Homework 3 – Due Tuesday, February 7

1. What would happen if you didn't swap the halves in each round of a Feistel network (Figure 4.3 in the textbook)?

2. Textbook page 120, Problem 4.2

3. Fill in the following table giving the basic parameters of DES:

Algorithm	Block Size(s)	Key Size(s)
DES		

   Imagine that we could make a special-purpose machine that could do a brute-force attack on DES that would take, on average, 2 minutes to find a key in a known plaintext attack. Assuming that it could test keys for any algorithm at the same speed, approximate how long would it take, on average, to break a cipher that uses an 80-bit key? (For your answer, give a precise amount, but then give an "understandable" amount — is it a few seconds? an hour? a day? week? etc.)

   What if we added another byte to the key so that is was 88 bits long?