COMP 443 / 543 – Fall 2022 - Project #1
Due: 06.11.2022 11:59 PM

- *By submitting this assignment, you agree to fully comply with the course syllabus and the Koç University Student Code of Conduct.*
- *Projects that are submitted after the due time will NOT be graded.*
- *Check the provided helper.py file for the frequency analysis dictionary.*
- *You can use any programming language.*
- *You have to submit one script for each question. In total you have to submit two scripts. Name the scripts as q1_studentID and q2_studentID. You do not need to submit the txt files but make sure that your scripts write the correct outputs to a txt file.*

1. (**40 pts)** Below ciphertext was encrypted with a shift cipher (similar to the Caesar method with a key *k* between 0 and 25). Write a program to try all possible shifts on the ciphertext below, select the right one and output the plaintext and the correct key to a txt file. Name the file as q1_studentID.txt, first line should be the key and second line should be the plaintext. You can use any programming language you like.

   "kyivv izexj wfi kyv vcmve-bzexj leuvi kyv jbp, jvmve wfi kyv unriwcfiuj ze kyvzi yrccj fw jkfev, ezev wfi dfikrc dve uffdvu kf uzv, fev wfi kyv urib cfiu fe yzj urib kyifev; ze kyv creu fw dfiufi nyviv kyv jyrufnj czv. fev izex kf ilcv kyvd rcc, fev izex kf wzeu kyvd, fev izex kf sizex kyvd rcc, reu ze kyv uribevjj szeu kyvd; ze kyv creu fw dfiufi nyviv kyv jyrufnj czv."

2. **(60 pts)** The following was encrypted using the Vigènere cipher:

   "Fwg atax: P'tx oh li hvabawl jwgvmjs, nw fw tfiapqz lziym,
   rqgv uuwfpxj wpbk jxlnlz fptf noqe wgw.
   Qoifmowl P bdg mg xv qe ntlyk ba bnjh vcf ekghn
   izl fq blidb eayz jgzbwx sqwm lgglbtqgy xlip.
   Pho fvvs ktf C smf ur ecul ywndxlz uv mzcz xxivw?
   Qomdmowl P bgzg, oblzqdxj C swas,
   B kyl btm udujs dcbfm vn yg eazl, pqzx,
   oblzq Q'ow mwmzb lg ghvk gxslz, emamwx apqu, wwmazagxv nomy bhlustk."

   Ghm qvv'f nbfx h vqe vgoubdg, pgh'a nuvw shvbtmk kbvzq.
   Baam jqfg pafs ixetqm wcdanw svc.
   Kwn'df dixs mzy ziym llllmfa, zjid wxl
   bf nom eifw hlqspuglowall, loyv sztq cu btmlw mhuq phmmla.
   Kwn'df htiirk yul gx bf noqe kbls. Kwz'b agjl naz mzcuoe mekydpqzx:
   lblzq'a gg moqb nhj svc, fpxjy'z va zhsx.
   Uwi basn fwg'dx ouzbql rgoy tunx zyym, uv mzcz ayied wvzzmk,
   qib'dq lxknywkmw an ldqzroblzq qg lbl eazev."

Attack it and find the plaintext and the key. Note that only the letter characters are encrypted. You have to use frequency analysis. You can use the dictionary provided to you for the letter frequencies. Output the plaintext and the correct key to a txt file. Name the file as q2_studentID.txt, first line should be the key and second line should be the plaintext. You can use any programming language you like.

(*Hint:* First you have to find the key length k. Then group ciphertext into k equivalence classes and perform frequency analysis for each class. For example: let ciphertext = “FUNHOMEWORK” and k = 3 equivalence classes are as follows: c1 = “FHER” c2= “UOWK” c3 = “NMO”)