Assignment 1

Due Date: September 26th, 2022

1. Encryption and Decryption

Write a program that can perform the following:

- Encrypt/Decrypt using Caesar or Vigenere cipher or playfair cipher based on user's selection.
- Programming to be done in **C/C++ language only**.

Description:

The program should first prompt the user for the type of encryption routine (Caesar or Vigenere Cipher or playfair cipher) he wants to use. It should then ask the user if he wants to encrypt or decrypt and also the KEY to be used. The program should read the plaintext/cipher text from a file called *process.txt.* The file *process.txt* will have either plaintext/cipher text as the case may be. The file *process.txt* will be placed in the same folder as your program.

2. Cryptanalysis:

Write a program to perform cipher-text only attack on Caesar and Vigenere cipher. The program should print the plain text as well as the key used for encryption. Cipher-text for each scenario is provided below. Use the cryptanalysis techniques discussed in the class. The program should also measure and print the processing time. You can use library function to measure execution time. You can safely assume that the alphabet ***A*** consists of only {a-z}. ***Brute force attacks won't be accepted as a solution.***

2.1 Caesar Cipher:

MUYDJUDTJERUWYDEDJXUVYHIJEVVURHKQHOKDHUIJHYSJUTIKRCQHYDUMQHVQH
UMUIXQBBUDTUQLEHYDIFYJUEVJXYIJEAUUFJXUKDYJUTIJQJUIEVQCUHYSQDUKJHQB
YDJXUULUDJEVJXYIDEJIKSSUUTYDWMUCQAUCUNYSEQFHEFEIQBEVQBBYQDSUEDJX
UVEBBEMYDWRQIYICQAUMQHJEWUJXUHCQAUFUQSUJEWUJXUHWUDUHEKIVYDQ
DSYQBIKFFEHJQDTQDKDTUHIJQDTYDWEDEKHFQHJJXQJCUNYSEYIJEHUSEDGKUHJXU
BEIJJUHHYJEHOYDJUNQIDUMCUNYSEQDTQHYPEDQJXUIUJJBUCUDJYDTUJQYBYIBUVJ

JEOEKOEKMYBBYDVEHCJXUFHUIYTUDJEVJXUQRELUCEIJIUSHUJBOQIIEEDQIJXUEKJRH
UQAEVMQHMYJXJXUKDYJUTIJQJUIEVQCUHYSQYISUHJQYDQDTQTTJXUIKWWUIJYEDJ
XQJXUIXEKBTEDXYIEMDYDYJYQJYLUYDLYJUZQFQDJEYCCUTYQJUQTXUHUDSUQDTQJJ
XUIQCUJYCUCUTYQJURUJMUUDZQFQDQDTEKHIUBLUIFBUQIUSQBBJXUFHUIYTUDJIQ
JJUDJYEDJEJXUVQSJJXQJJXUHKJXBUIIUCFBEOCUDJEVEKHIKRCQHYDUIDEMEVVUHIJX
UFHEIFUSJEVSECFUBBYDWUDWBQDTYDQVUMCEDJXIJECQAUFUQSU

Assume the following letter frequencies: [Given as fractions. Multiply by 100 to get percentages]. You may hardcode this info into an array in your C/C++ program.

{ "A": .08167, "B": .01492, "C": .02782, "D": .04253, "E": .12702, "F": .02228,

"G": .02015, "H": .06094, "I": .06996, "J": .00153, "K": .00772, "L": .04025,

"M": .02406, "N": .06749, "O": .07507, "P": .01929, "Q": .00095, "R": .05987,

"S": .06327, "T": .09056, "U": .02758, "V": .00978, "W": .02360, "X": .00150,

"Y": .01974, "Z": .00074 }

2.2 Vigenere Cipher text:

XUMGGVZINUHRDENSCMDCRREMCGUQNGXUMYVLBCGJXVBWCWPWMRPRBENCVV
DGGVXHGVNJLGXUMGGVZINOEPPIPIJISMRBENCWRVIIQNQTTIFMMDPRLAVCCMWT
MGMRVLNBCQYYLPTSQCCGLVOHNCRVCTCCBEFXRFTOIFAAIIFBOWWRBHGIAQGOEG
PEQTRZAVSENITWGBYRIQBHGXRFTVLRVBAXHZNKRTIFGAJPEGPFBHGCPWUNHFKRC
QOTEVLRUEUWNOEVLEWUILGPEOEPPIPIBVTJIEMCGMIQNIIALTJIBBHGVBXETEGWRY
SHTDPIRLTQWRBTJIVZMCGUQNGAVBHVLRAAOIJPEGPBZRQXBZOTHRZTQYAACTEZJL
GXUMMGWFIGGGBLEDSBSSYIEMDKWGZIDYGMDVSZMSUETMORIEITQVFAOVLNBTJI
LKOWPQMNVIEQNVLRKOTVRKTFIPZYRXVWNMILEHGREMCGMIQNIEGZAPWZQSUMB
VOTMTQNCPYGTJIRVIIQNPAFFRMNKRIMNVIQNOTGBUMGVPQANTHZPQWRABGJBZ
EVLROETQNVMKPVBATCFIWKXFWBXMBCSRSGMNVMNTIPXUMOTCVNTJITMROEAA
HCHFBUEOGWSVVBVGUXNVDCVQQZGHBXETEGQNITEWCGHHZEUXUMITGBLEUABC
LFMALEGHUIVGTEWVGRNTMQWGQMRSFAIDPRBOFIPQPJIEPOYIIMRVLRGBGGNUEE
EEMLGWFEHGRVBCCQRBOVLVAAUTRKTYLVKHWPGQMCXRTYDIPIMGXUMMCMAEE
COAMSUXUITJIYXEFXUMANPVMSVSQMCTCCBTJIPWDGWNATJITMROEABRQSCAWG
VRITVEPSIPKSISVEALRGPRVTNIFALAMGJEEEZMVKXNTFQVGPECPYQEUXBQNVIEKERX
NVDFIPZYRXGPEKVVVTGPYQGGRPMAVXUMEPHBNTJMEBYVABBHGGVXHGVOCRGEH
QNRSYINFSOBAKRRLAPIAQGOEZICJMAMTJILAHCVRLTJIVZIPJBZMCXVWNYMGPTJIOZI

VMFPAPHSZEPGUBOFIIMLQTPWDGFEMAMMAOTGGUVISYRATQGEMAVINLEFMPITG
HRNFQVGBOYEELSVLVAEPHGPEDVVBIULTWVGVAUEPXFMTWTGPEESQMAPHPQPJIE
ACJSBTLQGNBEFMAJUEOVVGJEZAHKVRJLGXPPLGCCIRMXUMRGXUMYDVBCGJXVVEZ
TRZTUMAUAVLRUAVMPALQKVKAPHCZODPRUSQPIQNIXUMSGRRERGGECIVWJWRMI
QBOIIGPETXBKRGEGMPTSGWTATRAOHIYMCVVBVIEQNKHKRRACQQCIRCFYMTQGBU
PWXRZSVSCZOFYPMDGGEGPVMBVOPEYIRIIEINFJNATGVFKANIGPEAORXTVLRAEGJS
WRVWUQGJPLAEEVRBIXIFWTJEGEOTHJWUNHAWTNINSTQXUMGGVZINHSEKEUWG
QLNFRTIGZVVGVLRQRESQMSVSOMFWPYGSGGHZEVLROETQNVSJEQJYVLVATKQRIDQ
TGMDVLRMNKKZICKTUMRUAVBHKRGPEKVNZMARNDYCMENOTGRINFWRKRGXFMR
XMPMS.KRGPEGEETYFELAAHIJKIRLRZSYIEMCTEPSEFFHBRGZRILGHYQTVPRPENTSCLK
RSWROEGQOP.MA1941VEYHRKRATGQOPWEMVGEYMDKRSWROEGQOPEOWUVKRZ
MCRLXLCRFNOTMADAFMAOGTIRKEUSBVAHXRZTJIRFPGVGAAVFYMTELYMYFIPZYRXR
LSGGEMTKRGMLNMTMNEIEMGCVQQNIXUMIVEYQAPRNDYTIFCLVMAOIPEAILNMRLV
KGGWRAHHZIPKGPEDEGBLGSSKARIZITCTNV