CS-364: Introduction to Cryptography and Network Security LAB
LAB Assignment II

Course Instructor: Dr. Dibyendu Roy Due: Feb 10, 2023, 11:59 pm

Instructions: Code must be written in C and well commented. Submission of code in any other file extension (.pdf, .docx etc) will not be considered. Write your name and roll number on the top of your code. The file name of the code will be YOUR ROLL NO.c

Implement the encryption as well as the decryption of the following SPN based cipher. The design of the SPN encyrption is given in the Figure 1.

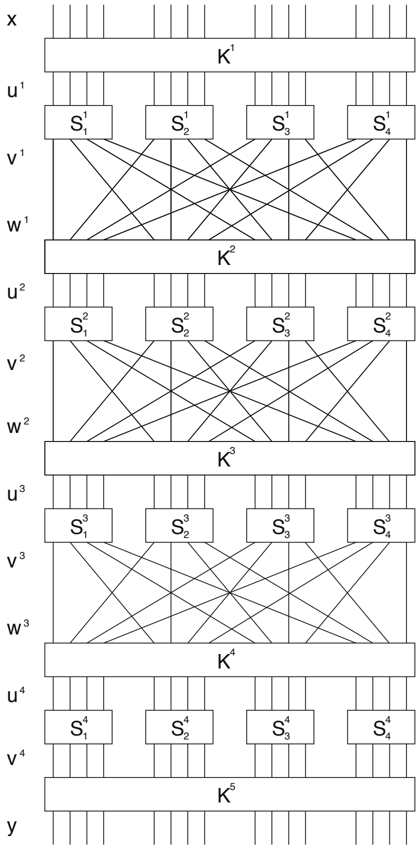

Figure 1: SPN Encryption

Here all the S-boxes are same (S) and it is defined below.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

The permutation (P) is also same for all the rounds and it is defined below.

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

We will consider x as the plaintext (input hexadecimal) and y will be the ciphertext (output). Here the secret key (input) is of 32-bit (hexadecimal) i.e., $K = (k_1, \ldots, k_{32}) \in \{0,1\}^{32}$. For $1 \leq r \leq 5$ the round key K^r consists of 16 consecutive bits of K, beginning with k_{4r-3}. These round keys are xor'ed with the 16 bit state in every round. After finishing the encryption perform the decryption and print the decrypted text in hexadecimal.