*UBI523 Cryptosystems and Cryptographic Protocols*

*Fall2018*

*Homework #2*

*Due Date: Oct. 15th 2018*

**2.6.** Assume we have a stream cipher whose period is quite short. We happen to know that the period is 150-200 bit in length. We assume that we do not know anything else about the internals of the stream cipher. In particular, we should not assume that it is a simple LFSR. For simplicity, assume that English text is ASCII format is being encrypted.

Describe in detail how such a cipher can be attacked. Specify exactly what Oscar has to know in terms of plaintext/ciphertext, and how he can decrypt all ciphertext.

**2.10.** We conduct a known-plaintext attack on an LFSR-based stream cipher. We know that the plaintext sent was:

1001 0010 0110 1101 1001 0010 0110

By tapping the channel we observe the following stream:

1011 1100 0011 0001 0010 1011 0001

1. What is the degree m of the key stream generator?
2. What is the initialization vector?
3. Determine the feedback coefficients of the LFSR?
4. Draw a circuit diagram and verify the output sequence of the LFSR.