CSE 565 Fall 2018
Homework 1
Due on September 13, 2018, in class at 9:30am

1. Problem 1.3 from the textbook.

2. Problem 1.5 from the textbook.

3. Consider the block encryption algorithm TEA described in problem 2.4 in the textbook. In the description, $\oplus$ denotes bitwise exclusive OR (XOR), $\boxplus$ denotes addition modulo 2^{32}, $x \lll y$ denotes circular left shift of value x by y bits, and $x \ggg y$ denotes circular right shift of x by y bits.

   (a) Suppose we are given this algorithm that consists only of two rounds and produces ciphertext $C = (L_2, R_2)$. Express the ciphertext as a function of the input, i.e., the message and key blocks as well as the constants δ_i.

   (b) Assume that the constants δ_i are publicly known. You don't have the knowledge of the key, but can mount the chosen plaintext attack (i.e., request ciphertexts on messages of your choice). Given this ability, what information can you learn about the key using the 2-round version of TEA? Justify your answer.

   (c) Would the answer described above change if the 4-round version of TEA is used instead? Justify your answer.

4. Read about AES-NI and research its use in programs.

   (a) Determine a way to use hardware accelerated AES in one programming language. Provide a segment of code to encrypt one block (16 bytes) of plaintext using AES hardware instructions such as aesenc, aesenclast, etc. Assume that the plaintext is initially stored in a binary buffer (array) and a 128-bit key is also stored in a binary buffer. Executing your code segment should result in a 16-byte cipher block.

   (b) Is hardware accelerated AES available in all programming languages? Explain.

   (c) List resources that were useful in working on this problem.

5. (a) Find an alternative implementation of AES in the form of a cryptographic library, preferably one that doesn't use AES-NI. Write a very small program using that library for accomplishing the task of the previous problem using that library, i.e., for encrypting a 1-block message with a 128-bit key in the ECB mode. Submit the name of the library, the programming language that you used (it can be different from the language in problem 4), and the code.

   (b) Compare the speed of the two implementations. For improved accuracy, run each program to encrypt 1000 1-block messages and report the total time for each of the two programs. If key expansion uses separate code, execute key expansion once followed by 1000 1-block encryptions. Report the times for both implementations and comment on the differences or similarities and any performance conclusions that you can provide.