Name : Tadepalli Shanmukha Datta Sai Sasank
NetID : na2500

a) Entry into S-boxes : 2A0B3A140815
- In Binary : 0010 1010 0000 1011 0011 1010 0001 0100 1101 1000 0001 0101
- Dividing it into 8 blocks of 6-bit:

001010 100000 101100 111010 000101 001101 100000 010101

- Now each 6-bit block is given to the corresponding S-Box to convert it into 4-bit block.
Each S-Box has 4 rows & 16 columns. Value at row i, col j gives 4-bit block.
To get row i, col j for a 6-bit block 'abcdef',
row i = decimal value(af), col j = decimal value(bcde)

1) 001010 → row = 00 = 0, col = 0101 = 5 → S1[0][5] = 15 → 1111
2) 100000 → row = 10 = 2, col = 0000 = 0 → S2[2][0] = 0 → 0000
3) 101100 → row = 10 = 2, col = 0110 = 6 → S3[2][6] = 3 → 0011
4) 111010 → row = 10 = 2, col = 1101 = 13 → S4[2][13] = 2 → 0010
5) 000101 → row = 01 = 1, col = 0010 = 2 → S5[1][2] = 2 → 0010
6) 001101 → row = 01 = 1, col = 0110 = 6 → S6[1][6] = 9 → 1001
7) 100000 → row = 10 = 2, col = 0000 = 0 → S7[2][0] = 1 → 0001
8) 010101 → row = 01 = 1, col = 1010 = 10 → S8[1][10] = 6 → 0110

- 32-bit Output after S-Box stage:
  1111 0000 0011 0010 0010 1001 0001 0111
- Output in HEX Format
  F0322916
- Final Answer : **F0322916**

b) Given, K = 3E2F0136224781

K = 0011 1110 0010 1111 0000 0001 0011 0110 0010 0010 0100 0111 1000 0001

First Half : 0011 1110 0010 1111 0000 0001 0011
Second Half : 0110 0010 0010 0100 0111 1000 0001

1) Doing 1 left Circular shift for K1
   F: 01111100010111100000000100110
   S: 11000100010010001111000000010
2) Doing 1 left circular shift for K2
   F: 11111000101111000000010011100
   S: 10001000100100011110000000101
3) Doing 2 left Circular shift for K3
   F: 11100010111100000001001110011
   S: 00100010010001111000000010110
4) Doing 2 left Circular shift for K4
   F: 10001011110000000100110011111
   S: 10001001000111100000010110000
5) Doing 2 left Circular shift for K5
   F: 00101111000000010011001111110
   S: 00100100011110000000101100010
6) Doing 2 left Circular shift for K6
   F: 10111100000001001100111110000
   S: 10010001111000000101100010000

After shifts, Key is

10111100000001001100111111000100100001111000000010110001000

Using Permutated Choice 2 table on the above key to get K6

K6 = 110111 100110 100100 000000 000100
000001 011001 100111

K6 in HEX Form:

DE6900101667

Final Answer: **DE6900101667**