Iran University of Science and Technology

School of Computer Engineering

The Simulation Project

Digital Logic (Fall 2020)

Deadline: before 22th of Bahman 1399

Design and implement a digital circuit to provide a simple symmetric cryptography mechanism. The Simple Data Encryption System (SDES) is the algorithm that you should implement digitally. The description of the SDES is provided in the attached file. Your design includes two parts:

Part 1 is the structure of SDES (the right dataflow diagram). A plaintext of 8 bits is entered to the circuit and finally an 8 bits cipher-text is generated. In fact, the plaintext is encrypted to the cipher-text. The decryption procedure is the inverse of encryption. It means that the circuit should work from bottom to top.

Part 2 is the key generation, which you see in the left side of page. A master key of 10 bits is entered to the circuit and the circuit generates two keys (K1 and K2), each one has 8 bits.

Let us introduce the components of the SDES circuit:

IP (initial permutation box) is a shuffle register. In the shuffle register, the position of bits is changed as a specific pattern. You can see this pattern in the attached file (the second page).

EP (Expanded permutation box) is a simple hardware component that expands 4 bits into 8 bits as a specific pattern shown in the attached file.

S0 and S1 are substitution boxes. They are simple hardware components that replace four input bits with two output bits as a specific pattern as shown in the attached file.

P4 (permutation box) is another shuffle register. Its operation has been discussed in the attached file.

IP^{-1} (the invers initial permutation box) is the inverse of shuffle initial permutation box and its operation has been discussed in the attached file.

$\oplus$ is a simple XOR gate that either xor 4 bits together or 8 bits based on position in the architecture.

Let us, discuss the components of the key generation part:

P10 is a permutation box. It is a shuffle register and its operation has been shown in the attached file.

P8 is similar to P10 and it's operation has been discussed in the attached file.

LS-1 = Rotate Left – 1 bit

LS-2 = Rotate Left – 2 bits

Please take care of LSB and MSB bits as shown in the attached file. Please consider the examples of shown in the attached file.

Input of your circuit: (1) a plaintext of 8 bits (an 8-bit register) (2) a master key of 10 bits (a 10-bit register)

Output of the circuit: a cipher-text of b bits (an 8-bit register)

For any question regarding the circuit and its operation, contact TAs or me via email or left your comment in the telegram group.

Good Luck!

Dr. Hakem Beitollahi,