Introduction to Cryptography—Homework 2
Due: Saturday, February 20, 2021, 11:59pm

- You may work on and submit your homework in **groups of 2** or individual.
- Submit your solutions to the appropriate dropbox folder on myCourses as single (readable) pdf file and a single python file (2 files total).
- The homework must be entirely your own work.
- Before you start on the homework, please read the rules on collaboration and submission in the syllabus.
- Keep in mind that, as stated in the syllabus, I will not answer e-mail questions the day the homework is due.
- Each homework problem indicates the number of points it is worth for grading purposes. While individual problems may be worth more or fewer points than others, each homework assignment carries weight as stated in the syllabus.

1. **(2 points)** Use Euclidean algorithm to find $gcd(65610, 10920)$. Show the details of computations.

2. **(4 points)** Let $n = 301 \times 463$. Implement the Blum-Blum-Shub generator to compute the first 42 bits of the generated output. Use seed $x_0 = 100001_2 = 33$.

   a) What is the sequence of keystream bits?

   b) Decrypt the ciphertext:

   $$011000000100101000011101000111111010100011$$

   encrypted with stream cipher and key stream generated in a). Each plaintext message is a sequence of characters; each character is represented as an **7-bit** binary number using the ASCII character encoding. What is the plaintext (in 7-bits ASCII character encoding)?

3. **(4 points)** Alex and Blake are encrypting messages using RC4. You, Harry the Hacker, are eavesdropping on their communications. Each plaintext message is a sequence of characters; each character is represented as an 8-bit binary number using the ASCII character encoding. Alex and Blake are using the same key to encrypt every message. Because RC4 does not define how to incorporate a nonce into the keystream generator algorithm, Alex and Blake are using this (insecure!) scheme: Generate the keystream using the (fixed) key, then add (mod 256) the nonce to each byte of the keystream. You

happen to know that when Alex sent the plaintext BARACKOBAMA with a nonce of 1, the ciphertext was:

01000011 00011011 00010010 00110000 11111000 10100111

10001110 11101001 00010100 00011101 01100100

You now observe Blake send the following ciphertext with a nonce of 2:

01000110 00010100 00001111 00110011 11110000 10101001

10010110 11111110 00000011 00011100 01110110

a) What is the plaintext of Blake's message?

b) Explain how you found the plaintext. Your answer must be a narrative description, not code or pseudocode.

4. **(3 points)** A linear feedback shift register (LFSR) is used to generate a keystream for a stream cipher. The LFSR has five bits $(s_4, s_3, s_2, s_1, s_0)$, the feedback bit is given by the formula $s_4 = (s_3 + s_2 + s_0) mod\ 2$, and the sequence of s_0 values forms the keystream. The LFSR is initialized with the value $(s_4, s_3, s_2, s_1, s_0) = (1, 1, 0, 1, 1)$.

a) What is the polynomial describing the LFSR above?

b) How many keystream bits will be generated before the keystream starts repeating?

c) What is the sequence of keystream bits?