ECE4802/CS4801 Assignment 1

- Due: 11:59 pm on Nov 7, 2018 (submit a soft copy via Canvas)

1. The ciphertext printed below was encrypted using a substitution cipher. The objective is to decrypt the ciphertext without knowledge of the key.
   a. Provide the relative frequency of all letters A...Z in the ciphertext.
   b. Decrypt the ciphertext with help of the relative letter frequency of the English language (e.g., search Wikipedia for letter frequency analysis). Note that the text is relatively short and might not completely fulfill the given frequencies from the table.
   c. Find the key and provide letter frequency for the given text.

Ciphertext:

```
CKCLBAELDK DGJ LFNSMBCA CGQEGCCAI JCUCKFS DGJ LACDBC SAFJMLBI BHDB LHDGQC
BHC OFAKJ DGJ NDVC FMA KEUCI CDIECA BHC LCKK SHFGCI OC JCSCGJ FG BHC LFNSMBCAI
MICJ EG GDBEFGDK ICLMAEBR DGJ BHC CKCLBAELDK IRIBCNI BHDB NDVC FMA LDAI
FSCADBC OCAC DKK LACDBCJ TR CKCLBAELDK DGJ LFNSMBCA CGQEGCCAI DB OSE OC
VCCS BHDB SAFQACII NFUEGQ PFAODAJ OEBH FMA EGGFUDBEUC ACICDALH DGJ FMB-FP-
BHC TFY DSSAFDLHCI BHC JCSDABNCGB FP CKCLBAELDK DGJ LFNSMBCA
CGQEGCCAEGQ DB OSE LHDKKCGQCI IBMJCGBI BF SMIH BHCNICKUCI BF MGJCAIBDGJ
IFLECBRI DGJ BCLHGFKFQRI LFNSKCY EIIMCI EG D TAFDJCA LFGBCYB BHDG OHDBI EG
PAFGB FP BHCN OC ODGB FMA IBMJCGBI OHCBHCA BHCR DAC CDAGEGQ DG
MGJCAQADJMDBC NEGFA FA D JFLBFADBC BF BDLVKC IFLECBRI NFIB SACIIEGQ SAFTKCNI
DGJ MGLFUCA GCO ODRI FP IFKUEGQ BHCN OHCBHCA EBI JCUCKFSEGQ IRIBCNI BHDB LDG
KFLDBC PEACPEQHBCAI EG BHC NEJJKC FP D TMAGEGQ TMEKJEGQ FA LACDBEGQ
GCMAFSAFIBHCBELI BHDB KFFV DGJ PMGLBEFG KEVC GDBMADK KENTI FMA PDLMKBR DGJ
IBMJCGBI DAC DB BHC PAFGB CJQC FP ACNDAVDTKC EGGFUDBEFG OHEKC DJUDGLEGQ
BCLHGFKFQECI EI DB FMA LFAC OC DKIF BDVC HMNDG LFGGCLBEFGI UCAR ICAEFMIKR EG
CLC OC SAEJC FMAICKUCI FG BHC PDNEKR-KEVC DBNFISHCAC OC LMKBEUDBC; PDLMKBR
IBMJCGBI DGJ IBDPP CGLFMADQC CDLH FBHCAI CUCAR IMLLCII DGJ DAC BHCAC PFA BHC
LHDKKCGQCI TFBH EG BHC LKDIIAFFN DGJ EG KEPC
```

2. Modular arithmetic is the basis of many cryptosystems. As a consequence, we will address this topic with several problems in this and upcoming chapters.
   a. Compute the results:
      i. $27 \cdot 13 \ mod \ 23$
      ii. $17 \cdot 13 \ mod \ 23$
      iii. $28 \cdot 15 \ mod \ 12$
      iv. $15 \cdot 29 + 11 \cdot 15 \ mod \ 23$

   b. Find the inverses in the given modular spaces:
      i. $4^{-1} \ mod \ 17$
      ii. $7^{-1} \ mod \ 17$
      iii. $5^{-1} \ mod \ 37$
      iv. $10^{-1} \ mod \ 15$

3. List all elements of modulo 36 with no multiplicative inverse.

4. An LFSR is given by $(9, (C_0, C_1, \cdots, C_9), (Z_0, Z_1, \cdots, Z_9)) = (9, \mathrm{x}^8 + x^6 + x^5 + x^4 + 1, (0,0,0,1,1,0,1,0,0))$.*
   a. Draw a circuit diagram for the given LFSR.
   b. Compute first 30 bits of the output bit stream
   c. Use Vernam Cipher to encrypt the following plaintext using the bit stream generated in part b.
      P=`111011000001101110110100111110`

   *Given polynomial is 8th degree irreducible polynomial.