Feistel System Practice – Scaled down DES

Note: Decryption proceeds exactly as encryption, but with the round keys used in reverse order (and swap at beginning).

1. Let `A = 010101`, `B = 110011`, `C = 111000`. Compute the following
   (a) $A \oplus B$
   (b) $A \oplus C$
   (c) $A \oplus B \oplus A$
   (d) $C \oplus C \oplus C$
2. Let `A = 1100000`, `B = 1100111`, `C = 1111000`. Compute the following
   (a) $A \oplus B$
   (b) $A \oplus C$
   (c) $A \oplus B \oplus A$
   (d) $C \oplus C \oplus C$
3. Let $1_N = 1$ denote the N-bit string of 1's. With $A = 010101$, $B = 110011$, and $N = 6$, compute
   (a) $A \oplus 1$
   (b) $B \oplus 1$
   (c) Explain the general relationship between a bit string S and $S \oplus 1$.
4. Perform the following round key evaluation computations using the key schedule given in class, for $K = 101101110$:
   (a) $f(000000, K_1)$
   (b) $f(101010, K_2)$
   (c) $f(111111, K_3)$
   (d) $f(000111, K_4)$
5. Consider the two-round Feistel cryptosystem similar to the three-round system described in class, but with the third round being removed. Use the same S-boxes from class.
   (a) Using this system with key $K = 011010001$, encrypt the plaintext $p = 101100111101$.
   (b) Using this system with key $K = 101011001$, encrypt the plaintext $p = 101100111010$.
   (c) Perform the corresponding decryption to the ciphertext that you obtained in (a).
   (d) Perform the corresponding decryption to the ciphertext that you obtained in (b).

Please email me answers as you work these, if they differ from what is below; I will update this page as they come in.

Answers (Thanks Erin!)

1. (a) 100110
   (b) 101101
   (c) 110011
   (d) 111000
2. (a) 0000111
   (b) 0011000
   (c) 1100111
   (d) 1111000
3. (a)
4. (a) 010010
   (b) 011101
   (c) 001110
   (d) 100000
5. (a) 0100 1100 1101
   (b) 0100 1110 1100
   (c) 1011 0011 1101
   (d) 1011 0011 1010