Homework 3

CSC 152 – Cryptography

If anything in this assignment does not make sense, please ask for help.

Quiz: We will have a closed-note 20-30 minute quiz on this homework in class Fri Mar 8.

Due: You should consider the due date to be when you take the quiz because the quiz may cover anything related to this homework, including programming topics. However, anything submitted before grading occurs will be considered on-time.

Non-submitted work:

Read: The One-Time Pad section from Chapter 1 and the Modes of Operation section from Chapter 4 of *Serious Cryptography*. A few notes are on Piazza regarding distinguishing games.

Written Problems:

There are three steps to follow for the written problems. Step 1: Do them as if they were homework assigned to be graded (ie, take them seriously and try to do a good job). Step 2: Self-assess your work by comparing your solutions to the solutions provided by me. Step 3: Revise your original attempts as little as possible to make them correct. Submit both your original attempt and your revision as separate files.

Submit two files to DBInbox following the procedure documented on Piazza. The first file should be named exactly **hw3.pdf** and should be your homework solutions before looking at my solutions. The second file should be named exactly **hw3revised.pdf** and should be your homework solutions after looking at my solutions and revising your answers.

NOTE: If you wish to handwrite your solutions you may, but only if your handwriting is easy to read and the file you submit is less than 1MB in size.

1) The AES S-box is a permutation, and therefore could be used in the modes of operation we learned (ECB, CBC, CTR). Use the S-box in each of the modes to encrypt "abc". In modes that need padding use 10^* padding. For modes that need an IV use 01010011. For modes that need a nonce, use 0110. Note that the S-box would never be used this way, I'm just using it as a readily available permutation for practice.

2) Let's say that a ciphertext that was created using a mode-of-operation has a single bit toggled in it's i-th block before decryption. How damaging is it to the decryption? Describe the damage with respect to errors in the resulting plaintext blocks (eg, "plaintext block i has a single bit error", or "all plaintext blocks later than i look random", etc). Do this for each of the modes ECB, CBC, CTR.

3) You are given a black box f that has either a standard 52-card deck-of-cards or a 48-card deck-of-cards for the game pinochle. You are allowed to activate f once, upon which a card is chosen at random and you are given the card. In pseudocode, give an algorithm that uses f once and then guesses either "standard" or "pinochle". Evaluate the advantage your algorithm achieves.

In this problem you can maximize your advantage by identifying all of the cards that are more likely with one type of deck and guess that type of deck if any of those cards appear.

4) You are given a black box f that has either a 30-sided die or a 34-sided die inside. Each time you activate f the die is rolled and you are told the resulting value. You are allowed q activations. In pseudocode, give an algorithm that uses f q times and then guesses either "30-sides" or "34-sides". Evaluate the advantage your algorithm achieves as a function of q.

Programming:

Read: C program requirements at `http://krovetz.net/152/programs.html` and an introduction to SSE at `http://krovetz.net/152/sse.html`

A) Redo Problem A from Homework 2 using SSE instructions to accelerate P152 as much as possible. Submit your function via DBInbox in a file named exactly `hw3_P152.c`. Your C file will need to #include <emmintrin.h> to access the SSE intrinsics. Some guidance will be posted soon in the Piazza Q&A.