Introduction to Cryptography, Spring 2024

Homework 2: On-site Test

Time: 5:30-9:00pm, 3/22/2024 (Friday)

Problem:

A. **MDES: implement the following modifications on DES:**

  a. Swap s-boxes S1 and S8.

  b. Replace S2 with the following function:
  $S2(\mathrm{b}_1 b_2 b_3 b_4 b_5 b_6)$
  $= (2 * b_1 + 3 * b_2 + 5 * b_3 + 7 * b_4 + 11 * b_5 + 13 * b_6) \text{ mod } 16$
  where $\mathrm{b}_1 b_2 b_3 b_4 b_5 b_6$ are 6 input bits to S-Box.

  c. The round keys in the key scheduling are left-rotated by the following table:

Round	1	2	3	4	5	6	7	8
# of rotated bits	2	2	2	1	2	2	2	1
Round	9	10	11	12	13	14	15	16
# of rotated bits	2	2	2	1	2	2	2	1

B. **Submission:**

  a. Input: two data lines of plaintext and key in ASCII, such as, “security 11131719”

  b. Output: two ciphertext lines in Hex, such as, “1B5123E67255C6D9”