Directions: In the following SHOW ALL WORK. Answers alone will receive NO CREDIT.

1. Consider the cipher discussed in class:



|  |  |
| --- | --- |
| **x1x2x3** | **S(x1x2x3)** |
| 000 | 11 |
| 001 | 01 |
| 010 | 00 |
| 011 | 10 |
| 100 | 01 |
| 101 | 00 |
| 110 | 11 |
| 111 | 10 |

Prove the deciphering algorithm works, that is show that



1. Using the S-box from problem one define



then define a 4-bit block cipher as 

1. Encipher x=10110010 and k=10 in ECB mode
2. Encipher x=10110010 and k=10 in CBC mode using IV = 0110
3. Write down the equations for deciphering the cipher described in problem 2 or explain why you cannot.

(more on back)

1. Define a cipher using a **3 round Feistel** construction with F as our round function. The input to the cipher is a block of size 6-bits and the output is also of size 6-bits.

|  |  |
| --- | --- |
| x1x2x3 | F(x1x2x3) |
| 000 | 101 |
| 001 | 010 |
| 010 | 111 |
| 011 | 100 |
| 100 | 111 |
| 101 | 000 |
| 110 | 001 |
| 111 | 011 |

1. Encipher the plaintext 101110110010 using
   1. ECB mode
   2. CBC mode with initial vector 110011
2. Decipher the ciphertext 110101001011 assuming it was enciphered using
   1. ECB mode
   2. CBC mode with initial vector 101010

(NOTE: you can check your answers to 1 & 2 by either decrypting or encrypting your result to see if it matches.)



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F



F