CS 4920/5920 Spring 2022

HW 3

HW 3 is due on 3/16. Explain how you reached your answers. Answers without explanations will receive no to little credit.

Submit a zip file for this HW since it includes programming in Problems 1 and 5. Your zip file should include the followings for the programming problems: code, compiler outputs or executables if applicable, and the programming output (what is being asked by the question).

Problem 1. DES Implementation

Implement Data Encryption Standard (DES). You will vary the number of rounds within DES and retrieve the ciphertext after applying IP^{-1} after the specified number of rounds.

a. Describe your program/implementation including: the description of your approach, the description and references to any online resources you used, the definitions of the functions and variables.
b. Take the three class-common input files and generate the ciphertexts. After the final round (which number is specified in the input file), apply IP^{-1}. Your output should be three output files following the file naming scheme below. For example, the ciphertext file using "class_input_1.txt" should be named "[last_name]_output_1" and have the matching index number (1 in this case).
c. Generate your own input file and the corresponding output file for ciphertext.
d. Generate 1,000 input files with 16 rounds and a fixed key while varying the message. The 16 number of rounds and the key should be fixed for the 1,000 input files you generate. Run your DES implementation 1,000 times using these input files. Measure the time it took to run the DES 1,000 times and estimate the average time it takes to run DES. Please submit your time measurements; there is no need to submit the 1,000 input files and the 1,000 output files for this part.
e. Using your measurements, estimate the time it takes to brute-force DES to find the key. Explain how you computed and dervied this estimation.

Input format: The first line consists of the number of rounds to compute. The second line is the 64-bit key in hexadecimals. The third line is the 64-bit message in hexadecimals.

Output format: The output file has only one line including the ciphertext without the key.

File Naming: Have the files in .txt and name your files in the format:

"[last_name]_output_[file_index]"

For example, if your name is John Doe, then the output file using "class_input_2.txt" is "Doe_output_2".

Problem 2.

This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key K and the plaintext, namely:

Hexadecimal notation: 8 9 A B C D E F 0 1 2 3 4 5 6 7

Binary notation: 1000 1001 1010 1011 1100 1101 1110 1111

0000 0001 0010 0011 0100 0101 0110 0111

a. Derive K_1, the first-round subkey.
b. Derive L_0, R_0.
c. Expand R_0 to get E[R_0], where E[·] is the expansion function, e.g., as given from: https://en.wikipedia.org/wiki/DES_supplementary_material
d. Calculate $A =$ E[R_0] $\oplus$ K_1.
e. Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.
f. Concatenate the results of (e) to get a 32-bit result, B.
g. Apply the permutation to get P(B).
h. Calculate R_1 = P(B) $\oplus$ L_0 .
i. Write down the ciphertext.

Problem 3.

a. Develop a set of tables similar to Table 5.1 in the textbook for GF(5).
b. Determine if the follow are reducible over GF(2), i.e., coefficients mod 2.
   i) $x^3 + 1$
   ii) $x^3 + x^2 + 1$
   iii) $x^4 + 1$

Problem 4.

a. Develop a set of tables similar to Table 5.3 for GF(4) with $m(x) = x^2 + x + 1$.
b. Develop a table similar to Table 5.5 in the textbook for GF(2^4) with $m(x) = x^4 + x + 1$.

Problem 5. Finite-Field Calculator Programming

Implement a simple four-function calculator in GF(2^8) using the irreducible polynomial used in AES, i.e., m(x)=x^8+x^4+x^3+x+1. The four functions are addition, subtraction, multiplication, and division (multiplication by the multiplicative inverse). Your code should take two elements/numbers and the choice of the function as inputs and output the calculation result. The computations, including the multiplicative inverses, should be done on the fly without using a pre-computed table.

a. Describe your program/implementation including: the description of your approach, the descriptions and references to any online resources you used, the definitions of the functions and variables.
b. Explain and show (with evidence) how you tested the different calculations of the calculator program.