COMPSCI 4CR3 - Assignment 1

1. Recall that a Linear Feedback Shift Register (LFSR) of degree n is given by a recurrence relation $a_n = p_{n-1}a_{n-1} + \cdots + p_1a_1 + p_0a_0$ where $p_{n-1}, \ldots, p_1$ are called the coefficients. An LFSR (mod 2) is determined by a sequence of coefficient bits. For example, the sequence `110101` represents an LFSR of degree 6 in which $p_0 = 1, p_1 = 1, p_2 = 0, p_3 = 1, p_4 = 0, p_5 = 1$, so, the recurrence for this LFSR is

$$a_6 = a_5 + a_3 + a_1 + a_0 \pmod 2.$$

For the initial value of $a_0a_1 \ldots a_5 =$ `011001`, this LFSR produces the output

$$a_0a_1a_2a_3 \cdots = \texttt{0110010000100110010000100110010 0...}$$

Alice and Bob want to communicate securely using a stream cipher. They use a stream cipher that is based on an LFSR, i.e., the key bits are generated by an LFSR. They choose an LFSR of degree 20 given by coefficients `11010100010001101010` and initial value `00110110010101101111`. The coefficients are the secret key used by both parties, but the initial value is public.

   (a) (25 points) Perform the steps of the protocol on the plaintext

   `00111101011100111000000111001100010011010110110100`.

   The protocol consists of Alice generating the key bits and encrypting the plaintext, and then Bob generating the key bits and decrypting the ciphertext.

   (b) (25 points) Suppose Trudy somehow gains access to the output of the key stream (i.e., the output of the LFSR). Write down the steps Trudy would follow to compute the (secret) coefficients of the LFSR. Be sure to consider how many key bits Trudy would need to successfully perform this computation. Here, you will generate the necessary number of key bits using the LFSR described above.

   (c) (25 points) Instead of gaining access to the key stream, suppose Trudy gains access to the plaintext. Can Trudy still carry out the attack described in Part (b)? Explain.

2. (25 points) Recall the Affine Cipher from the lecture: for an alphabet of length m, where each letter is identified with an element of $\mathbb{Z}_m$, the key is a pair $(a, b) \in \mathbb{Z}_m$. A plaintext $x \in \mathbb{Z}_m$ is encrypted using the transform $ax + b \bmod m$, and a ciphertext $y \in \mathbb{Z}_m$ is decrypted using the transform $a^{-1}(y - b) \bmod m$. Is this encryption scheme vulnerable to the frequency analysis attack? Explain.