Programming Assignment – Toward DES

Background

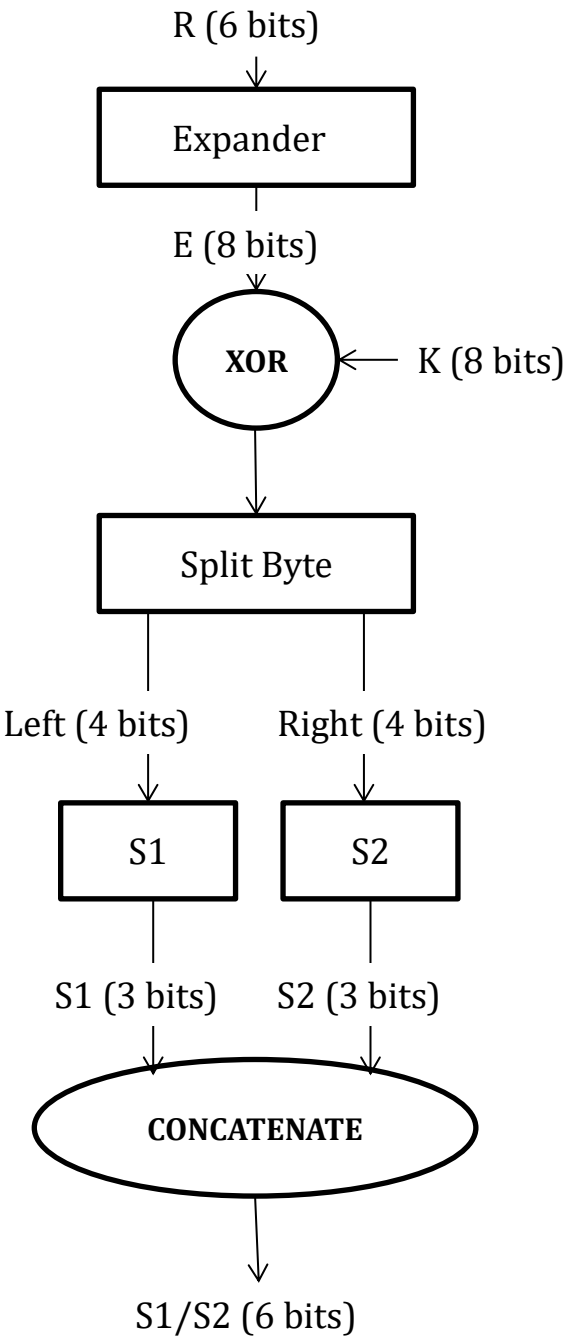
The cryptography systems use various forms of substitution, transposition, and key-based arithmetic/logical operations to perform encryption and decryption. Many of those operations are rooted in the Feistel system, named after Horst Feistel, who was part of the IBM team that developed LUCIFER, the basis for the DES cryptography system. In this assignment you will implement a Feistel System function.

Specification

The Feistel System function you will implement receives two arguments, a 6-bit value and an 8-bit key. It returns a 6-bit value stored in the right-most 6 bits of an 8-bit **`byte`**. Your function should implement these as bytes using the following method definition:

```
public static byte feistel(byte R, byte K)
```

The operations are shown in the following flow chart:


R (6 bits)
Expander
E (8 bits)
XOR
K (8 bits)
Split Byte
Left (4 bits)
Right (4 bits)
S1
S2
S1 (3 bits)
S2 (3 bits)
CONCATENATE
S1/S2 (6 bits)

Use the following main method to demonstrate your code:

```
public static void main(String[] args) {
   byte K = (byte)(0b10101010 & 0xFF);
   System.out.println("\t S Feistel");
   for (int i = 0; i < 2; ++i) {
      for (int j = 0; j < 8; ++j) {
         // -- set up index to S boxes from i and
         byte Sindex = (byte)(((i << 3) | j) & 0x0F);
         // -- combine 3 bits from S1 and S2 into a 6 bits
         byte R = (byte)((S1(Sindex) << 3) |
                         S2((byte)(Sindex)));
         // -- send S values to Feistel function with the key
         byte f = feistel(R, K);
         System.out.println(
                    int2binary((byte)(((i << 3) | j) & 0x0F), 4) +
                    ": " +
                    int2binary(R, 6) + " " +
                    int2binary(f, 6));
      }
   }
}
```

Deliverables

- Source code (.java) files
- Screen shot of your running program using the main function given (above)
- Reflective essay describing
    - Successes
    - Difficulties (if any) and how you addressed them
    - Lessons learned

If you do this assignment as a programming pair include both names and both reflections in a single document. Each person should submit the requested [identical] documents to Canvas under their own name.