Homework 1 (Program)

■ Vigenère Cipher Attack

The Vigenère cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution.

The Vigenère cipher has been reinvented many times. The method was originally described by Giovan Battista Bellaso in his 1553 book La cifra del. Sig. Giovan Battista Bellaso; however, the scheme was later misattributed to Blaise de Vigenère in the 19th century, and is now widely known as the "Vigenère cipher".

You are to write a program to break Vigenère cipher based on Friedman test. (see handout)

The Input

One line ciphertext in uppercase.

The Output

Two line:

First line is the secret key in uppercase.

Second line is the plaintext in uppercase.

Key’s length is limited between 1 and 20. (0 < length < 21)

***Note that we also accept the keys which is n times repeat the original key. For example, if the original key is “NCTUCS”, you can answer “NCTUCS”, “NCTUCSNCTUCS”, or “NCTUCSNCTUCSNCTUCS”. But “NCTUCSNCTUCSNCTUCSNCTUCS” is not accepted due to the length limit.**

■ Sample Input:

(next page)

Sample Input 1

```
KERWXAETHMJTVORLNTRGIDRKEAVYUTTKOOOGWAZCMCHAOJNFQSALTFLVIOJEC
GFBZGZPVKENTHMJSKQWYGMTNKPDJQVCBYWEOSOCCPIERCCHAEJADYZMSNKF
NZIELFLLQDUYCLTSXNZACMVFFUCUYNBFQSBLJVYVXOSTHCDDWOLAWHFUECZGL
QYRQHXRVOFQDGZWIRQNTUECKAVVYRQCMIAHPPHIAPKGCZSJENYFNWGCFTKSG
RZLYTGXVMUTRGAYBDQXGRLDMHRRPVSUHNVGHVHEIDRQJJQNLWXWNSMMJVA
PSYSAENLEFSVVVYCDGLLPLPLWXJZQQHDLTSYLKGWCBBHVRWLQZQKNVDIYOBTS
MOMNGISHBNTHTQGVDAWMDMHRSEGDTOCJYQEEGOHPABWCEBSKAJWZLVMJ
HLJARIAHTQSCLQSGDZRNPSWTZGYEUGHTRWSYLPSRGCCXDVNSGKTAHVYCWHB
WSCTMYCERDWRNWAGUBMTVQLBTUHTQDMXVWMDMAADOMFBXQIETMSGEG
GWEGPUCGAEOENYEMTNZLSLOBNLDLMJJVUPLBBRYZMBZGZQCHWNPZNMTSTJG
CZEEAYBKWFINPXMEETSCKMSTKGHMSJIEFOMSMSMSBEFBCGFOMUDYCRGBOOR
ZQFIJYCWMHCSFGXWYZRWMHRICQLZGPXKXGDFTSCAZKVFPXXSGEWJMALJRRIAE
ZODRAUHQIRPGTGHTLYQFNZDTBSAOEUZILYVFPOEOUEUZILYVKPDEBFTR
```

Sample Output 1

```
CRYPTANALYSIS
INTHEARTWORLDMANYARTISTSWITHWEAKBODIESHAVESHOWNUSASTRONGPO
WERINTHEIRGREATWORKSOFARTTAKEFRIDAKAHLOFOREXAMPLESHEWASAHEALT
HYGIRLUNTILSHEWASKNOCKEDDOWNBYABUSATTHEAGEOFTWELVEMUCHOFHER
BODYWASSERIOUSLYHURTBUTHERMINDWASNTINHERPAINTINGSWECANFEELHER
STRONGLOVEOFARTANDLIFEANOTHEREXAMPLEISCHRISTYBROWNHEWASBORNIN
BADHEALTHANDTHEONLYPARTOFHISBODYTHATCOULDMOVEWASHISLEFTFOOTH
OWEVERUSINGHISONLYFOOTHESTILLWASABLETOWRITEANDDRAWWONDERFULL
YINHISAUTOBIOGRAPHYBROWNWROTEWHATHAPPENEDINHISLIFEANDHOWHEBE
GANTODRAWPICTURESWITHHISLEFTFOOTANDDONTFORGETSTEVIEWONDERHEB
ECAMEBLINDSOONAFTERHEWASBORNBUTHEISNOWAPOPULARSINGERANDSONG
WRITERTHESEARTISTSWITHWEAKBODIESBRINGUSMANYGOODTHINGSANDMUCH
HOPEWITHTHEIRSTRONGMINDSTHEIRSTORIESTELLUSTHATTHEMOSTIMPORTANT
THINGINLIFEISNOTWHATWEHAVEBUTWHATWEMAKEOFIT
```

Sample Input 2

```
BPVYWHBPTNKERVAYTWJCLUNAGVEYIAENPBQDVXXXKFNXBFNSTGGYCJGJXZQJR
UMQJWAGOYTKUGPYPLBWMNJWYKMNNWTKKFYGEGTLGVEKWCPYPNHUMKBG
OYTQBPXCPLUGOCNDNIXWCDYGWBGJYKMNNWEGWLKVVPZBQGQQGYOGEPBHI
DVVMFGJRFKCFAAIAIQVNUDYFZRTFIVZRTBZUZREHONVTQMIXAFKMBGJTTTHFEB
VAYTSFKMBCVOGXHCOUKEYUAAEXNJWLFLYGFRCVBQLUGKNJSGUTAQGQKWYCZR
TFIVZRTLUKVFQMBGQCCVEGVNPBWGTNUDYVXBTECVLYGKYFJVFBHIZBQWNQLN
MXNQZRTZLCFQOHNJWEYAYPLUGUUUCRVPUUJRCWSVZRNBNVDRIBLNHHVHHJ
WETXXEDBCDUPVXKLMGVUGKGQLUGKAQGQDRYTWZGFVGJTQLNTSVIANVGTTT
HFENUAIWKRJXLOGGJXLESHVBIPWQFHHVVNYWFGSYQGAVZRYTSCFQREYCKRFHH
VLNNDNQKGTTHIWEUMBGOBQWMCJRFTHIWEQNMFGAVPITJLOHGOQFCBXNAG
VEYTWQTBXKFTJHIFAYNUYESEGYONTHVPBGFYKMNNWEGWLKVVPZBQGQPHNKU
RFLIOWYQOYNQSNHQGJFKGNJWJQHXUKUGYITYBVAYTHEQFCUWGQAYTEBVAYTK
UGICECRFTZGOJCMWJWQVAYDMGVXLHDVGLZNAGCUIWLSQKUYZVNXFKKGGGYF
LBVAYHJBILWTGNMBHISAFMBGFCKVEGVNHXQOGEGECVLYGKYFJVFBHIZBQWQCK
RPCIAAAIMBGONTFMWEZGKXCQFQFOEZGJTNUZRFBXPLAQMCEWNFTLMKUCWIY
SCRKICUUKGAQMGQYNJWSQKYULOGACPVUGK
```

Sample Output 2

```
NCTUCS
ONCEUPONATIMETHEREWASALITTLEGIRLWHOLIVEDINAVILLAGENEARTHEFOREST
WHENEVERSHEWENTOUTTHELITTLEGIRLWOREAREDRIDINGCLOAKSOEVERYONEI
NTHEVILLAGECALLEDHERLITTLEREDRIDINGHOODONEMORNINGLITTLEREDRIDIN
GHOODASKEDHERMOTHERIFSHECOULDGOTOVISITHERGRANDMOTHERASITHADB
EENAWHILESINCETHEYDSEENEACHOTHERTHATSAGOODIDEAHERMOTHERSAIDSO
THEYPACKEDANICEBASKETFORLITTLEREDRIDINGHOODTOTAKETOHERGRANDMOT
HERWHENTHEBASKETWASREADYTHELITTLEGIRLPUTONHERREDCLOAKANDKISSED
HERMOTHERGOODBYEREMEMBERGOSTRAIGHTTOGRANDMASHOUSEHERMOTHE
RCAUTIONEDDONTDAWDLEALONGTHEWAYANDPLEASEDONTTALKTOSTRANGERS
THEWOODSAREDANGEROUSDONTWORRYMOMMYSAIDLITTLEREDRIDINGHOODI
LLBECAREFULBUTWHENLITTLEREDRIDINGHOODNOTICEDSOMELOVELYFLOWERSI
NTHEWOODSSHEFORGOTHERPROMISETOHERMOTHERSHEPICKEDAFEWWATCHE
DTHEBUTTERFLIESFLITABOUTFORAWHILELISTENEDTOTHEFROGSCROAKINGANDT
HENPICKEDAFEWMORELITTLEREDRIDINGHOODWASENJOYINGTHEWARMSUMME
RDAYSOMUCHTHATSHEDIDNTNOTICEADARKSHADOWAPPROACHINGOUTOFTHEF
ORESTBEHINDHER
```

■ Hand in & Deadline

Upload your source code on **e3** before 23:59:59 on **October 20th. No late submission.**

■ Grading Policies

Pass two sample tests --- 60%

Pass another two extra tests --- 40%

No copying from others (or the Internet), or you will fail in this course.