ECE/CS 578 Assignment 1

* Due: 11:59 pm on Sept 18, 2023 (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; frequencies may not exactly match those listed in Wikipedia or elsewhere.
   c. Find the Plaintext/Ciphertext letter pairs, alphabetized by plaintext.
   d. Provide letter frequency for the given plaintext.

Ciphertext:

AKALBIELCK CFJ LDNSMBAI AFQEFAAIG JAUAKDS CFJ LIACBA SIDJMLBG BHCB LHCFQA BHA ODIKJ CFJ NCVA DMI KEUAG ACGEAI BHA LAKK SHDFAG OA JASAFJ DF BHA LDNSMBAIG MGAJ EF FCBEDFCK GALMIEBR CFJ BHA AKALBIELCK GRGBANG BHCB NCVA DMI LCIG DSAICBA OAIA CKK LIACBAJ TR AKALBIELCK CFJ LDNSMBAI AFQEFAAIG CB OSE OA VAAS BHCB SIDQIAGG NDUEFQ PDIOCIJ OEBH DMI EFFDUCBEUA IAGACILH CFJ DMB-DP-BHA TDY CSSIDCLHAG BHA JASCIBNAFB DP AKALBIELCK CFJ LDNSMBAI AFQEFAAIEFQ CB OSE LHCKKAFQAG GBMJAFBG BD SMGH BHANGAKUAG BD MFJAIGBCFJ GDLEABRG CFJ BALHFDKDQRG LDNSKAY EGGMAG EF C TIDCJAI LDFBAYB BHCF OHCBG EF PIDFB DP BHAN OA OCFB DMI GBMJAFBG OHABHAI BHAR CIA ACIFEFQ CF MFJAIQICJMCBA NEFDI DI C JDLBDICBA BD BCLVKA GDLEABRG NDGB SIAGGEFQ SIDTKANG CFJ MFLDUAI FAO OCRG DP GDKUEFQ BHAN OHABHAI EBG JAUAKDSEFQ GRGBANG BHCB LCF KDLCBA PEIAPEQHBAIG EF BHA NEJJKA DP C TMIFEFQ TMEKJEFQ DI LIACBEFQ FAMIDSIDGBHABELG BHCB KDDV CFJ PMFLBEDF KEVA FCBMICK KENTG DMI PCLMKBR CFJ GBMJAFBG CIA CB BHA PIDFB AJQA DP IANCIVCTKA EFFDUCBEDF OHEKA CJUCFLEFQ BALHFDKDQEAG EG CB DMI LDIA OA CKGD BCVA HMNCF LDFFALBEDFG UAIR GAIEDMGKR EF ALA OA SIEJA DMIGAKUAG DF BHA PCNEKR-KEVA CBNDGSHAIA OA LMKBEUCBA; PCLMKBR GBMJAFBG CFJ GBCPP AFLDMICQA ACLH DBHAIG AUAIR GMLLAGG CFJ CIA BHAIA PDI BHA LHCKKAFQAG TDBH EF BHA LKCGGIDDN CFJ EF KEPA

2. An LFSR is given by $[\mathrm{m}, (C_0, C_1, \cdots, C_9), (Z_0, Z_1, \cdots, Z_9)] = [10, P(x), (1,0,0,1,1,0,0,0,0,1)]$. Pick one polynomial for LFSR from the given list below.
   a. Draw a circuit diagram for the given LFSR.
   b. Compute the first 512 bits of the output bit stream. You can use any program of your choice.
   c. What is the period of the output stream?
   d. Encrypt the following 32-bit plaintext using the first 32 bits of the key stream generated above. P=`11101100000110111011010011111010`
   e. Decrypt the ciphertext you found in part d using the bit same key stream generated above.

List of Degree 10 polynomials

- $x^{10} + x^3 + 1$
- $x^{10} + x^4 + x^3 + x + 1$
- $x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$
- $x^{10} + x^8 + x^3 + x^2 + 1$
- $x^{10} + x^8 + x^4 + x^3 + 1$
- $x^{10} + x^8 + x^5 + x + 1$
- $x^{10} + x^8 + x^5 + x^4 + 1$
- $x^{10} + x^8 + x^7 + x^6 + x^5 + x^2 + 1$
- $x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$
- $x^{10} + x^9 + x^4 + x + 1$
- $x^{10} + x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $x^{10} + x^9 + x^8 + x^6 + x^3 + x^2 + 1$
- $x^{10} + x^9 + x^8 + x^6 + x^5 + x + 1$
- $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$
- $x^{10} + x^7 + x^6 + x^5 + x^4 + x^2 + 1$
- $x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + 1$
- $x^{10} + x^9 + x^3 + x + 1$
- $x^{10} + x^8 + x^7 + x^6 + x^4 + x$