Charles Lee
23728976
Sec 102
Neil Gong

1. if we construct a table w/ all possible k1 values that correspond to $DES_{k1}^{-1}(c)$, then we can use the result in the next feistral cycle, where it would cancel out with DES_{k1}, leaving just DES_{k2}^{-1}. From there, we can brute force attack by comparing results from the $DES_{k_1}^{-1}$ table and $DES_{k_2}^{-1}$ tables until we find matching pairs (when (k_1^{-1}, c) (k_2^{-1}, c))

2. $C_i = E_k(P_i \text{ xor } C_{i-1})$
   $C_{-1} = IV$

These are the equations for CBC mode. An error in C_i will affect C_i and C_{i+1} as shown

$$C_{i+1} = E_k(P_i \text{ xor } C_i)$$

if C_i is an error C_e

a) 1. $(C_{e+1} = E_k(P_i \text{ xor } C_e))$

2 So C_e and C_{e+1} will be affected by the error. The rest of the cipher blocks will continue as usual

3 $C_{i+1} = E_k(P_{i+1} \text{ xor } C_{e+1})$
$C_{i+2} = E_k(P_{i+2} \text{ xor } C_{i+1})$
and so on

3. Because xor is communative,

$$C = m \text{ xor } k \text{ xor } k^R = m \text{ xor } (2^l - 1)$$

So the attacker can determine the key to be $2^l - 1$ where l is the length of the plaintext. and $m = C \text{ xor } (2^l - 1)$

4. 1) $F(a_L, a_R) \rightarrow a_R,\ a_L \text{ xor } f(a_R, k)$

2) $F(a_R,\ a_L \text{ xor } f(f(a_R, k), k) =$

$F(a_L \text{ xor } f(f(a_R, k), k),\ a_R)$

1) $F(b_L, b_R) \rightarrow b_R,\ b_L \text{ xor } f(b_R, k)$

2) $F(b_R,\ b_L \text{ xor } f(b_R, k)) \rightarrow b_L \text{ xor } f(b_R, k),\ b_R \text{ xor } f(a_L, k)$

$q = a_R \text{ xor } b_R$

if $C_L = d_L$

$(C_L, C_R) = F(f(a_L, a_R))$

$(d_L, d_R) = F(F(b_L, b_R))$

(C_L, C_R)

$(C_L, dR) = F(f(a_L, dR))$

$q = C_R \text{ xor } d_R$

5. a) It prints the x and Y coordinates of the solution of the dual elipitical curve problem. If Q were to be published, anyone could find the x and y of the DC problem. It took a few seconds to run

b) Qx = 0x7a926a19fbdc7aa7e2e6c1476c368f0019e1d7cfdc2504d ada2e75c99e798

Qy = 0xfc8929031165790a40cdab6ec87e2078601447315e11a792cd4be67daaafa8

c) Qx = b89995a230041279c9cf06fa4eeaf7e95b10714dad42601038f1eaa8e63407a99a42204d2833b80df1c95bfad53d0fab

Qy 50ea7c117720729baba003e9c14e606e30ab3cc29f5ffd681379031ffe464b110873ddabf8dc85037e580d3f5fde70c

d) Qx f272381fd9b736ce6f9eb6810f98103919bafbd7b5538c3cbb785a9cc6dd75693851415c5b132c25831aebc22a2f71684c51b15e9f468d73d690dfdc437d997cc8

Qy 9afecd5b35fdead12550fa9e99d1ec49c3ab79bd1a2eb7b25c81ca0de315e363a006de5db6c89421cbb8c59810f51756484583c2f758ddc15edc0be92d8f511629