Puzzled Pint
December 2012

Yousa thinkin ME a racist caricature?
I daresay I protest, sir!
Kindly inspect these other arguably offensive characters from **actual Disney movies**.
Then, use **monoalphabetic substitution keyword ciphers** to find out what we should all aspire to be, in the end!

FJHKN

BUQSK

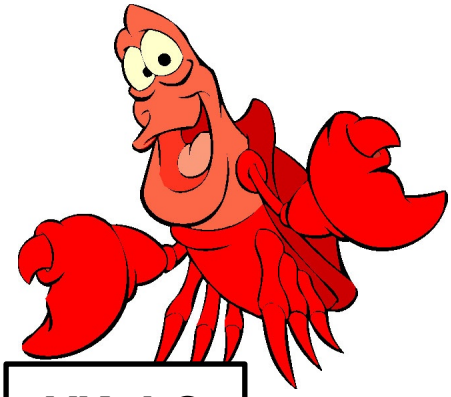
OPTDI

URYNG

WUPFM

JLRDI

SMABU



VKTLG

Keyword cipher

A **keyword cipher** is a form of monoalphabetic substitution. A keyword is used as the key, and it determines the letter matchings of the cipher alphabet to the plain alphabet. Repeats of letters in the word are removed, then the cipher alphabet is generated with the keyword matching to A,B,C etc. until the keyword is used up, whereupon the rest of the ciphertext letters are used in alphabetical order, excluding those already used in the key.

```
Plaintext:   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Encrypted:   K R Y P T O S A B C D E F G H I J L M N Q U V W X Z
```

With KRYPTOS as the keyword, all As become Ks, all Bs become Rs and so on. Encrypting the message "knowledge is power" using the keyword "kryptos":

```
Plaintext:   K N O W L E D G E I S P O W E R
Encoded:     D G H V E T P S T B M I H V T L
```

Only one alphabet is used here, so the cipher is monoalphabetic.

The best ways to attack a keyword cipher without knowing the keyword are through known-plaintext attack, frequency analysis and discovery of the keyword (often a cryptanalist will combine all three techniques). Keyword discovery allows immediate decryption since the table can be made immediately.

Do you have an iOS device?

Scan the QR Code below to install **ARG Tools**, then select “Substitution” under “Interactive Tools” to use a **monoalphabetic substitution keyword cipher**.

http://itunes.apple.com/us/app/arg-tools/id374959430?mt=8