ECE/CS 578 Assignment #1

- Due: 11:59 pm on Sept 15, 2025 (submit a soft copy via Canvas)
- Submit a record of your AI/LLM interactions. You may provide a shareable link if one is generated, or alternatively, upload a text file containing your interactions.

1. **Substitution Cipher:**
   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:

Vin ror Eqtlqk sgct iol eohitk lg dxei?
Wteqxlt oz dqrt iod ytts soat q ktqs lioyz stqrtk.
Yxf Yqez: Eqtlqk'l eohitk lioyztr tqei stzztk wn 3. Lodhst, wxz oz athz eqlxqs lfgghl qvqn ykgd iol dosozqkn gkrtkl.

Vin ror zit Lhqkzqf dtllqut sgga soat fgfltflt?
Wteqxlt oz vql zqatf gxz gy egfztbz (soztkqssn gyy zit lzoea).
Yxf Yqez: Q lzkoh gy hqkeidtfz vkqhhtr qkgxfr q kgr ktctqstr zit ztbz. Vozigxz zit kouiz kgr, zit stzztkl vtkt lekqdwstr.

Vin ror zit Qzwqli eohitk yqos ozl ztlz?
Wteqxlt oz qsvqnl uqct zit ghhglozt qflvtk.
Yxf Yqez: Qzwqli, ykgd qfeotfz Itwktv, lodhsn ysohl zit qshiqwtz (Q->M, W->N, tze.). Oz'l gft gy zit gsrtlz afgvf lxwlzozxzogf eohitkl.

Vin rgf'z Coutftkt xltkl tctk sglt qkuxdtfzl?
Wteqxlt zitn qsvqnl iqct zit sqlz atn.
Yxf Yqez: Xlofu q kthtqzofu atnvgkr, Coutftkt roluxoltr stzztk yktjxtfeotl, wqyysofu eknhzqfqsnlzl ygk etfzxkotl.

Vin vql zit Hsqnyqok eohitk wqr qz lhgkzl?
Wteqxlt oz egxsrf'z iqfrst lofustl.
Yxf Yqez: Hsqnyqok (1854) tfeknhzl hqokl gy stzztkl oflztqr gy lofustl. Oz vql xltr of VVO qfr VVOO ygk yotsr egddxfoeqzogfl.

Vin ol KGZ13 soat q wggdtkqfu?
Wteqxlt viqz ngx ltfr gxz qsvqnl egdtl wqea zit lqdt.
Yxf Yqez: KGZ13 lioyzl stzztkl wn 13. Tfeknhzofu zvoet ktzxkfl zit gkouofqs ztbz--lg rteknhzogf ol zit lqdt ql tfeknhzogf.

Vin vql zit gft-zodt hqr qsvqnl ofcoztr zg hqkzotl?
Wteqxlt oz vql htkytezsn ltexkt.

Yxf Yqez: Oy zkxsn kqfrgd qfr ftctk ktxltr, zit gft-zodt hqr ol xfwktqaqwst. Zit hkgwstd: liqkofu qfr atthofu zit hqrl ltektz.

Vin ror zit Tfoudq dqeioft iqzt ldqss zqsa?
Wteqxlt tctknziofu oz lqor eqdt gxz egdhsoeqztr.
Yxf Yqez: Vozi wossogfl gy hgllowst ltzzoful, Tfoudq lttdtr xfwtqzqwst. Qssotr eknhzqfqsnlol ekqeatr oz, liqhofu zit gxzegdt gy VVOO.

Vin ror zit Sgktfm eohitk wktqa xh vozi Tfoudq?
Wteqxlt oz vqfztr q wouutk vitts gy ygkzxft.
Yxf Yqez: Sgktfm LM dqeioftl, xltr wn Fqmo ioui egddqfr, vtkt tctf dgkt egdhstb ziqf Tfoudq. Wkozoli eknhzqfqsnlzl wxosz Egsgllxl zg ekqea zitd.

Vin rg eknhzgukqhitkl qsvqnl eqkkn lfqeal?
Wteqxlt zitn wtsotct of ltexkt eiohl.
Yxf Yqez: Zgrqn'l eohitkl ktsn gf iqkr dqzi hkgwstdl (soat yqezgkofu wou fxdwtkl gk dgrxsqk qkozidtzoe) oflztqr gy lodhst stzztk zkoeal.

2. **LFSR:**
   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

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