National Technical University of Athens
School of Electrical and Computer Engineering

Computational Cryptography

(ECE, SEMFE, ALMA, AMS)

1st Exercise Set

Deadline: November 3rd 2022

Question 1. Below you are given a ciphertext of an English text encrypted using a substitution cipher.

```
ODQSOCL OW GIU BOEE QRROHOCS QV GIUR KIA QF Q DQCQSLR WIR ICL IW CQFQF EIYQE YIDJUVLR
FGFVLDF GIU SLV OCVI GIUR IWWOYL IC VXQV DICPQG DIRCOCS VI WOCP VXL JXICLF ROCSOCS
LHLRG YQEELR OF Q POFVRQUSXV YICWUFLP CQFQ BIRMLR QCP LHLRG YQEELR QFFURLF GIU VXQV
XOF IR XLR WOEL IR QYYIUCVOCS RLYIRP IR RLFLQRYX JRIKLYV LHLRG ICL IW BXOYX OF DOFFOCS
WRID VXL YIDJUVLR FGFVLD OF QAFIEUVLEG HOVQE
```

You are tasked with writing a program in Python, C/C++, Java, or any other programming language of your choice in order to decrypt the above ciphertext. What is the corresponding plaintext, and what encryption key was used ?

Question 2. The texts given below were produced by using an affine cipher, and the latin alphabet. Your task is to find the encryption and decryption functions, by utilising the correspondence between two letters of the ciphertext and the plaintext.

- (a) The ciphertext is LNUWN CZCZY CWWQM HI, and the ciphertext letters C and N correspond to I and H, respectively, in the plaintext.
- (b) The ciphertext is COGCZ JSSNO FYGCZ, and the ciphertext letters S and Z correspond to E and T, respectively, in the plaintext.
- (c) The ciphertext is YLNNY ELQXP HSNSY N, and the ciphertext letters L and N correspond to N and D, respectively, in the plaintext.
- (d) The ciphertext is TSDRG DOFES RGBDF MXMEX, and the ciphertext letters S and G correspond to U and O, respectively, in the plaintext.

Question 3.

1. Consider a cipher which has the property of perfect secrecy, is it required for every key to be chosen with the same probability? Does anything change if the Message, Key, and Cipher spaces have the same cardinality? Prove your claims vigorously.

2. Prove that the following sentences are equivalent to Shannon's perfect secrecy definition:

   i. $\forall x \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y] = \Pr[C = y | M = x]$

   ii. $\forall x_1, x_2 \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y | M = x_1] = \Pr[C = y | M = x_2]$

Question 4.

i. Two friends want to enhance the security of the Vigenère cipher. They came up with the following idea: They will augment the key with an integer k, every time the key runs through its period they will shift the key by the integer k.

   (a) Argue whether or not this change yields a more secure cipher. Are there any choices for k which work better than others? Explain your reasoning.

   (b) By taking into account only how the new cipher works try to come up with an efficient attack to break it.

ii. What is the product of two Vigenère ciphers with distinct key lengths?

Note: the two questions i and ii don't have anything in common other than the fact that they have to do with the Vigenère cipher.

Question 5.

Below you are given a text which is encrypted using the Vigenère cipher. You are tasked with writing a program in Python, C/C++, or any other language of your choice, using common libraries (i.e. not a subroutine which solves the cipher directly), which on input a ciphertext will produce the ten most likely plaintexts along with their corresponding keys. In addition the program will output the Index of Coincidence of each plaintext.

There should also be included a text which will describe the basic functions of your code.

Input ciphertext:

```
Mlrec dwrl xur ngfg; mlr ickgre thsdk vrk wnvj: Lvrki tymga gai qnpc, peheq fcsg.
Zr qnegfsel, Wbhjk hutx untw hbbp'q, nlv kehytur, sbq mlbhezh jbxu zc- Lvnm iirp
owga e semdwp piypmes ghsx Gfw hunrqrp sbq mlr fsfgubrr, nlv ccisfrb Xfrx lrnplg,
skir smjsuxeqf-wgi ngh V npw cyw; Syq yys utxu lcl vvl lbammf ngh uvq lcve; Hrnrz
qyhwrf ydz: onx fbkwhubrt rpw hux iaq, Qgar psex mx bbupr amls, ztc lrr ts qhrr,
Aml iauipbkabt fia gfsh fmvbic owga Kbqq. Lvr emturk przma gm lkvgoyr djcz mlr emuyf:
Mlr ymfu qtc jnlwg: gai fymo abhr pygepf: mlr qcwd Zheaf pgiaw avgf eoar zbvawg.
Phqr, zw xfvxrqf, 'R ag ahx gbm dogx xb fcwy n gijrp oceeh. Chqz csy, eaq qahgbrt
jcdz vg seqcj gzbxr Gfw gbnrqvly thkvbjq; xce fc chphcfx lbybk Hb levy zwmbgh guc
```

kialig, nlv hux fngfk Cs tpy gfw krlxrel khnkw, haraz V wmr. Vr eol ui guyl hux khydk kvep jnqz if wsja: Gl anr fr jc kvnep gbsuv gai Unnhm Vlprf, Yfr fxi guc yfrtx Npfazyxw, jume kr drrj. Rzc' zngu vq loxxr, zhaz oobhrf; yfr gas' Jr yjs ahx abu lvnm wgecfuga auvaz wa hpq qyqg Zhzrq csfga eaq fwoixr, guyl kubgu jc sfr, pi nec; Gbr xuhnj lsziie bd zsehmp ucsfgl, Qnqc osnd fl gges ngh snrw, phm wgemfu vg avyj Lc fmvvic, lc fxix, gm xwaw, eaq lgh gh cvrjv.

The output of the program should look something like this: KEY1 PLAINTEXT1 IC1
KEY2 PLAINTEXT2 IC2
KEY3 PLAINTEXT3 IC3
KEY4 PLAINTEXT4 IC4
... (and so on for at most 10 lines)

Other ways of solving the exercise are allowed, however you might receive a lower mark. In addition you should explain the way you solved the exercise. You are not allowed to use a Vigenère decoder, however you can utilise online calculators for Index of Coincidence.

Best of Luck !