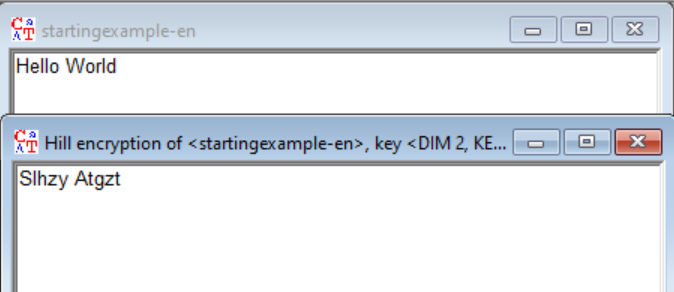
**LAB 2**

**EXERCISE**

1. Explain the working of Hill cipher. Encrypt the text “Hello World” with a key K = [C B

D E].



**Working of Hill Encryption/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 --> 00 H --> 07 O --> 14 U --> 20

B --> 01 I --> 08 P --> 15 V --> 21

C --> 02 J --> 09 Q --> 16 W --> 22

D --> 03 K --> 10 R --> 17 X --> 23

E --> 04 L --> 11 S --> 18 Y --> 24

F --> 05 M --> 12 T --> 19 Z --> 25

G --> 06 N --> 13

The actual alphabet consists of 26 characters. The first alphabet character is encoded to the number 0.

**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:

* For the Hill encryption and decryption the Hill matrix is multiplied by a column vector from right.
* The selected Hill matrix is of dimension 2x2.
* 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.

**3. Hill Encryption:**

Selected Hill matrix for encryption:

H[t] = [ C B ]

[ D E ]

This matrix encoded to numbers:

H[n] = [ 02 01 ]

[ 03 04 ]

Encryption of the plaintext: "HE":

This plaintext vector P is below encoded to numbers:

P[n] = [ 07 04 ]

Computation of the Hill encryption by the row\*column matrix\*vector product (the vector P[n] is a column vector):

S <-- 18 = 02\*07 + 01\*04 (mod 26)

L <-- 11 = 03\*07 + 04\*04 (mod 26)

The Hill ciphertext is: "SL".

**4. Hill decryption:**

The inverted Hill matrix for decryption:

D[t] = [ G F ]

[ P Q ]

This matrix encoded to numbers:

D[n] = [ 06 05 ]

[ 15 16 ]

Decryption of the ciphertext: "SL":

Ciphertext vector C decoded to numbers:

C[n] = [ 18 11 ]

Computation of the Hill decryption by the row\*column matrix\*vector product (the vector C[n] is a column vector):

H <-- 07 = 06\*18 + 05\*11 (mod 26)

E <-- 04 = 15\*18 + 16\*11 (mod 26)

The Hill plaintext is: "HE".

1. 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”

