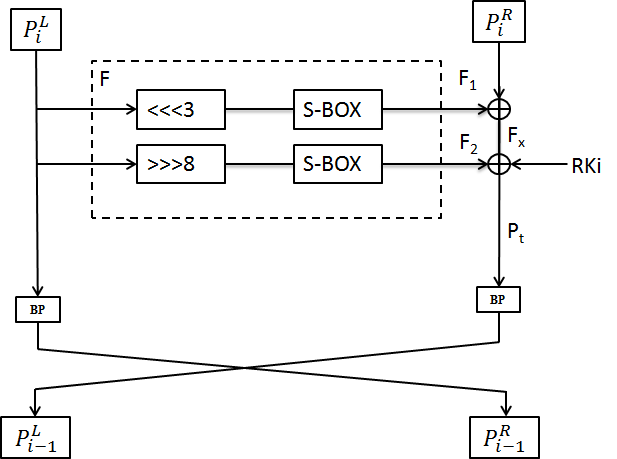
Assignment:

ANU Design : Write a C program as well as Keil program for the following design. Use the data given below.

ANU has 25 rounds cipher :-

32 – Bit MSB 32 – Bit LSB



Notations:-

* PT 64-bit input plaintext block
* CT 64-bit output cipher text block
* RKi 128-bit Round sub key for round i
* F 1 & F2 Function
* ⊕ Bitwise exclusive-OR operation
* <<<n Left cyclic shift by n bits
* >>>n Right cyclic shift by n bits
* RCiRound counter i
* **||** Concatenation of two strings
* ! Bitwise NOT operation
* BP Bit Permutation
* LCS Left circular shift
* RCS Right circular shift

S – Box :

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

P – Layer:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 |
| **BP[** | 20 | 16 | 28 | 24 | 17 | 21 | 25 | 29 |
|  | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 |
| **BP[** | 22 | 18 | 30 | 26 | 19 | 23 | 27 | 31 |
|  | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| **BP[** | 11 | 15 | 03 | 07 | 14 | 10 | 06 | 02 |
|  | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| **BP[** | 09 | 13 | 01 | 05 | 12 | 08 | 04 | 00 |

Key scheduling:

1. KEY <<< 13.

2. [K3 K2 K1 K0] ←S [K3 K2 K1 K0]

3. [K7 K6 K5 K4] ←S [K7 K6 K5 K4]

4. [K63 K62 K61 K60 K59] ← [K63 K62 K61 K60 K59] ⊕ RCi