

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 gnb or: gung vf gur dghrfvgba
Key 0: gb or, be abg gnb or: gung vf gur dghrfvgba
Key 1: fa ng, ad zar fha ng: ftmf ue ftq cgggefuaz
Key 2: ez mp, zc yze ehz mp: dsle td esp befpdety
Key 3: dy lo, yb xyd dhy lo: drkd sc dro a@eocdsyx
Key 4: cx kn, xa wxc chx kn: cqjc rb cqn z@dnbcxw
Key 5: bw jm, wz vwb bhw jm: bpih qa bpm y@cnabqvw
Key 6: av il, vy vva shv il: aohb pz aol x@blapvu
Key 7: zu hk, ux tuz zhu hk: zngz oy znk w@akyzout
Key 8: yt gj, tw sty ykt gj: ymfy nx ymj v@zjxynts
Key 9: xs fi, sv rsx xfs fi: xlex mw xli u@yiwmsr
Key 10: wr eh, ru qwr whr eh: wkdw lv wkh t@hwltrq
Key 11: vq dg, qt pqv vqg dg: vjcv ku vjp s@quvkgp
Key 12: up cf, ps opu upf cf: uibu jt uif r@vftujpo
Key 13: to be, or not t%o be: that is the q@uestion
Key 14: sn ad, nq mns shn ad: sgzs hr sgd p@tdsrhnm
Key 15: m xc, mp lmr rma xc: rfyf gq rfc q@scrgnl
Key 16: ql yb, lo klq qal yb: qexq fp qeb n@rbpqflk
Key 17: pk xa, kn jkp pkk xa: pdwp eo pda m@qaopekj
Key 18: oj wz, ja ijo oej wz: ocvo dn ocz lapznodji
Key 19: nl ey, il hin nkl vy: nbun cn nby k@oyncibh
Key 20: mh ux, hk ghm mhh ux: matn bl max j@nklabhg
Key 21: lg tw, gj fgl lgt tw: lzsl ak lzw i@nklagf
Key 22: kf sv, fi efk kfi sv: kyrk zj kyv h@lvjkzfe
Key 23: ie ru, eh dej jhe ru: jxaj yi jxu g@kuijyed
Key 24: id qt, dq cdi idt qt: iwdi xh iwt f@jthixdc
Key 25: hc ps, cf bch hkc ps: hvoh wg hvs e@ishwcb
```