

CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2005
George Washington University

Homework IV

due 2 November, 6 pm.

70 marks

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the test and final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

Any violations will be treated as violations of the Code of Academic Integrity.

PLEASE submit this HW on Blackboard only. One compressed file should contain all your code. Name your files:

CS283_HW1_LASTNAME_FIRSTNAME.zip or .rar

CS172_HW1_LASTNAME_FIRSTNAME.zip or .rar

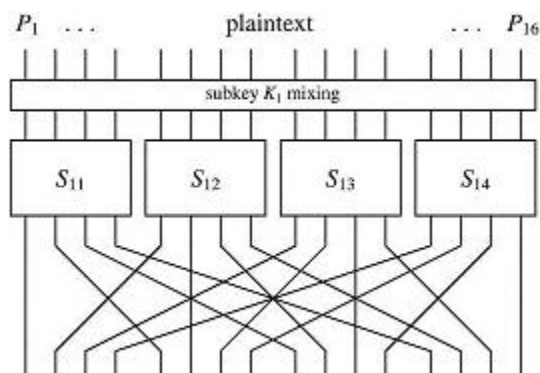


Figure 1: One layer of an SPN. From H. M. Heys, “A Tutorial on Linear and Differential Cryptanalysis”.

1. (35 marks) Implement an SPN layer with a single row of 4 S-boxes. Each S-box takes as input 4 bits.

Your program takes as input:

- an input x of length 2 bytes
- a key K of length 2 bytes
- the S-box function f as a byte-array of length 16; the first four bits of each byte are 0, the last four bits of, say, byte 7, is the S-box output when the input is 0111 (the binary representation of 7).
- the permutation function σ as a byte-array of length 16; the first four bits of each byte are 0, the last four bits of, say, byte 9, are the binary representation of the position bit 9 goes to on permutation.
- an integer a of value 0 indicating encryption, and value 1 indicating decryption.

Your program should produce the following output:

- an output y of length 2 bytes
- the same input key K of length 2 bytes
- the same S-box function f as a byte-array of length 16;
- the same permutation function σ as a byte-array of length 16;
- an integer a of value 0 indicating decryption was performed, and value 1 indicating encryption was performed.

Note that your program’s output is different from your program’s input in exactly two places: the output string y is either an encrypted or decrypted version of x , and the bit a indicating encryption/decryption is flipped.

The TA will test the correctness of your program by giving it any input file (see a sample online) and then running it again with your output file as input. The second output file should be identical to the first input file. You may use Java, C, C++ or Python for this assignment. Submit electronic copies of all code, and a sample input and output to demonstrate that your program works. As with all programming assignments for this class, your code should run on a seas account.

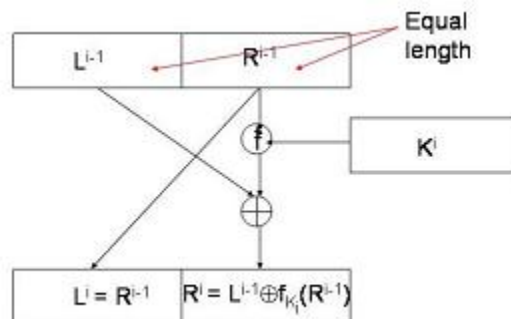


Figure 2: The Feistel Cipher

2. (35 marks) Implement a Feistel Cipher with a 16-bit message and an 8-bit key.

The f function of the cipher is as follows:

$$f_K(R) = \text{FirstFourBits}(R \oplus K) \circ \text{LUT}(\text{LastFourBits}(R \oplus K))$$

where \circ denotes concatenation, and LUT is a look-up table that takes only the last 4 bits of the $R \oplus K$ as input.

Your program takes as input:

- an input x of length 2 bytes
- a key K of length 1 byte
- the LUT as a byte-array of length 16; the first four bits of each byte are 0, the last four bits of, say, byte 7, is the LUT output when the last four bits of $R \oplus K$ are 0111 (the binary representation of 7).
- an integer a of value 0 indicating encryption, and value 1 indicating decryption.

Your program should produce the following output:

- an output y of length 2 bytes
- the same input key K of length 1 byte
- the same LUT as a byte-array of length 16;
- an integer a of value 0 indicating decryption was performed, and value 1 indicating encryption was performed.

Note that your program's output is different from your program's input in exactly two places: the output string y is either an encrypted or decrypted version of x , and the bit a indicating encryption/decryption is flipped.

As in 1, the TA will test the correctness of your program by giving it any input file (see a sample online) and then running it again with your output file as input. The second output file should be identical to the first input file. You may use Java, C, C++ or Python for this assignment. Submit electronic copies of all code, and a sample input and output to demonstrate that your program works. As with all programming assignments for this class, your code should run on a seas account.