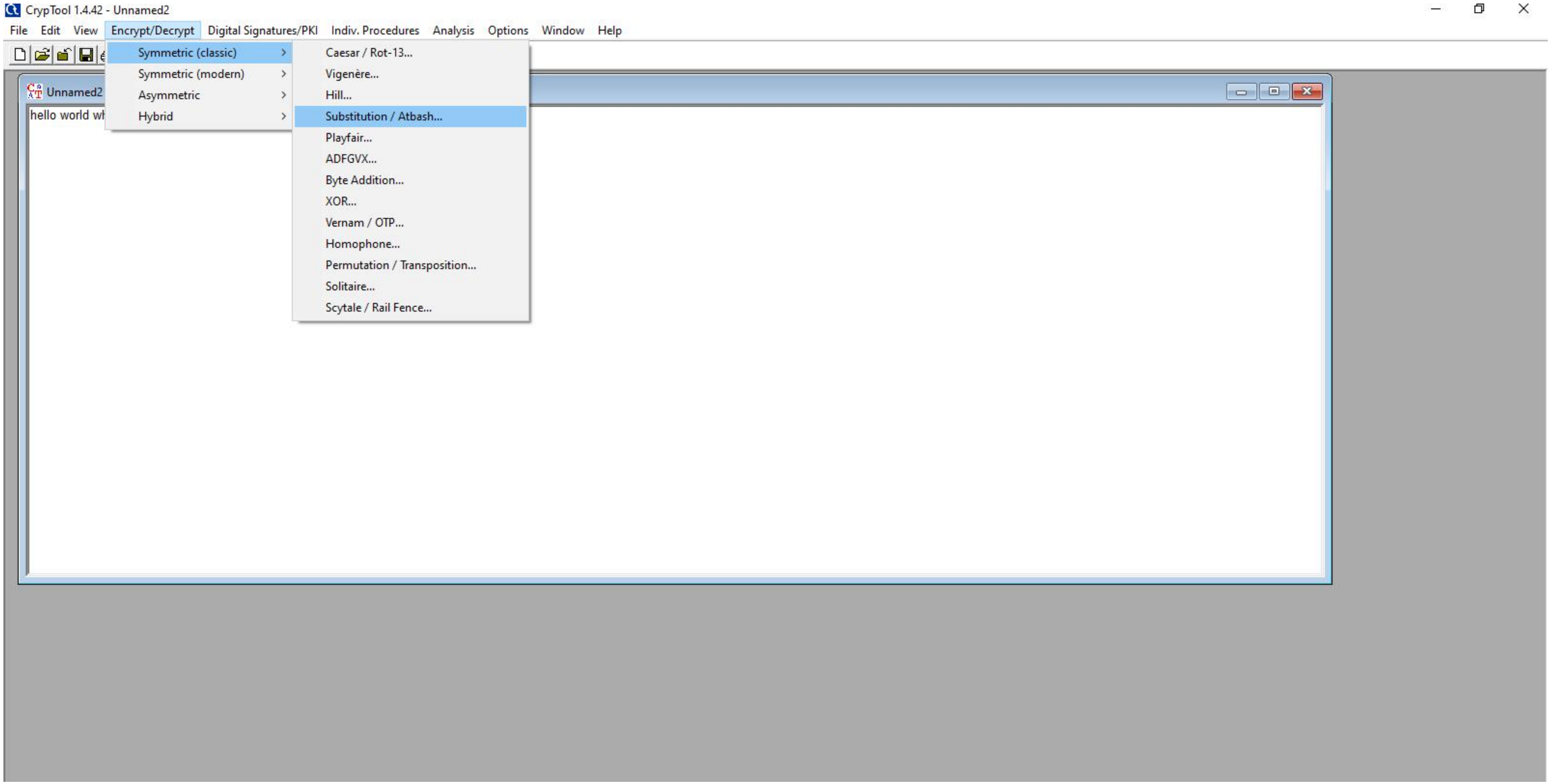
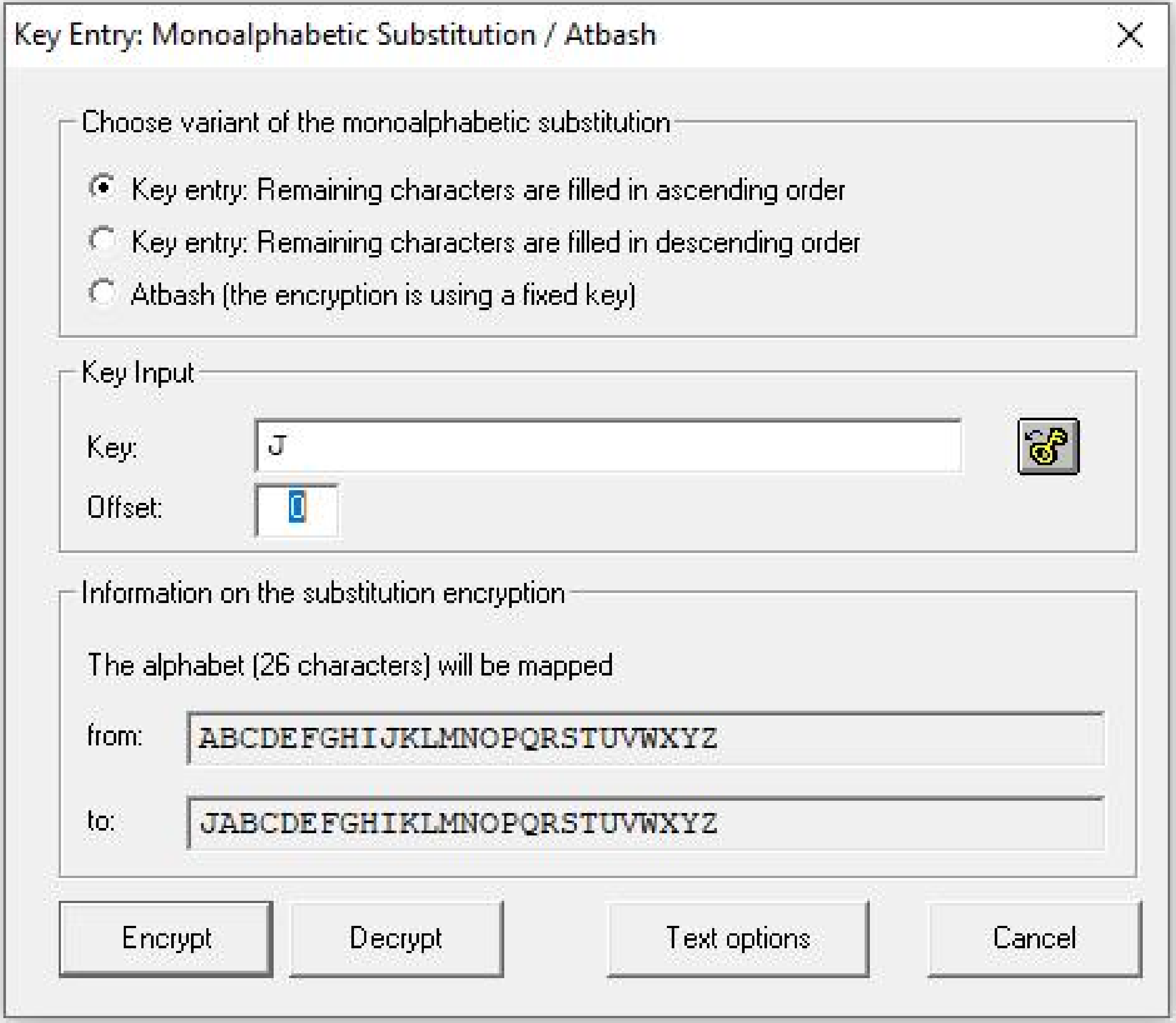


hello world wh



Key Entry: Monoalphabetic Substitution / Atbash

Choose variant of the monoalphabetic substitution

● Key entry: Remaining characters are filled in ascending order

○ Key entry: Remaining characters are filled in descending order

○ Atbash (the encryption is using a fixed key)

Key Input

Key: J

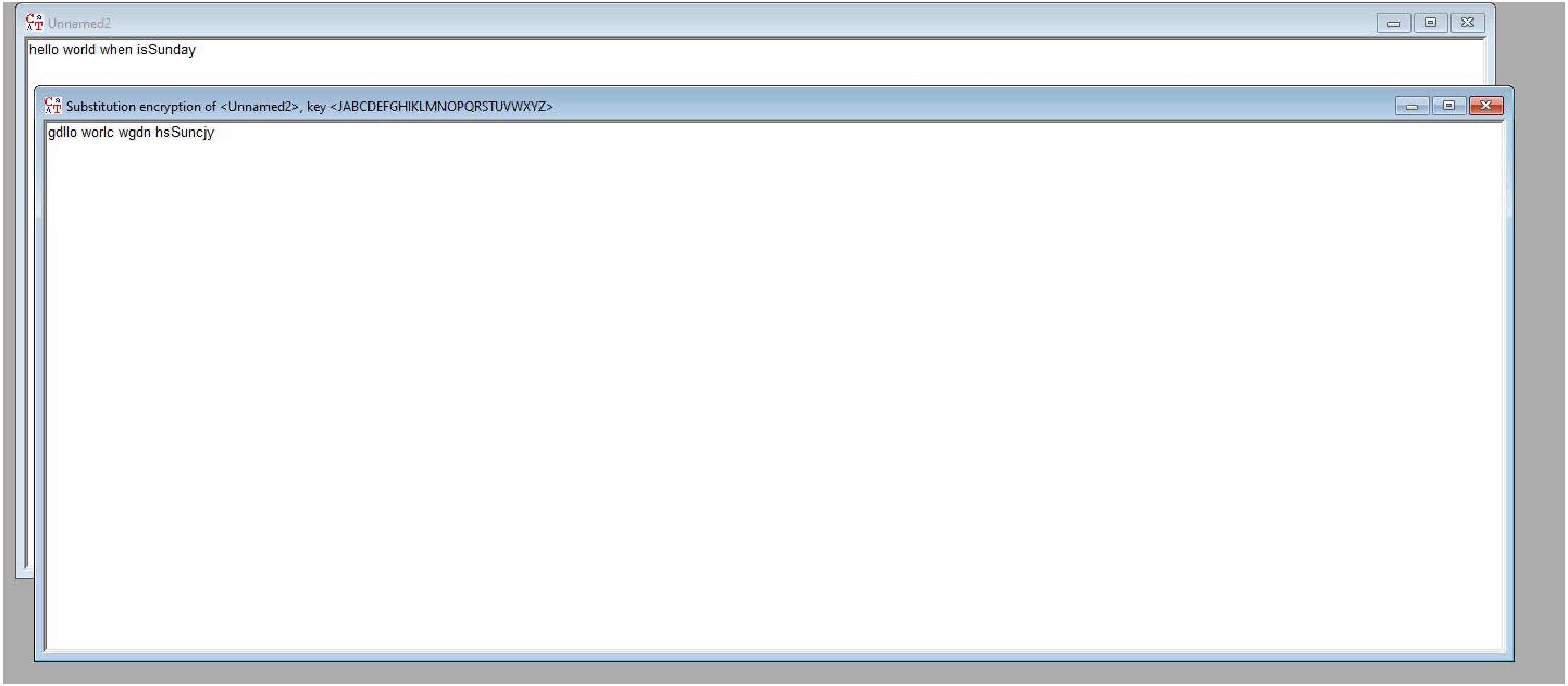
Offset: 0

Information on the substitution encryption

The alphabet (26 characters) will be mapped

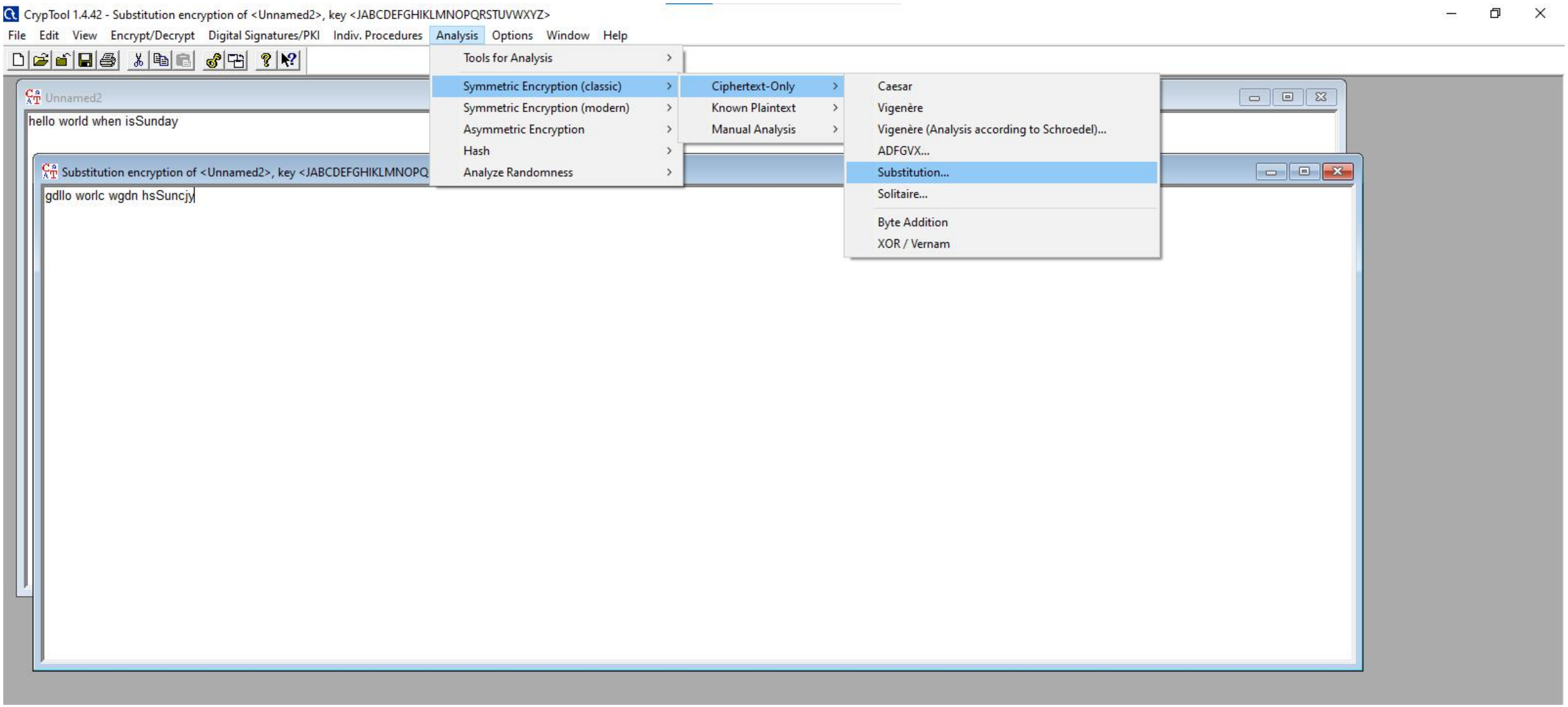
from: ABCDEFGHIJKLMNOPQRSTUVWXYZ

to: JABCDEFGHIKLMNOPQRSTUVWXYZ


Unnamed2
Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>

```
hello world when isSunday
```

```
gdllo worlc wgdn hsSuncjy
```



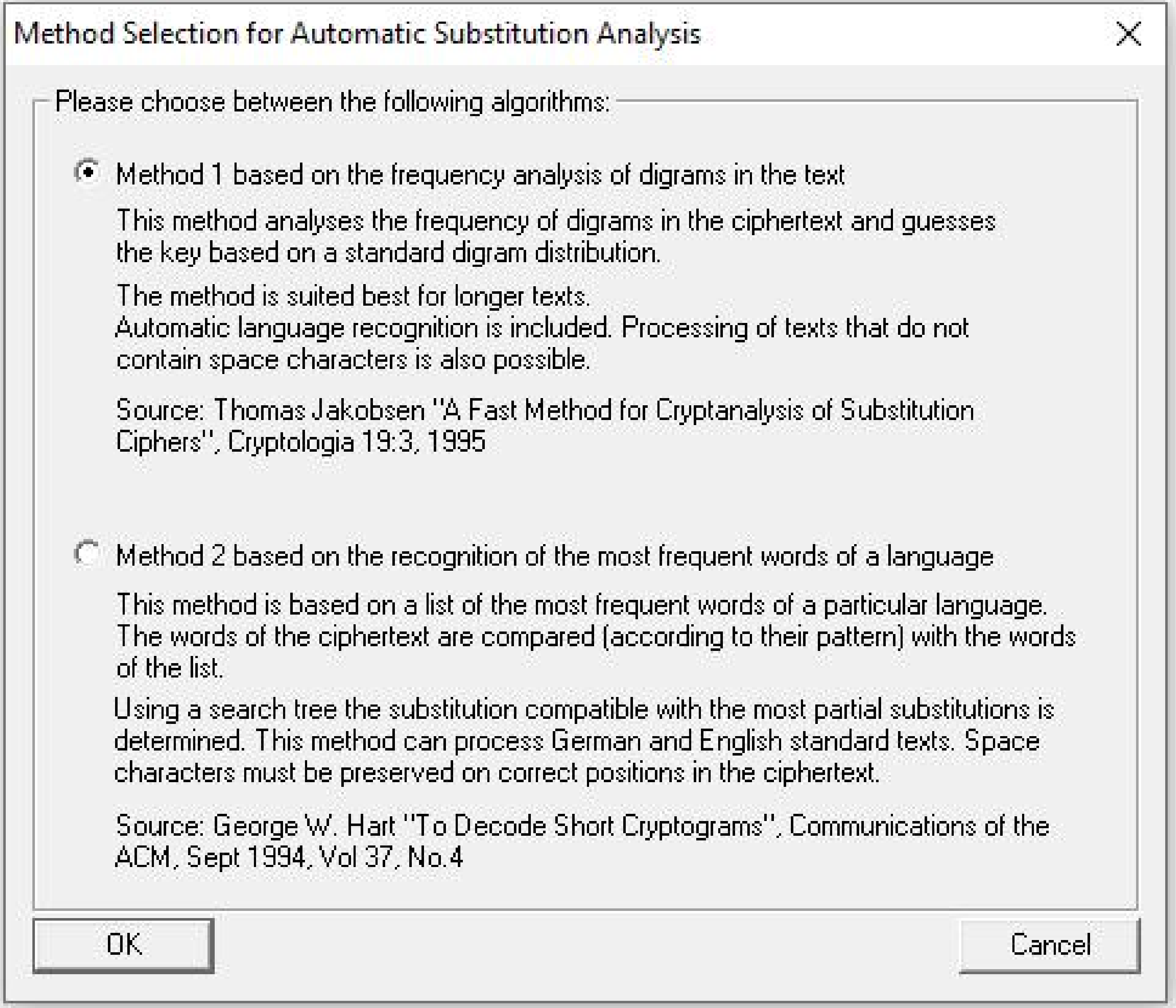
CrypTool 1.4.42 - Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>

Unnamed2

hello world when isSunday

Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQ

gdllo worlc wgdn hsSuncjy



Please choose between the following algorithms:

● Method 1 based on the frequency analysis of digrams in the text

This method analyses the frequency of digrams in the ciphertext and guesses the key based on a standard digram distribution.

The method is suited best for longer texts.
Automatic language recognition is included. Processing of texts that do not contain space characters is also possible.

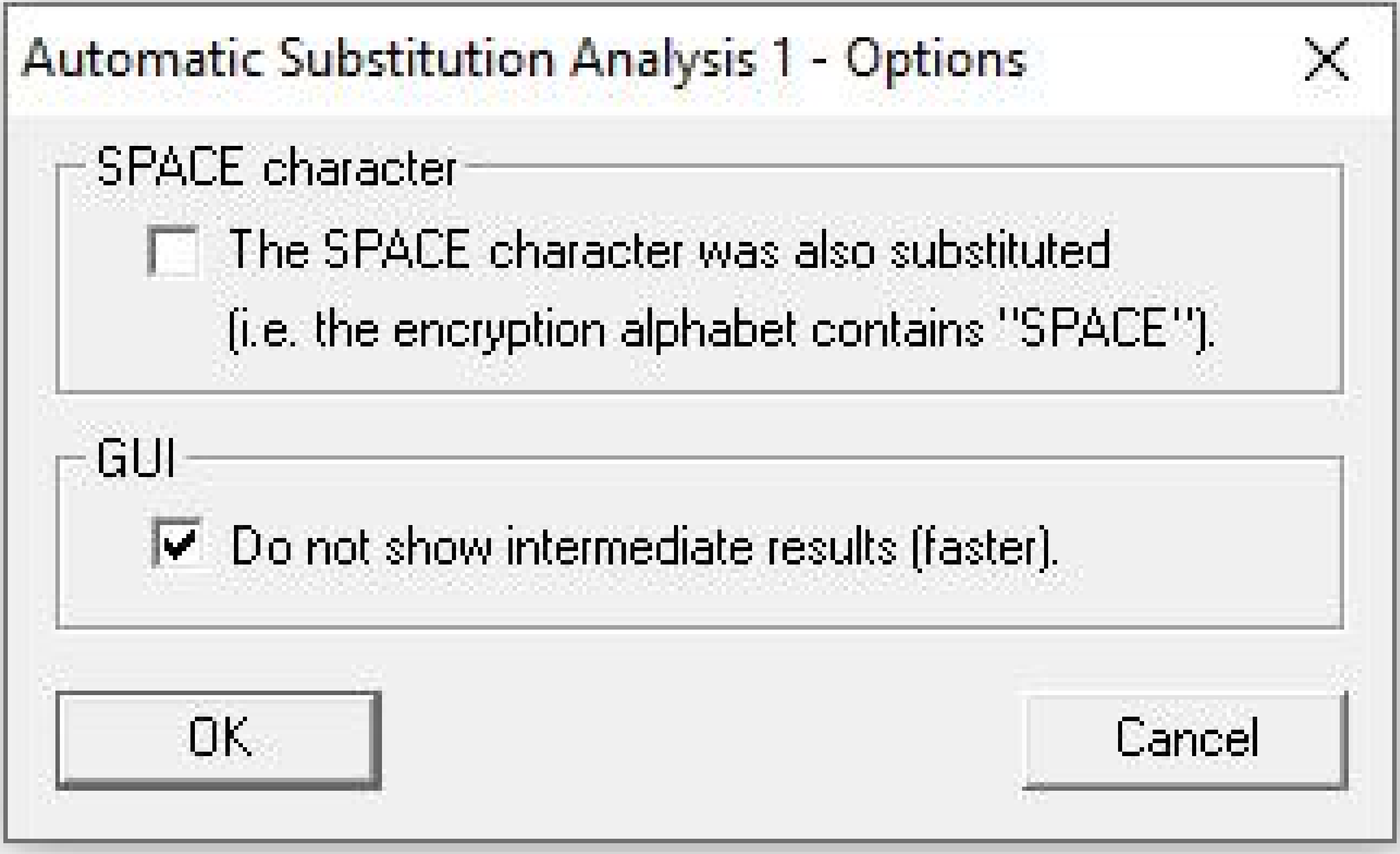
Source: Thomas Jakobsen "A Fast Method for Cryptanalysis of Substitution Ciphers", Cryptologia 19:3, 1995

○ Method 2 based on the recognition of the most frequent words of a language

This method is based on a list of the most frequent words of a particular language. The words of the ciphertext are compared (according to their pattern) with the words of the list.

Using a search tree the substitution compatible with the most partial substitutions is determined. This method can process German and English standard texts. Space characters must be preserved on correct positions in the ciphertext.

Source: George W. Hart "To Decode Short Cryptograms", Communications of the ACM, Sept 1994, Vol 37, No.4



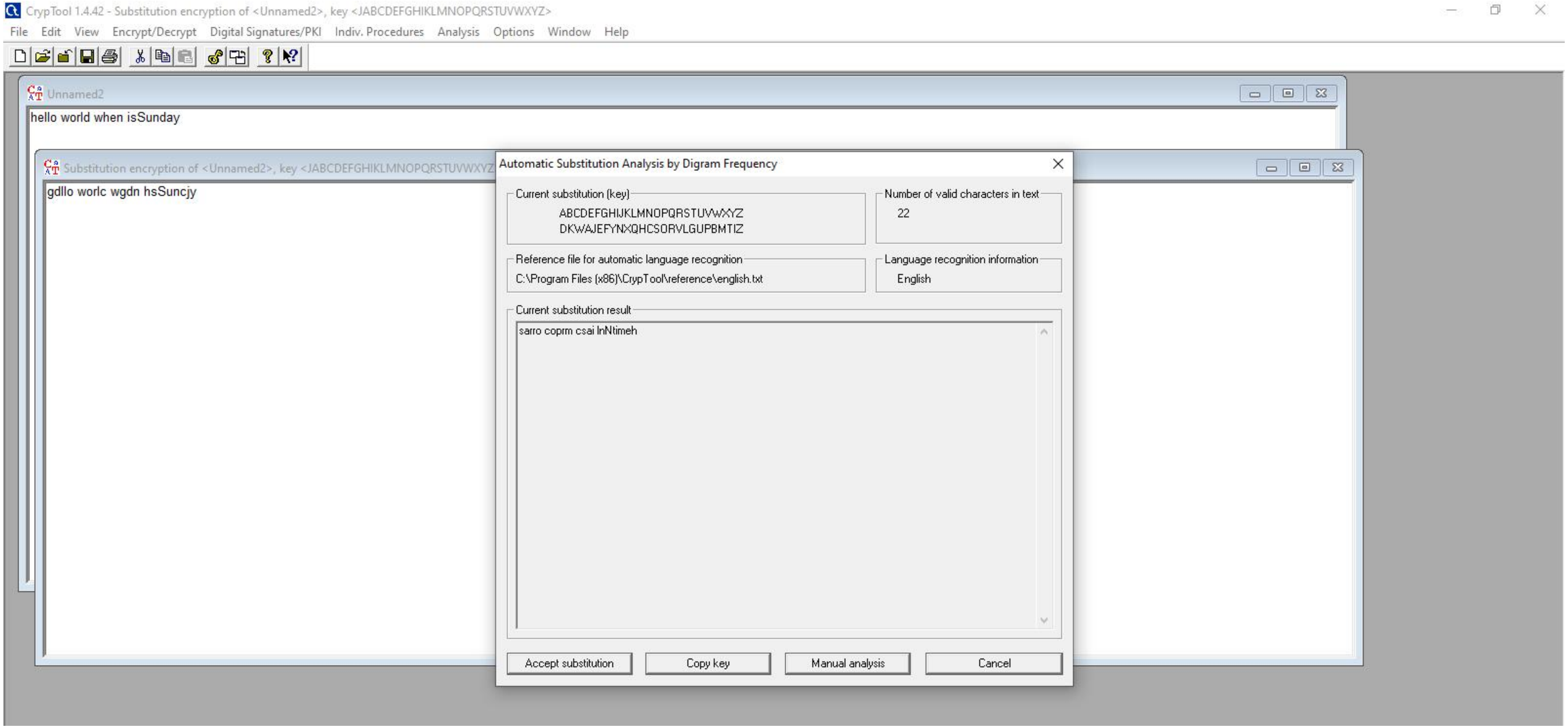
Automatic Substitution Analysis 1 - Options

SPACE character

□ The SPACE character was also substituted (i.e. the encryption alphabet contains "SPACE").

GUI

☑ Do not show intermediate results (faster).



CrypTool 1.4.42 - Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed2

hello world when isSunday

Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ

gdllo worlc wgdn hsSuncjy

Automatic Substitution Analysis by Digram Frequency

Current substitution (key)

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DKWAJEFYNXQHCSORVLGUPBMTIZ

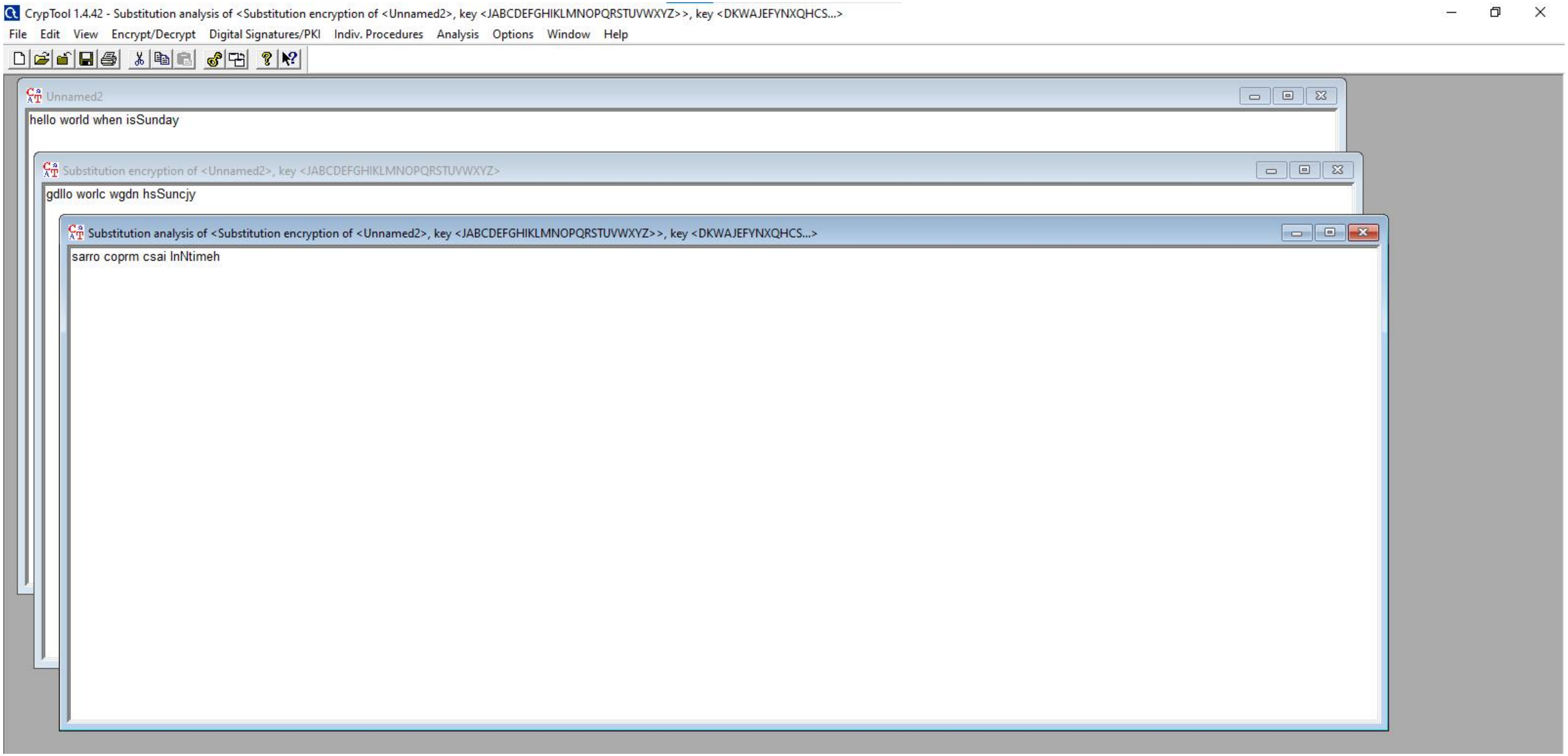
Number of valid characters in text: 22

Reference file for automatic language recognition: C:\Program Files (x86)\CrypTool\reference\english.txt

Language recognition information: English

Current substitution result

sarro coprm csai lnNtimeh


CrypTool 1.4.42 - Substitution analysis of <Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>>, key <DKWAJEFYNXQHCS...>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

Unnamed2

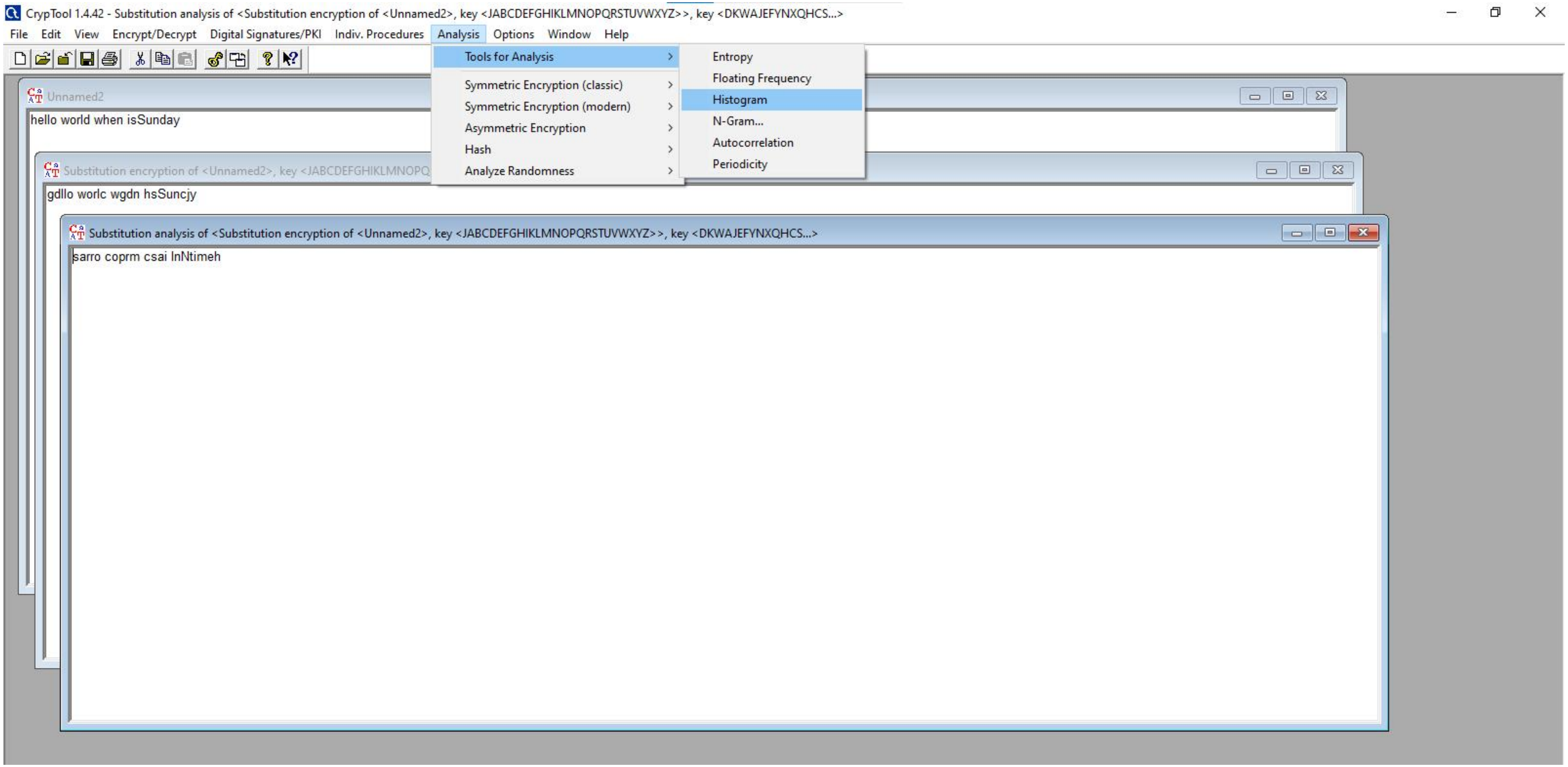
```
hello world when isSunday
```

Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>

```
gdllo worlc wgdn hsSuncjy
```

Substitution analysis of <Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>>, key <DKWAJEFYNXQHCS...>

```
sarro coprm csai InNtimeh
```



CrypTool 1.4.42 - Substitution analysis of <Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>>, key <DKWAJEFYNXQHCS...>

Unnamed2

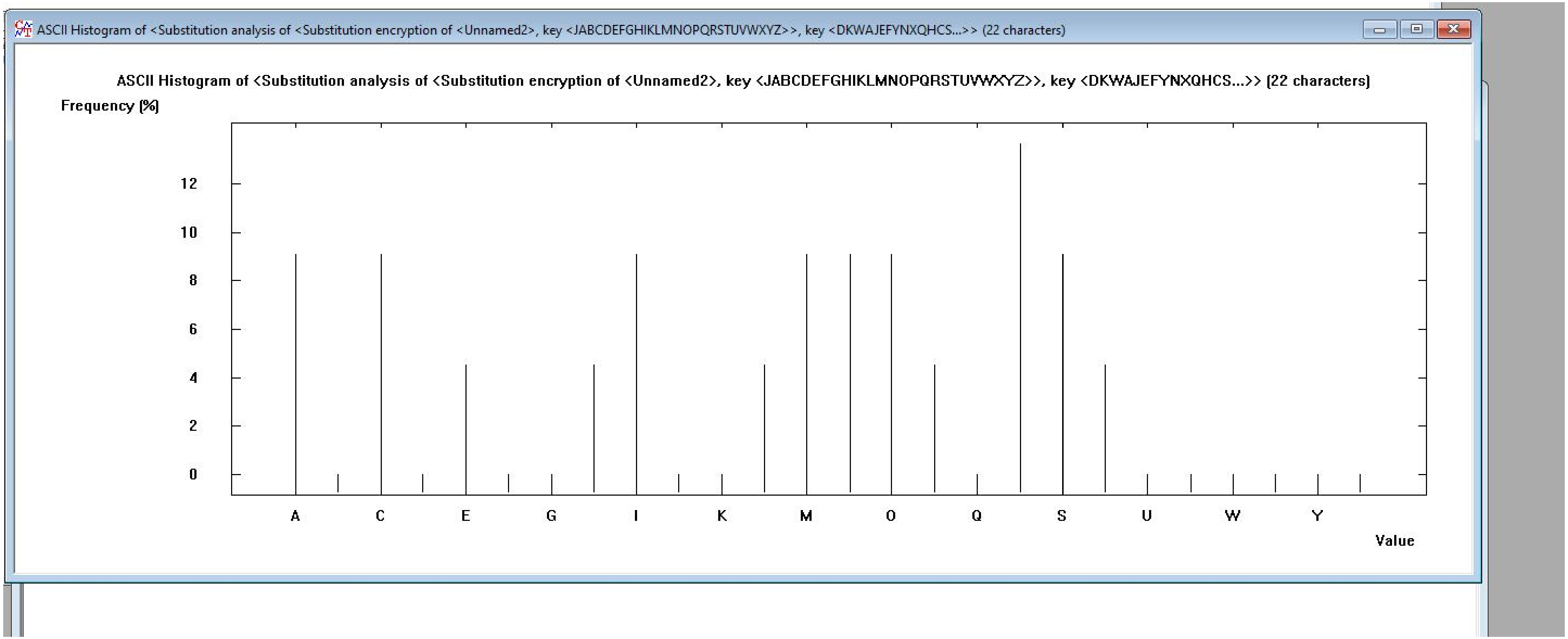
hello world when isSunday

Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQ

gdllo worlc wgdn hsSuncjy

Substitution analysis of <Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>>, key <DKWAJEFYNXQHCS...>

sarro coprm csai lnNtimeh



ASCII Histogram of <Substitution analysis of <Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>>, key <DKWAJEFYNXQHCS...>> (22 characters)

ASCII Histogram of <Substitution analysis of <Substitution encryption of <Unnamed2>, key <JABCDEFGHIKLMNOPQRSTUVWXYZ>>, key <DKWAJEFYNXQHCS...>> (22 characters)