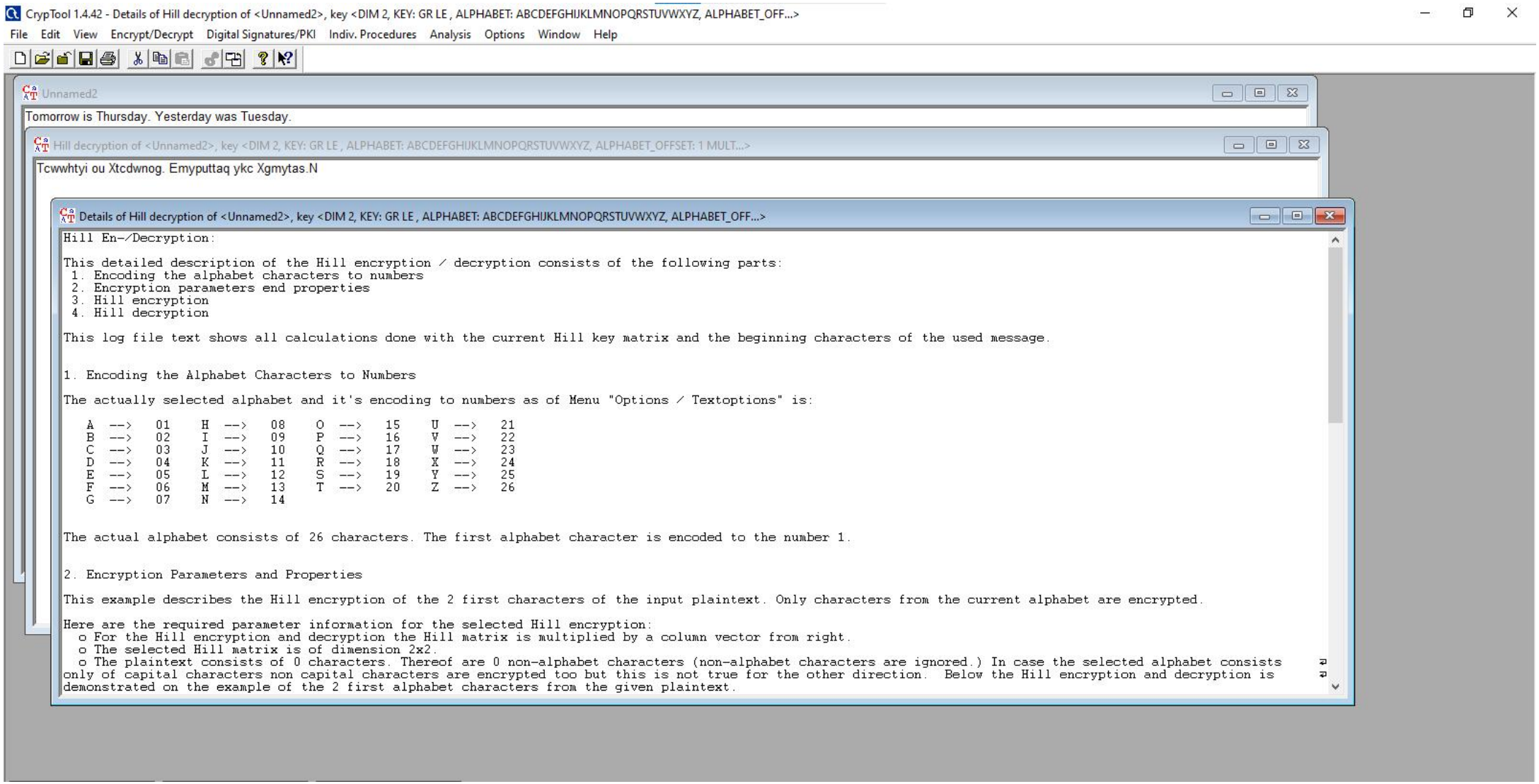

CrypTool 1.4.42 - Unnamed2
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
Caesar / Rot-13...
Vigenère...
Hill...
Substitution / Atbash...
Playfair...
ADFGVX...
Byte Addition...
XOR...
Vernam / OTP...
Homophone...
Permutation / Transposition...
Solitaire...
Scytale / Rail Fence...
Unnamed2
Tomorrow is Thursday. Yesterday was Tuesday.


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
Alphabet characters
E H
N G
Number values
05 08
14 07
Multiplication variant
(row vector) * (matrix)
(matrix) * (column vector)
Size of matrix
1 x 1
2 x 2
3 x 3
4 x 4
5 x 5
Generate random key
Reset key
Larger matrix
Show details and single steps of the Hill cipher
Encrypt
Decrypt
Further Hill options
Text options
Cancel


CrypTool 1.4.42 - Details of Hill encryption of <Unnamed2>, key <DIM 2, KEY: EH NG , ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFF...>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2
Tomorrow is Thursday. Yesterday was Tuesday.
Hill encryption of <Unnamed2>, key <DIM 2, KEY: EH NG , ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFFSET: 1 MULT...>
Lucaznyg oy Hxodwhwg. luupmnbkw qaq Hkuubku.L
Details of Hill encryption of <Unnamed2>, key <DIM 2, KEY: EH NG , 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 end 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.


CrypTool 1.4.42 - Details of Hill decryption of <Unnamed2>, key <DIM 2, KEY: GR LE , ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFF...>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2
Tomorrow is Thursday. Yesterday was Tuesday.
Hill decryption of <Unnamed2>, key <DIM 2, KEY: GR LE , ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ, ALPHABET_OFFSET: 1 MULT...>
Tcwwhtyi ou Xtcdwnog. Emyputtaq ykc Xgmytas.N
Details of Hill decryption of <Unnamed2>, key <DIM 2, KEY: GR LE , 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 end 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.