CS 655 Fall, 2017, Homework 1

Due: Tuesday, September 19, 2017

In this homework, the subscript x indicates hexadecimal notation.

1. The first S-box for DES is defined in the Federal Register by the 4×16 table shown in `http://www.cs.purdue.edu/homes/ssw/cs655/S1.txt` . Use this table to construct the difference distribution table for the first S-box. Print the last ten rows of it. Use the (full) table for the next two questions.

(Hint: The answer is a 64×16 table. The fourth row, the one for input XOR 3_x, begins 14, 4, 2, 2, 10, 6, 4, 2. The fifteenth row, the one for input XOR E_x, begins 0, 4, 8, 8, 6, 6, 4, 0.)

2. Parts a, b, c, are independent. Part d combines them. Notation: $S1_E$ and $S1_E^\star$ refer to the six bits in the output of the E-expansion that affect the first S-box. $S1'_O$ is the four-bit output XOR of the first S-box. $S1_K$ means the six bits of the round subkey that affect the first S-box.
a. Suppose $S1_E = 20_x$, $S1_E^\star = 24_x$, and $S1'_O = D_x$. What can you say about $S1_K$?
b. Suppose $S1_E = 13_x$, $S1_E^\star = 18_x$, and $S1'_O = D_x$. What can you say about $S1_K$?
c. Suppose $S1_E = 3F_x$, $S1_E^\star = 3E_x$, and $S1'_O = 6_x$. What can you say about $S1_K$?
d. Could a single key $S1_K$ have been used in all three of a, b, c? If so, what can you say about it?

3. What is the probability that $2B_x$ may cause 0_x by the first S-box? What is the probability that $3B_x$ may cause A_x by the first S-box? What is the probability of the 1-round DES characteristic with $\Omega_P = 00000202\ 40000000_x$ and $\Omega_T = 00000000\ 40000000_x$?