Project1: Breaking a Simple Cipher

In this project, you will break a simple cipher, referred to as SC-1, by obtaining the key.

SC-1 is a 64-bit block cipher, using 64-bit keys. Capital letters (like A, B, C) will be used to denote 64-bit values. Suppose A is a 64-bit data item. The 64 bits in A will be referred to as (a63, a62, a61, …, a1, a0), and a0 is the least significant bit (the rightmost bit). The 64-bit value can also be considered as 8 bytes, which are denoted as A0, A1, A2, A3, …, A6, A7. A0 is the rightmost byte. So the eight bits in A7 are (a63, a62, a61, .., a57, a56); the eight bits in A6 are (a55, a54, a53, .., a49, a48), and so on.

Let K be the key of 8 bytes and P the plaintext block. Note that there are 8 bytes in P and P7 is the first byte in the plaintext stream. SC-1 works as follows.

1. Compute D = P ⊕ K, where ⊕ is bit-wise exclusive or (XOR).

   `di = pi ⊕ ki , where i = 0 .. 63.`

2. Compute E = D « 17, where « is rotate left operation.
3. Perform S-Box on each byte of E to produce the ciphertext C.

   `C0 = SBox[E0], C1 = SBox[E1], …, C7 = SBox[E7].`

The S-Box used in Step 3 is the same as the S-Box in AES. It maps a byte to another byte.

As in the current format, SC-1 is not secure. Suppose you know the following pair of plaintext and ciphertext, find out the key used in the encryption.

```
Plaintext : F5EF5D981B5DB510
Ciphertext: 2AAA8E541A37D5AF
```

An implementation of the cipher in PHP is provided. You can check the source code and know the details of the cipher. You can also verify the key you have obtained.

Submit a report in PDF format in which you describe how you obtain the key. Make sure write down your name on your report.

Extra questions

Do not include the extra questions in your report.
Can you still break SC-1 if it is revised in the following ways?

1. The rotation amount (17) in Step 2 depends on the key.
2. The rotation is Step 2 is replaced by a 64-bit permutation that depends on the key.
3. Steps 1 to 3 are repeated one more time (with P = C for the second round).