CSE 565 Fall 2018
Homework 2
Due on September 25, 2018, in class at 9:30am

1. To facilitate learning about how encryption modes work, this question asks you to derive formulas for encryption and decryption in the CFB and OFB modes. In particular, the lecture presented formulas for computing cipherblocks from plaintext and plaintext from cipherblocks for almost all modes of operation including CFB. For this question, derive similar encryption and decryption formulas for the CFB mode used as a stream cipher with r-bit messages ($r < n$). You can use notation $S_r(a)$ employed in the textbook to denote the first (most significant) r bits of a. Also use notation $||$ to denote concatenation (i.e., $a||b$ means b appended to the end of a).

   Repeat the exercise for the OFB mode used as a stream cipher with r-bit messages.

2. Suppose researcher Alice discovers a ground-breaking algorithm for which she thinks the public is not ready. Instead of announcing it, Alice describes the algorithm in a document and publishes a cryptographic hash of it in the current issue of a newspaper. When 15 years later the research community gets close to rediscovering the algorithm, Alice announces the result.

   (a) Can the digest published in the newspaper be used as a proof (i.e., convince a judge) that the algorithm was discovered 15 years ago? Justify your answer.

   (b) Would your answer change if a cryptographic signature of the document was published instead of the hash? Justify.

3. Suppose Alice and Bob store their respective RSA encryption public keys in a file on a server. They communicate regularly using confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice's an Bob's public keys.

   (a) How should Eve alter that file so that she can read confidential messages sent between Alice and Bob and forge messages from either? After altering the file, how would she need to modify the communication to achieve the above?

   (b) How might Alice and/or Bob detect Eve's subversion of the public keys?

4. Read the paper "Why Cryptosystems Fail" (available from `http://www.buffalo.edu/~mblanton/cse565/wcf.pdf`) and answer the following questions about it:

   (a) What does the article tell you about security of computer systems and how the field of security evolves?

   (b) What does it tell you about building and operating secure systems?

   (c) What is the main proposal of the paper?

   (d) How do you think the situation with the banking industry today compares with what is described in the article? What are some of the protection mechanisms that you encountered in your banking experience?

   (e) How do you think computer security in other industries compares to the security in the banking sector?