Homework – 3: (Due on October 29th in class)

1. Assuming an initial state of ($s_3 = 1$, $s_2 = 0$, $s_1 = 0$, $s_0 = 0$), determine the sequences generated by LFSR-s with the following polynomials:

   - $X^4 + X + 1$
   - $X^4 + X^2 + 1$
   - $X^4 + X^3 + X^2 + X + 1$

   What are the cycle lengths for the above three cases?

2. One important property that makes DES secure is that the S-boxes are non-linear. In this problem, we verify this property by computing the output of the S-box S1 for several pairs of inputs.

   Show that $S_1(X_1) \oplus S_1(X_2) \neq S_1(X_1 \oplus X_2)$, where $\oplus$ denotes bitwise XOR, for the following inputs:

   - $X_1 = 000000$, $X_2 = 000001$
   - $X_1 = 111111$, $X_2 = 100000$
   - $X_1 = 101010$, $X_2 = 010101$

3. What is the output of the first round of DES when the plaintext and key are:
   - Both all zeros
   - Both all ones

4. Use Likelihood Ratio Test (LRT) to decrypt the following text which was encrypted with a Shift Cipher:

   gyznkjgeycktzheznkkburazoutulroqkotzurubkcgygiikrkxgzkjcnozklgtmnosykrlhkmgtzumx
   ucgcgxkulozznuamnotnoyiutyiouaytkyynkqtkctuzcngzrubkcgyozsgtolkyzkjozykrlzunosgyg
   buojotnoyhkotmgnatmxeginotmekgxtotmbuojzngzirgsuaxkjzuhklorrkjozcgygvgotgtjgtatx
   kyzgtjozxkikobkjkgyksktzutreheznkzuainulznktkcmujoyvxkyktikgzyainzoskyrubkcgypuezu
   nosgcorjqkktznxorrotmygzoylgizouthazcnktgcgelxusnoymujznkvgotgtjznkatxkyzxkzaxtkjz
   nkbuojotnosyvxgtmavgtjvxkyykjgmgotyznoscoznozyksvzotkyygtjznknatmkxmtgckjgtjmtg
   ckjatikgyotmre

   [**Hint**: Compute the Log Likelihood Ratio (LLR) for the decrypted text for all possible shifts and find the shift which had the maximum value of the LLR. You will need to have the distribution of the characters under English (P_E) and under noise (P_N). The distribution P_E is given in Table 2.1 (page - 17) of the textbook.]