David Morris
Computer Security
Assignment 1
Due: February 19, 2015

1:

A = 11
B = 6
CryptText: QJKES REOGH GXXRE OXEO
PlainText: IFYOU BOWAT ALLBO WLOW
Decyphered: If You Bow At All Bow Low

2:

A:
L1 = R0
R1 = (L0 ^+ 0)

L2 = (L0 ^+ 0)
R2 = (R0 ^+ 0)

L3 = (R0 ^+ 0)
R3 = ((L0 ^+ 0) ^+ 0)

L4 = ((L0 ^+ 0) ^+ 0)
R4 = ((R0 ^+ 0) ^+ 0)

C = (((L0 ^+ 0) ^+ 0), ((R0 ^+ 0) ^+ 0))

B:
L1 = R0
R1 = (L0 ^+ R0)

L2 = (L0 ^+ R0)
R2 = (R0 ^+ (L0 ^+ R0))

L3 = (R0 ^+ (L0 ^+ R0))
R3 = ((L0 ^+ R0) ^+ (R0 ^+ (L0 ^+ R0)))

L4 = ((L0 ^+ R0) ^+ (R0 ^+ (L0 ^+ R0)))
R4 = ((R0 ^+ (L0 ^+ R0)) ^+ ((L0 ^+ R0) ^+ (R0 ^+ (L0 ^+ R0))))

C = (((L0 ^+ R0) ^+ (R0 ^+ (L0 ^+ R0))),((R0 ^+ (L0 ^+ R0)) ^+ ((L0 ^+ R0) ^+ (R0 ^+ (L0 ^+ R0)))))

C:
L1 = R0
R1 = (L0 ^+ K1)

L2 = (L0 ^+ K1)
R2 = (R0 ^+ K2)

L3 = (R0 ^+ K2)
R3 = ((L0 ^+ K1) ^+ K3)

L4 = ((L0 ^+ K1) ^+ K3)
R4 = ((R0 ^+ K2) ^+ K4)

C = (((L0 ^+ K1) ^+ K3),((R0 ^+ K2) ^+ K4))

D:
L1 = R0
R1 = (L0 ^+ (R0 ^+ K1))

L2 = (L0 ^+ (R0 ^+ K1))
R2 = (R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2))

L3 = (R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2))
R3 = ((L0 ^+ (R0 ^+ K1)) ^+ ((R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2)) ^+ K3))

L4 = ((L0 ^+ (R0 ^+ K1)) ^+ ((R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2)) ^+ K3))
R4 = ((R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2)) ^+ (((L0 ^+ (R0 ^+ K1)) ^+ ((R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2)) ^+ K3)) ^+ K4))

C = (((L0 ^+ (R0 ^+ K1)) ^+ ((R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2)) ^+ K3)),((R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2)) ^+ (((L0 ^+ (R0 ^+ K1)) ^+ ((R0 ^+ ((L0 ^+ (R0 ^+ K1)) ^+ K2)) ^+ K3)) ^+ K4)))

3:

P0 = IV ^+ D(C0,K),
P1 = P0 ^+ D(C1,K),
P2 = P1 ^+ D(C2,K),
...

CBC Mode can encrypt the same plaintext(in different positions) to different ciphertext
Even if the encryption process garbles one block, with the correct keys the cipher will only lose two blocks, and everything after that will still be valid.