AARHUS UNIVERSITY - COMPUTER SCIENCE DEPARTMENT

Cryptology - Handin 4

Peter Burgaard - 201209175

October 5, 2016

1 STINSON 3.3

Let $DES(x,K)$ represent the encryotion of plaintext x with key K using the DES cryptosystem. Suppose $y = DES(x,K)$ and $y' = DES(c(x),c(K))$ where $c(\cdot)$ denotes the bitwise complement of its argument. Prove that $y' = c(y)$.

The DES encryption makes use of the *Feistel cipher*, described in section 3.5.1 as

$$L^i = R^{i-1}$$
$$R^i = L^{i-1} \oplus f(R^{i-1}, K^i)$$

To ease the notation from the exercise, let $x = L_0R_0$ and $c(x) = L_0'R_0'$ and $DES(L_0R_0,K) = y$ and $DES(L_0'R_0',K') = y'$. To prove $y' = c(y)$ we have to show $L_i' = c(L_i)$ and $R_i' = c(R_i)$ for any step in the process. We will prove by induction

Proof.

For basecase i = 1
For $DES(L_0R_0,K)$, by definition

$$L_1 = R_0$$
$$R_1 = L_0 \oplus f(R_0,K_0)$$

For $DES(L_0'R_0', K')$

$$\begin{aligned} L_1' &= R_0' \\ &= c(R_0) \\ &= c(L_1) \\ R_1' &= L_0' \oplus f(R_0', K_0') \\ &= c(L_0) \oplus f(c(R_0), c(K_0)) \end{aligned}$$

Pr step 2 on p. 96 Stinson, we know that f uses bitwise $\oplus$ on $c(R_0)$(after its expansion) and K_i before permutation in the S-boxes, and by $\oplus$ being communitativ and associative, we get

$$\begin{aligned} &= c(L_0) \oplus f(R_0, K_0) \\ &= c(L_0 \oplus f(R_0, K_0)) \\ &= c(R_1) \end{aligned}$$

Which proves the basecase.

INDUCTION HYPOTHESIS: Assume the claims holds for all $i < n$. We will consider the case where $i = n$

For $DES(L_0R_0, K)$, by definition

$$\begin{aligned} L_n &= R_{n-1} \\ R_n &= L_{n-1} \oplus f(R_{n-1}, K_{n-1}) \end{aligned}$$

For $DES(L_0'R_0', K')$

$$\begin{aligned} L_n' &= R_{n-1}' \\ &= c(R_{n-1}) \\ &= c(L_n) \\ R_n' &= L_{n-1}' \oplus f(R_{n-1}', K_{n-1}') \\ &= c(L_{n-1}) \oplus f(c(R_{n-1}), c(K_{n-1})) \\ &= c(L_{n-1}) \oplus f(R_{n-1}, K_{n-1}) \\ &= c(L_{n-1} \oplus f(R_{n-1}, K_{n-1})) \\ &= c(R_n) \end{aligned}$$

□

By Sting 3.5.1, we know DES uses 16 rounds of Feistel cipher, and there for, by the results above

$$y' = L_{16}'R_{16}' = c(L_{16}'R_{16}') = c(y)$$

which is the wanted answer.

2 EXTRA QUESTION

Given a chosen plaintext attack, show that you can use the complementation property to do exhaustive key search in about half the time it would normally take.

The reason for the key search space being half of its size using exhaustive key search comes from the fact that, when sending plaintext x we get output $DES(x,k) = y$, and since we can obtain the result for $DES(x',K') = y'$, without using the DES-function but just getting y's compliment we'll have checked both K and K' with one DES call. This implies the keyspace is now reduced from 2^{26} to $\frac{2^{56}}{2} = 2^{55}$ possible keys, which means it has been halfed.