Project 1
Computer Security (CSCI 399)

Please give complete solutions with clear explanations. Credit will be based on both the *correctness* and *completeness* of your solutions.

Due Date: Please submit your work to **Canvas** by **9pm Feb 27th, 2022**.

---

(1) (20 points)Write a program to allow the user to encrypt and decrypt Vigenere ciphertext using a user-specified keyword. For example, `"MAYTHEFOURTHBEWITHYOU"` encrypts to `"XUIXSYPSFLDLMYGMEBISF"` using keyword `"LUKE"`. Demonstrate that your code works by decrypting the Vigenere ciphertext in `cipherKnownKey.txt` with the keyword `"TAGORE"` on Canvas.
(2) (30 points)Write a program to cryptanalyze Vigenere ciphertext when the keyword is *unknown*. Demonstrate that your code works by decrypting the Vigenere ciphertext in `cipherNoKey.txt` on Canvas.
(3) (30 points)Write a program to allow the user to encrypt and decrypt LFSR-based ciphertext using a user-specified key. Speed is very important for stream cipher design, so you are required to implement the stream cipher using bitwise operations. `LFSR.encrypted` was encrypted using the output bits directly from a single 8-bit LFSR with recursion relation $a_n = a_{n-4} + a_{n-5} + a_{n-6} + a_{n-8} \mod 2$ and initial fill `255=11111111`$_2$. Demonstrate that your code works by decrypting the ciphertext `LFSR.encrypted` on Canvas.

Deliverables:

(1) Code for encryption and decryption using Vigenere cipher and a decrypted file `plainKnownKey.txt`.
(2) Code for cryptanalysis and a decrypted file `plainNoKey.txt`.
(3) Code for encryption and decryption using LFSR-based stream cipher, a decrypted file `LFSR.decrypted`.