Understanding Cryptography **Homework No. 1** **Due Date:**

Solve the following exercises in your textbook "Understanding Cryptography":

Exercise 1.8, 1.9, 1.10 and 1.11.

Do the following projects with the useful program "CrypTool".

EX1. The Vigenere cipher is a method of encrypting alphabetic text by using a series of different Ceasar ciphers based on the letters of a keyword.

a) Search about the history of Vigenere cipher and write a text which contains more than 500 words about it (Note that your text only contains the letters of English alphabets).
b) Considering the mapping between the elements of $\mathbb{Z}_{26}$ and the letters of English alphabet, make your keyword of Vigenere cipher as follows:
   1. Make a 17-digits sequence by concatenating your national ID-number and IUT student number.
      EXP: 12198912649007575
   2. Calculate your student number modulo 17.
      EXP: $x = 9007575 \; mod \; 17 = 6$
   3. Remove the $(x+1)$th digit of the 17-digits sequence in step 1. Then you have a 16-digits sequence.
   4. EXP: $6 + 1 = 7 \quad \longrightarrow$ We must remove the 7th digit: 1219892649007575
   5. Do the following for each couple of your 16-digits sequence. Find its equivalent modulo 26, and then map it to the equivalent English letter, as follows:

1219892649007575	12 19 89 26 49 00 75 75	12 19 11 00 23 00 23 23
Your 16-digits sequence	Modulo 26 equivalents	Mapping to the English alphabets
	12 19 11 00 23 00 23 23	M T L A X A X X

   Use these English letters as your keyword. (EXP: MTLAXAXX)
c) Now you can encrypt your text in part (a) of this exercise using the following sequence of items in the main menu in CrypTool:
   Crypt/Decrypt :: Symmetric (classic) :: Vigenere ...
   In the dialog box you need to specify your encryption key. Use the key you obtain in part (b) and then press the encryption button
d) Now, try to break the cipher text by CrypTool:
   Analysis :: symmetric Encryption (classic) :: Ciphertext-only :: Vigenere
   Has CrypTool broken the cipler text correctly?
e) Now use a totally random key with a much longer length (for example 50 letters) to encrypt your text. Then analyze the cipher text and check whether CroopTool can break your cipher or not?
f) Save all your answers and results in one file.

EX2. In this exercise, we want to encrypt your text in the previous exercise with a substitution cipher.

a) Consider unrepeated letters in your keyword in part (b) of the previous exercise concatenated with your unrepeated letters of your first and last name and make your key for this exercise as follows:
   EXP: My keyword in the previous: MTLAXAXX
   My name: PARVIN RASTEGARI
   My keyword for this exercise: MTLAXPRVINSEGBCDFHJKOQUWYZ
b) Now, encrypt your text in the previous exercise by your key in part (a):
   Crypt/Decrypt :: Symmetric (classic) :: Substitution / Atbash
c) Find the relative frequency in your plain text and compare it with a reliable table of relative frequencies of letter in English language (page 9 of your book). Then find the relative frequency in your cipher text and try to match the English letters with their encrypted counterpart. You can use the following sequence of items in the main menu in CrypTool:
   Analysis :: Tools for Analysis :: N-Gram…
d) Now, use CrypTool to break the cipher:
   Analysis :: symmetric Encryption (classic) :: Ciphertext-only :: Substitution
   Did CrypTool succeed in this case??
e) Briefly explain the difference between the two methods which is used in substitution analysis (the two methods which are mentioned in the first dialog box of the substitution analysis window).
f) Can CrypTool break the following cipher? (with each of two methods). If no explain why?

```
lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt
```

Can CrypTool break the following cipher? (with each of two methods).

```
lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt

wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb
```

g) Find the table of relative frequencies of letter in Persian language and compare it with table of relative frequencies of letter in English language.

EX3. Thank to a very smart spying and eavesdropping mission, we gained to a piece of plain text and a cipher text which is encrypted with an unknown key with HILL cipher:

Plain Text	Cipher Text
If a man is offered a fact which goes against his instincts, he will scrutinize it closely, and unless the evidence is overwhelming, he will refuse to believe it. If, on the other hand, he is offered something which affords a reason for acting in accordance to his instincts, he will accept it even on the slightest evidence. The origin of myths is explained in this way.	Fq i fmk kf jnfkkvd t zfco hnzaw ikwy erzscpf hop jjsmdzklk, lf ozbi tkbytbnvhu vv dbwvbtx, qcm atsqor dyf ofynbmry sl kbwzlrnzwxxz, di jtlv dnughp zs bajndrj gc. Yk, tw pvn pfsaj kiur, ru lj wbsmkro ojscroiub wxugk kpkmhgv q vmlxhq rxn effnhs ti zsgpmkuzci lw xfj dqtcabmtt, oe hxnc roqtmm el yrei lz fqr cvurxcfkb uztjxbid. Tyv sjfzci nb fplwa hr helgvqdsi hc xulc wba.ICAK

Use this pair to break the following cipher:

Thg xiwxv oxlpssjseme omxch gnfz tx oqevs uqsr w mnihzj ocw ij tgav kgbzvq vi vr rxlihc ysax p hcjgzh poe.