Vivek Patel

CSC440

Assignment 4

1. First we split P into the left and right sides, L0 and R0, respectively.

   [L0][R0] –K-> [R0][L0 $\oplus$ f(R0, K)]

   L1 = R0 , and R1 = L0 $\oplus$ f(R0, K)

   We also split P' into left and right sides, L0' and R0'

   [L0'][R0'] –K'-> [R0'][L0' $\oplus$ f(R0', K')]

   R0' = R0 $\oplus$ 111…, L0' = L0 $\oplus$ 111…, and K0' = K0 $\oplus$ 111…,

   L0' $\oplus$ f(R0', K') = L0' $\oplus$ R0 $\oplus$ 111… $\oplus$ K $\oplus$ 111… = L0' $\oplus$ R0 $\oplus$ K = L0' $\oplus$ f(R0, K)

   And

   L0' $\oplus$ f(R0', K') = L0 $\oplus$ 111… $\oplus$ R0 $\oplus$ K = L0 $\oplus$ R0 $\oplus$ K $\oplus$ 111…

   = L0 $\oplus$ f(R0, K) $\oplus$ 111…= R1 $\oplus$ 111… = R1'

   Therefore:

   [L0'][R0'] –K'-> [R0'][L0' $\oplus$ f(R0', K')] = [L1'][R1'] = C'

2. The message m is encrypted to c like this: m -> EK2 -> a -> EK2 -> b -> EK1 -> c

   We can use a brute force attack by encrypting m with all 2^56 possible keys, one of which is K2 and leads to a. We do the inverse for c and decrypt it with all possible keys, resulting in b and K1. We can now use our set of possible a's and K2's to encrypt for b as we know a ->EK2 ->b. We can now use this set of b's and compare them to the ones we found in the earlier decryption step. Any pairs that match will give us a set of pairs of keys K1 and K2. We can test these keys with other m and c pairs to find the true keys K1 and K2.