

ECE4802/CS4801 Assignment 1

* Due: 11:59 pm on Nov 6, 2020

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 SAFTKCNIG DGJ MGLFUCA GCO ODRI FP IFKUEGQ BHCN OHCBHCA EBI JCUCKFSEGG
IRIBCNI BHDB LDG KFLDBC PEACPEQHBCAI EG BHC NEJJKC FP D TMAGEGQ TMEKJEGQ FA
LACDBEGQ GCMASFSAFIBHCBELI BHDB KFFV DGJ PMGLBEFG KEVC GDBMADK KENTI FMA
PDLMKBR DGJ IBMJCGBI DAC DB BHC PAFGB CJQC FP ACNDAVDTKC EGGFUDBEFG OHEKC
DJUDGLEGG 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. Do the followings for the given LFSRs.

- i. $(m, \text{gate positions}, \text{intial state}) = (9, (C_0, C_1, \dots, C_7, C_8), (Z_0, Z_1, \dots, Z_7, Z_8)) = (9, (1, 0, 1, 0, 0, 0, 0, 1, 1), (0, 0, 0, 1, 1, 0, 1, 0, 0))$.
- ii. $(m, \text{gate positions}, \text{intial state}) = (9, (C_0, C_1, \dots, C_7, C_8), (Z_0, Z_1, \dots, Z_7, Z_8)) = (9, (0, 0, 1, 0, 0, 0, 0, 1, 1), (0, 0, 0, 1, 1, 0, 1, 0, 0))$.

- a. Draw a circuit diagram for the given LFSR.
- b. What is the maximum length of the key stream this LFSR can produce?
- c. Compute first 30 bits of the output bit stream
- d. Use Vernam Cipher to encrypt the following plaintext using the bit stream generated in part b. P=`111011000001101110110100111110`