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 deciphering or enciphering your result to see if it matches.)

1. Suppose that you were a cryptanalyst and you knew that a **2 round** Feistel cipher with a 3-bit to 3-bit S-box was used in the encryption process (just like above, but you don’t know the F(x1x2x3) column in the table). You have cleverly intercepted some transmissions and you know that

E(111 000) = 101 001

and

E(000 111) = 110 010

 a) Use this information to fill in as much as the secret table as you can (this is a “known plaintext/ciphertext attack”) :

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

b) Even if an “attacker” can’t fill in the entire table in part a and completely break the cipher, it is considered a successful attack if the person can still use the information to successfully encrypt a “new message” (I.e., find the correct ciphertext for a plaintext other than the ones they know). Use the information you found in part a) to try to find the ciphertext that corresponds to a plaintext other than 000 111 OR 111 000. Find at least 2 sets of plaintext/ciphertext pairs.

c) In an “adaptive chosen plaintext (resp. ciphertext)” attack the attacker is allowed to ask the “oracle” (that’s me) for the ciphertext corresponding to any plaintext (resp. ciphertext). You may query the oracle as many times as you wish.You may ask me “What is the ciphertext that corresponds to xxx xxx (some plaintext of your choosing)?” or “What is the plaintext that corresponds to xxx xxx (some ciphertext of your choosing).

 You may query the oracle as many times as you wish. Do this by emailing me a question (e.g “What is the ciphertext that corresponds to xxx xxx (some plaintext of your choosing)?”) I will reply, then you fill in more of the table and if you haven’t completed it, you can query me again. Choose your plaintexts wisely to minimize the number of queries needed to completely break the cipher. Once you can fill in the entire table of values for F(x1x­2x­­3) you have completely broken the cipher. Challenge: Break the cipher using as few queries as possible.

 *4 queries: Try harder*

*3 queries: Capable Code Cracker*

*2 queries: Super Code Cracker*

*1 query: Master Code Cracker*

*0 queries: Lucky Guesser*

F

F

F

F

F

F

F

F



F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F

F