CS 4920/5920 Applied Cryptography Spring 2018

Assignment 3

This assignment is due at the beginning of class on February 28. Please explain how you reached your answers.

Problem 1.

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

Binary notation: 0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 1100 1101 1110 1111

a. Derive K_1, the first-round subkey.
b. Derive L_0, R_0.
c. Expand R_0 to get $E[R_0]$, where $E[\cdot]$ 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 2.

Using the extended Euclidean algorithm, find the multiplicative inverse of

a. 1234 mod 4321
b. 24140 mod 40902
c. 550 mod 1769

Note: Please explain the reason if the multiplicative inverse does not exist. Alternatively, provide a table similar to *Table 2.4* in the textbook; feel free to write a computer program to fill in the entries for the table.

Problem 3.

a. Develop a set of tables similar to *Table 5.1* in the textbook for GF(5).
b. Develop a table similar to *Table 5.5* in the textbook for GF(2^4) with $m(x) = x^4 + x + 1$.

Problem 4.

Show the following:

a. Show that the matrix given here, with entries in GF(2^4), is the inverse of the matrix used in the MixColumns step of S-AES.

$$\begin{pmatrix} x^3+1 & x \\ x & x^3+1 \end{pmatrix}$$

b. Verify *Equation (6.13)* in Appendix 6A in the textbook. That is, show that $x^i \bmod (x^4+1) = x^{i \bmod 4}$.

Problem 5.

Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101}:

a. Show the original contents of **State**, displayed as a 4 × 4 matrix.
b. Show the value of **State** after initial AddRoundKey.
c. Show the value of **State** after SubBytes.
d. Show the value of **State** after ShiftRows.
e. Show the value of **State** after MixColumns.