CS 380/525 Intro to Cryptography
Fall 2022
Assignment 1, due 9/12, before class
Total points: 100

August 29, 2022

1. (10 points) Show that the Caesar (shift by 3) cipher and Vigenère cipher defined over the 128-character ASCII character set, are easy to break by doing a chosen-plaintext attack. How much plaintext is needed to recover the key for each of the ciphers?

2. (10 points) Consider the case where the Caesar (shift by 3) cipher and Vigenère cipher are defined over the 26-character English alphabet. How much plaintext is needed to recover the key for each of the ciphers?

3. (20 points) Consider the MAC presented in the slides. What happens when Charlie tries to modify the Tag, as well as the ciphertext in transit? Explain why this attack will fail, i.e, Bob will always be able to detect a modified Tag/ciphertext.

4. Consider the CBC mode of encryption:

   (a) (20 points) Assume Alice is encrypting all the blocks, and Bob is decrypting them. Draw the corresponding diagram for Bob's decryption.

   (b) (20 points) Assume Alice has encrypted 5 message blocks, M_1, M_2, M_3, M_4, M_5, and the corresponding ciphertext blocks are C_1, C_2, C_3, C_4, C_5. Now assume Charlie tampers with block C_1 in transit, and changes it to C_1'.

   How will this affect Bob's decryption? Will he be able to able to decrypt all blocks correctly? Or none? Or some?

   (c) (20 points) What happens if the Initialization Vector (IV), i.e, the initial randomness fed in to the first block arrives mangled at Bob's end? How will this affect Bob's decryption? Will he be able to able to decrypt all blocks correctly? Or none? Or some?

How to submit: Please upload your **pdf** file on Canvas. You can use my posted template for typesetting your assignment, but aren't required to do so. If you haven't tried LaTeX before (or are rusty, and would like practice), this is an opportunity to do so.

Please use the citation style provided in my templates for citing references (outside of the slides/book) used in your assignment.