

Assignment 1- Part 3 - Report

Eugenio Ribón

Code description

The code first takes ciphertext as an input, then it iterates through all the keys in the dictionary shifting the ciphertext character by that key if it is a letter and ignoring the rest of characters. It then displays the result for every key allowing the user to manually look for the correct one. It can be run by using the `./mc cipher` file and then introducing the text to decipher.

Attack method

This is a brute force attack that decrypts the ciphertext for every key. It makes no distinctions between lower and upper case characters. Also it only affects letters from the english alphabet and ignores all other characters.

Alternative method

Instead of a brute-force attack, you could use Frequency Analysis. This method relies on the statistical fact that certain letters in the English language appear more frequently than others . By calculating the frequency of letters in the ciphertext and comparing them to standard English letter frequencies, the program can programmatically determine the most likely key without human review.

Results

Key = 13 left, 13 right.

Plaintext = “to be, or not t%o be: that is the q@uestion”

```
eugenio@MacBook-Pro-7:Part_3 % ./mc_cipher
Enter the ciphertext: Gb or; be abg gkb or; gung vf gur d@hrgvba
Key 0: gb or; be abg gkb or; gung vf gur d@hrgvba
Key 1: fa nr; ad zaf fkw nq; ftfm ue ftq @cgefuaz
Key 2: ez mp; zc yze e@z mp; esle td esp b@fpdetzy
Key 3: dy lo; yb xyd dhey lor; drke sc dro @eoecdsvx
Key 4: cx wu; xa wxc e@w u; c@tj c@tj @eduhcrwx
Key 5: jm jn; ym ym jm jn jm jn @bm @bm @bm @bm
Key 6: av il; vy uva a@v il; ahdha pz aol @bzlzapvu
Key 7: zu hk; ux tuz zhu hki; zngz oy znk @e@skyzout
Key 8: yt gj; tw sty y@t gj; ymfy nx ynj @e@zjxnyts
Key 9: xs fi; sv rsx x@s fi; xlex mw xl@iuyixwmsr
Key 10: wr eh; ru qrw w@r eh; wkdw lv wkh te@hwlrq
Key 11: vr dg; qn pov v@r dg; v@r dg @e@v@r dg
Key 12: qn v@r dg; os v@r dg; v@r dg @e@v@r dg
Key 13: to be; or not tho be: that is the question
Key 14: so ad; ng mns s@m ad; szgs hr sgd p@tdrsnhn
Key 15: rr zc; m_lmr r@m zc; r@fr gg rfc o@scargm
Key 16: ql yb; ln klq q@l yb; qexq fp geb ne@rbpfuI
Key 17: pk xa; kn jpk x@b pdpw eo pda me@qaopekl
Key 18: oj wz; jn ljo o@j wz; ocdm dn ocz le@przhof
Key 19: ni ul; ul ul ul ul; w@tun w@tun w@tun w@tun
Key 20: h@l ux; h@l ghm m@h; matm b@l max j@nxwlmhbg
Key 21: lg tw; gj fgl l@g tw; lzsl ak i@w i@w i@w i@w
Key 22: kf sv; fi efk kf@f sv; kykrk z@j kyy h@lvkjzfd
Key 23: je ru; eh de@j ke ru; qxaj y@l kxu g@kujijef
Key 24: id qt; d@l cdi i@d qt; i@pwi xh iwt fe@jthixd
Key 25: hc ps; cf bch h@c ps; hvoh w@j hvs e@jsghwcb
```