Assignment – 4 Date: September 12, 2018

Submission Deadline: September 19, 2018

All assignments will be marked out of 20. No assignment will be marked after the deadline.

Implement an Iterated Substitution Permutation Network (SPN) consisting of Nr = 4 rounds, with the following specifications:

1. Each round consists of round-key mixing followed by a substitution and a permutation.
2. Assume the plain text and cipher text blocks, each to be 8-bits long.
3. The round key mixing is done by a bitwise XOR operation.
4. Key whitening is to be performed not only at the beginning, but also at the end of the SPN.
5. The key schedule is generated by selecting $(4r\text{-}3)^{th}$ through $(4r+4)^{th}$ key bits as the round key for round r. (The minimum length of the key is given by 1×8+Nr×4=24 bits. Select a random string of 24 bits as the key.)
6. The substitution function at each round is specified by the following S-box, where all notations are hexadecimal:

i/p	0	1	2	3	4	5	6	7
o/p	E	4	D	1	2	F	B	8

…

i/p	8	9	A	B	C	D	E	F
o/p	3	A	6	C	5	9	0	7

7. The permutation function for each round is:

Input	1	2	3	4	5	6	7	8
Output	1	4	5	7	3	6	2	8

(Drop the permutation function at the last round. Think why.)

Implement both the encryption and decryption functions for the above cipher.

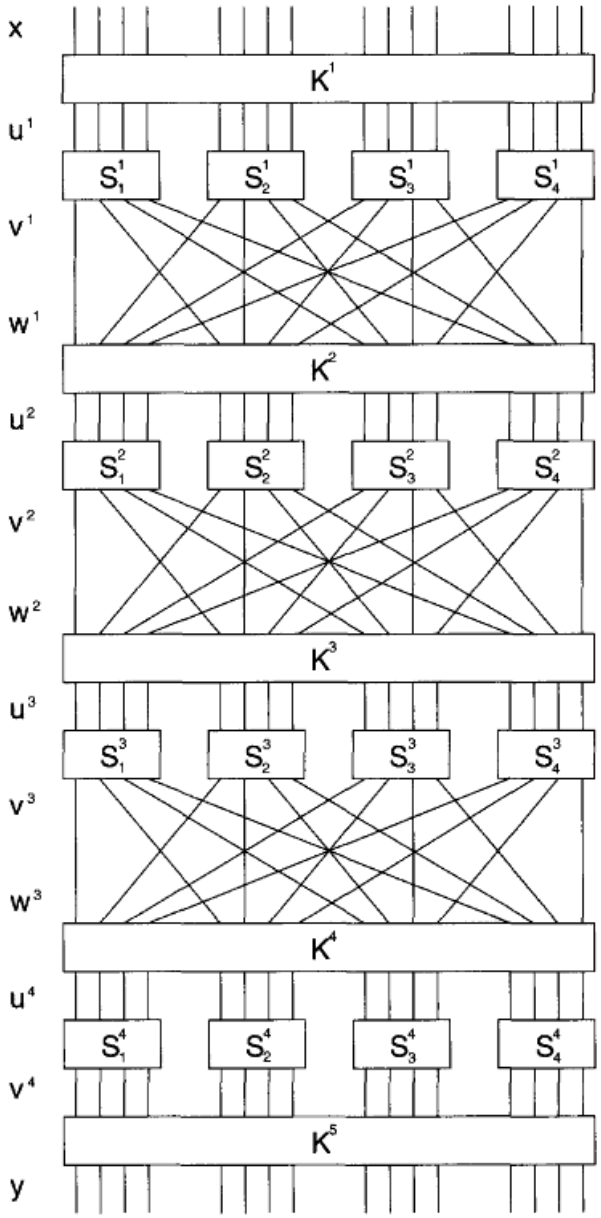

Fig.: Example of a typical SPN