Encryption/Decryption

Background

You have created a series of methods culminating in the Feistel algorithm. The next step is to take these methods and build an encryption system similar to (but simpler than) the Data Encryption Standard (DES) algorithm.

Specification

Write a method called

```
static short encode12 (short plain, int round, short key9)
```

to perform the following operations:

1. Extract an 8-bit key from key9 (which is 9 bits) starting at the position specified by round
2. Isolate the left and right 6-bit values from plain (which is 12 bits)
3. Apply the Feistel method to the right 6-bit value and the key
4. Exclusive-or the result of step 3 with the left 6-bit value
5. Concatenate the right 6-bit value (on the left) with the 6-bit value from step 4 (on the right)

Write a method called

```
static short decode12 (short cipher, int round, short key9)
```

exactly the same as the encode12 method with one exception:

1. Extract an 8-bit key from key9 (which is 9 bits) starting at the position specified by round
2. Swap the first 6 bits with the last 6 bits of cipher (which is 12 bits)
   $l_5l_4l_3l_2l_1l_0r_5r_4r_3r_2r_1r_0$ -> $r_5r_4r_3r_2r_1r_0l_5l_4l_3l_2l_1l_0$
3. Isolate the left and right 6-bit values from plain (which is 12 bits)
4. Apply the Feistel method to the right 6-bit value and the key
5. Exclusive-or the result of step 3 with the left 6-bit value
6. Concatenate the right 6-bit value (on the left) with the 6-bit value from step 4 (on the right)
7. Swap the first 6 bits with the last 6 bits of the value obtained in step 6 (which is 12 bits)
   $l_5l_4l_3l_2l_1l_0r_5r_4r_3r_2r_1r_0$ -> $r_5r_4r_3r_2r_1r_0l_5l_4l_3l_2l_1l_0$

Use the following main method to demonstrate your code:

```
public static void main (String[] args) {
   short[] datap = { 0b010000010100, 0b001001000011,
                     0b010001000100, 0b010101000110 };
   short key = (short)(0b011001011);
   for (int i = 0; i < datap.length; ++i) {
      short cipher = encode12 (datap[i], 1, key);
      System.out.print(int2binary(cipher, 12) + " ");
      short plain = decode12(cipher, 1, key);
      System.out.println(int2binary(plain, 12));
   }
   System.out.println();
}
```

The results should be:

```
010100111010 010000010100
000011110010 001001000011
000100001011 010001000100
000110001001 010101000110
```

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.