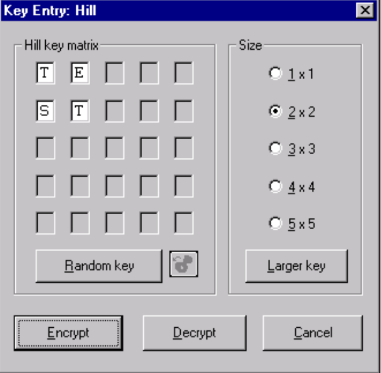
|  |
| --- |
| **Lab Session 04** |

**OBJECT: Implementation of Hill Cipher.**

The text HILLCIPHER is to be encrypted with the key T E S T. To do this, a new document is created (via File \ New) and the text HILLCIPHER is entered. Under the classical encryption algorithms lower case letters are always replaced by the corresponding upper case letters. However, CrypTool keeps upper and lower case letters distinct in order to make the text easier for you to read. These two aspects can be disabled independently of each other via the options Keep characters not present in the alphabet unchanged and Keep uppercase / lowercase (if possible) in the Text Options dialog box. Therefore it does not matter whether the text contains lower case letters. To demonstrate this we will use Hillcipher instead of HILLCIPHER:



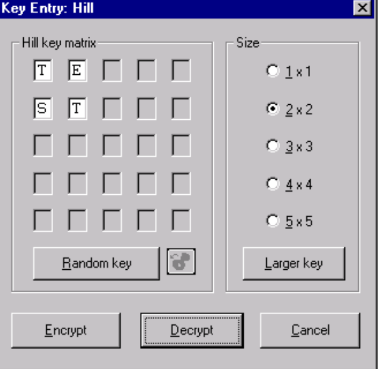
**We now select Encrypt/Decrypt \ Classical \ Hill, following which this dialog box appears:**

****

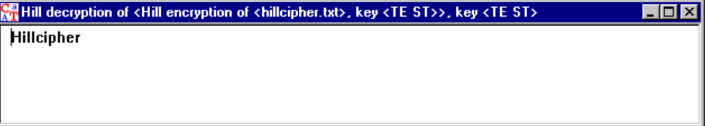
After entering the key T E S T it can be saved in the clipboard (in order to avoid having to enter it again later on at the decryption stage) by clicking on the Copy button. Information on the clipboard will be found in the Help facility on the toolbar. Now click on the Encrypt button, and a new window that contains the encrypted text opens.



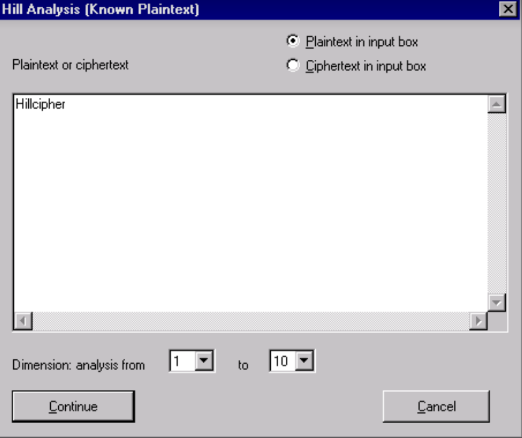
The encrypted text is now decrypted for checking purposes. The decryption procedure is identical to encryption, except that this time the Decrypt option must be selected, i.e. the radial button next to that option must be selected. This is done by clicking on the field with the mouse. The key can now either be typed in manually as before or else it can be inserted from the clipboard using the Paste button if it had previously been copied.



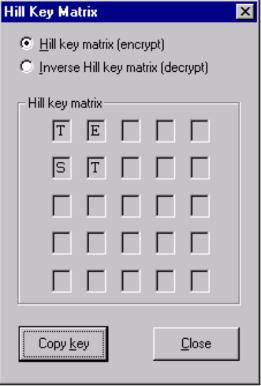
Now click on Decrypt, and the plaintext reappears.

****

CrypTool will now work out the key using a Known Plaintext attack. Such an attack requires that both the plaintext and the encrypted text are available. The easiest approach is to copy the plaintext (mark with the mouse pointer and then press the key combination Ctrl+C) from one of the two windows which contain Hillcipher to the clipboard. Now make the window containing the encrypted text the active window again (by clicking on it with the mouse) and select the menu option Analysis \ Known Plaintext \ Hill to view the Analysis Hill cipher window. The plaintext is then pasted from clipboard into this window (using the key combination Ctrl+V).



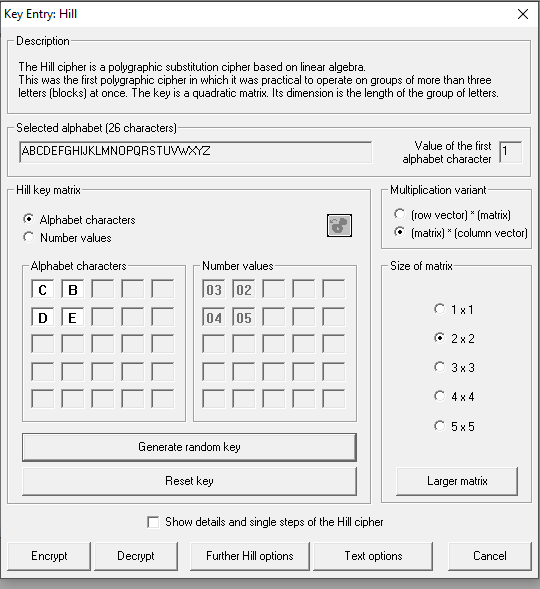
The analysis starts when the Continue button is clicked and the key T E S T appears in the following window.

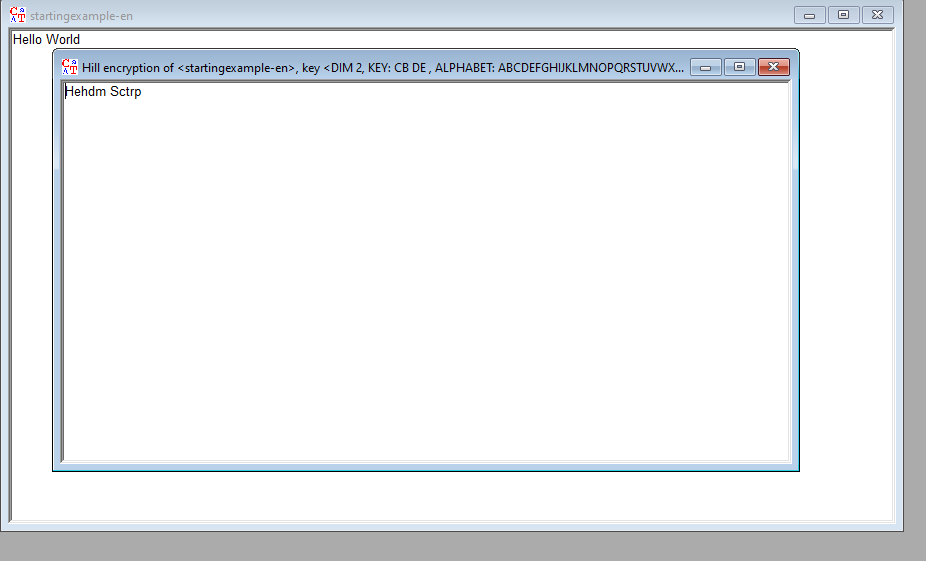


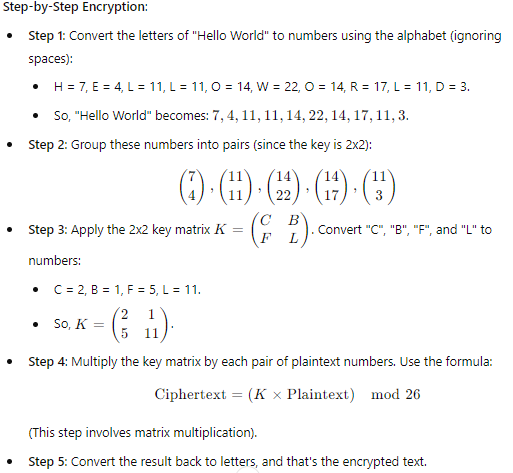
In this way the key was worked out simply from knowing the plaintext and the corresponding encrypted text.

## EXERCISE

1. Explain the working of the Hill cipher. Encrypt the text "Hello World" with a key K =  . What is the result?



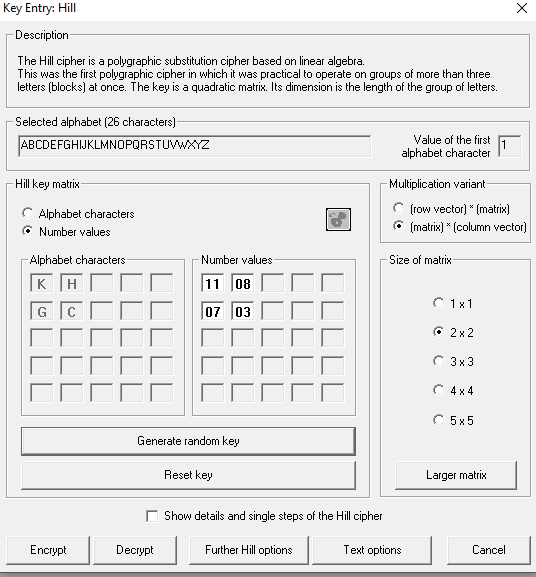


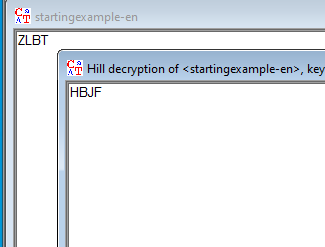


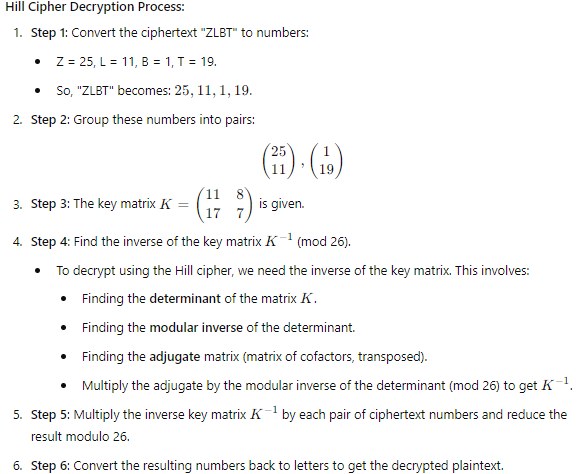


2. Decrypt the text "ZLBT" using the key K =

and explain the process.

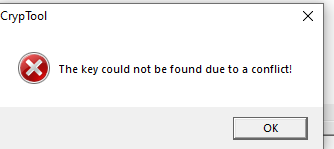






**3. Using analysis in Cryptool, apply the known plain text attack and find out the key of Hill**

**Cipher. Known Plain Text “friday” and corresponding cipher text is “PQCFKU**

****