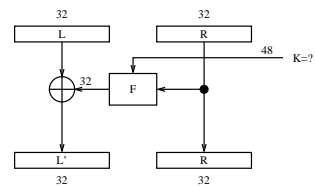


Block Ciphers — Tutorial

A Known Plaintext Attack on 1-Round DES

After removing the permutations IP and FP we get:



A Known Plaintext Attack on 1-Round DES (cont.)

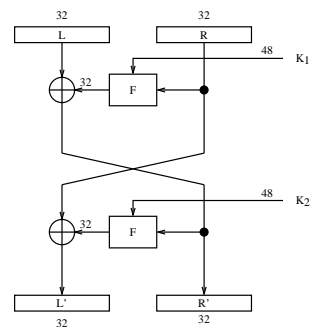
We are given a pair (M, C) where $M = (L, R)$ and $C = (L', R')$ and we want to find the 48-bit key K .

We know that:

$$F(R, K) = L \oplus L'$$

1. Why is the output of all S -boxes known?
2. Given the 4 bits output of S_1 how many 6-bit combinations are possible as input to S_1 ?
3. How many 6-bit combinations are possible as the 6 bit key which takes part in the creation of the input to S_1 ?
4. How many 48-bit combinations are possible for K ?

A Known Plaintext Attack on 2-Round DES



A Known Plaintext Attack on 2-Round DES (cont.)

Thus, we have:

- $F(R, K_1) = L \oplus R'$
- $F(R', K_2) = L' \oplus R$

As in the attack on one round, the first expression reduces the number of possibilities for the 48 bits of K_1 to $4^8 = 2^{16}$ (as only a fraction of 2^{-32} of the keys pass the test).

The second expression reduces the number of possibilities for the 48 bits of K_2 to $4^8 = 2^{16}$ as well.

The set of possibilities for K_1 and K_2 intersects on 40 bits, as there are 40 key bits which are common to both round keys K_1, K_2 . Thus, thus we get that the average number of possible 56-bit keys is slightly above 1.

A Known Plaintext Attack on 4-Round DES

After 4 rounds there are still bits which are unaffected by some key bits. For example:

- Original key bit 46 is not used in round 1.
- It is used in round 2 (in K_2) for the creation of the input to S_5 , thus it affects the 4 bits at the output of S_5 .
- These 4 bits become bits 8, 14, 25 and 3 after the permutation P.
- Key bit 46 is not used in round 3.
- Bits 8, 14, 25, 3 affect the output of $S_1, S_2, S_3, S_4, S_6, S_7$ in round 3, thus leaving the output bits of S_5 and S_8 unaffected by key bit 46.
- There are 8 bits in the left 32-bit output of round 3 unaffected from key bit 46.
- There are 8 bits in the right 32-bit output of round 4, unaffected from key bit 46 (but they are affected by the other key bits and by the plaintext).

A Known Plaintext Attack on 4-Round DES (cont.)

This property can be used for a known plaintext attack:

1. Fix key bit 46 to be zero.
2. For every key K^1 with the key bit 46 set to zero (there are 2^{55} such keys):
 - (a) Encrypt the plaintext: $C' = E_{K^1}(P)$.
 - (b) Compare the 8 bits which are unaffected by key bit 46 in C' with the same 8 bits in the given ciphertext C .
 - (c) If those bits are the same:
 - Denote K^1 with the 46'th bit set to one by K^2 .
 - If $E_{K^1}(P) = C$ then K^1 is probably the key.
 - If $E_{K^2}(P) = C$ then K^2 is probably the key.
 - If neither, continue to next key.

A Known Plaintext Attack on 4-Round DES (cont.)

Analysis: We encrypt the plaintext with all 2^{55} possibilities for the key K^1 . 2^{47} keys on average agree with the ciphertext on the 8 bits. Therefore, we encrypt 2^{47} possible K^2 values in order to find the original key. The resulting time complexity is $2^{55} + 2^{47}$ encryptions instead of 2^{56} .

Remark: When using the complementation property with this attack we get $2^{54} + 2^{46}$ encryptions in the worst case, and $2^{53} + 2^{45}$ encryptions in the average case.

A Known Plaintext Attack On 5-Round DES

Key bit 52 can be also used for an attack on 4 rounds:

- Original key bit 52 is not used in round 1.
- It is used in round 2 (in K_2) for the creation of the input to S_1 , thus it affects the 4 bits at the output of S_1 .
- These 4 bits become bits 9, 17, 23 and 31 after the permutation P.
- Key bit 52 is not used in round 3.
- Bits 9, 17, 23, 31 affect the output of $S_2, S_3, S_4, S_5, S_6, S_8$ in round 3, thus leaving the output bits of S_1 and S_7 unaffected by key bit 52.
- There are 8 bits in the left 32 bit output of round 3 unaffected from key bit 52.
- There are 8 bits in the right 32 bit output of round 4 unaffected from key bit 52.

A Known Plaintext Attack On 5-Round DES (cont.)

Key bit 52 has another property — it is not used in the 5'th round.

A Known Plaintext Attack On 5-Round DES (cont.)

Thus, we can use it for the following known plaintext attack:

1. Fix key bit 52 to be zero.
2. For every key K^1 with the key bit 52 set to zero (there are 2^{55} such keys):
 - (a) Encrypt the plaintext up to round 4: $E_{K^1}^4(P)$.
 - (b) Decrypt the ciphertext one round: $D_{K^1}^1(C)$.
 - (c) Compare the 8 bits which are unaffected by key bit 52 in $E_{K^1}^4(P)$ to the same 8 bits in $D_{K^1}^1(C)$.
 - (d) If those bits are the same:
Denote K^1 with the 52'th bit set to one by K^2 .
If $E_{K^1}(P) = C$ then K^1 is probably the key.
If $E_{K^2}(P) = C$ then K^2 is probably the key.

A Known Plaintext Attack On 5-Round DES (cont.)

Analysis: We encrypt the plaintext with all 2^{55} possibilities for the key K^1 with key bit 52 set to zero. We are left with 2^{47} keys on average. We also encrypt these 2^{47} possible K^2 in order to find the original key. Thus, we perform $2^{55} + 2^{47}$ encryptions instead of 2^{56} .

Remark: As in the attack on 4 rounds when using the complementation property we get $2^{54} + 2^{46}$ encryptions in the worst case, and $2^{53} + 2^{45}$ encryptions in the average case.