CS5760: Topics in Cryptanalysis **2025**

Lecture 2: 19 January 2025

Instructors: Maria Francis and M. V. Panduranga Rao *Scribe: Gautam Singh*

2.1 Cryptanalysis of DES Reduced to 4 Rounds

The notation for this reduced DES cryptosystem is shown in Figure 2.1.

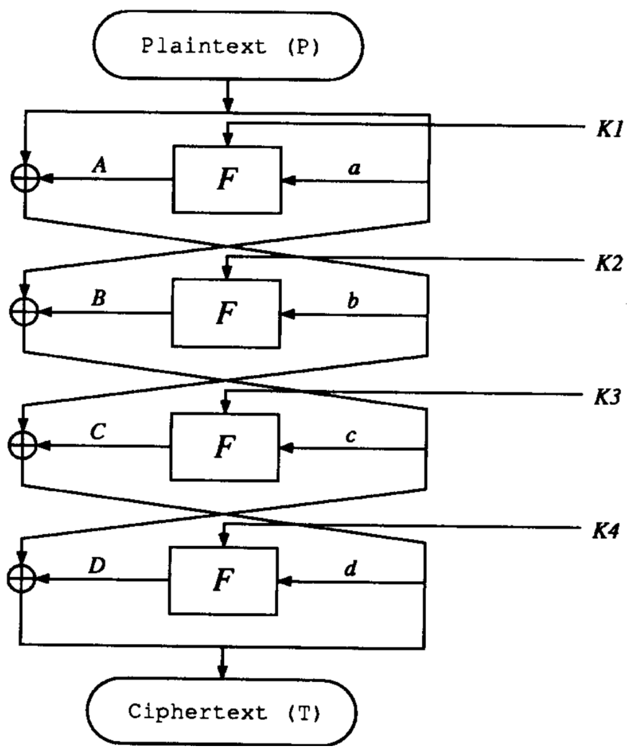

Figure 2.1: DES reduced to four rounds.

To find the master key, we make use of the characteristic shown in Figure 2.2. Using this characteristic, we have $a' = 0_x \implies A' = 0_x$. Thus, $b =$ `20 00 00 00` necessarily, and the single bit difference only diffuses from here on.

Since $a' = 0$, we write

$$c' = D' \oplus l' = a' \oplus B' \tag{2.1}$$

$$\implies D' = l' \oplus B', \tag{2.2}$$

where $T' = (l', r')$ is the ciphertext XOR. Further, we have $d' = r'$, so d' is completely known. Observe that $S'_{Eb} = 0$ for S2, ..., S8. Thus, $S'_{Ob} = 0$ always for 28 bits. Hence, S'_{Od} is known for S2, ..., S8. We find the 6-bit subkey blocks corresponding S_{Kd} using bruteforce to verify (2.3).

$$S(S_{Ed} \oplus S_{Kd}) \oplus S(S^*_{Ed} \oplus S_{Kd}) = S'_{Od}. \tag{2.3}$$

Since Ω^1_P has probability 1 and (d', D') is a right pair, we will find the right value of S_{Kd} with probability 1. Thus, we have found 42 bits of the subkey $K4$. If the DES key-scheduling algorithm is followed, these correspond to 42 key bits of the master key K. Finding the other 14 bits can be done by exhaustively searching the 2^{14} possibilities and verifying that the plaintexts are correctly encrypted. This leads to an attack with 2^{14} encryptions, which runs efficiently.

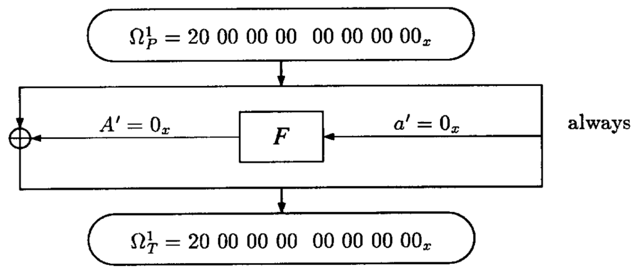

Figure 2.2: Characteristic used for cryptanalysis of DES reduced to four rounds.

2.1.1 DES With Independent Subkeys

Differential cryptanalysis can also work if the subkeys $K1, \dots, K4$ are generated independently and do not depend on a key-scheduling algorithm. As before, we can find 42 bits of $K4$. To find the remaining 6 bits, we use Ω^2_P shown in Figure 2.3. With this characteristic, we have $S1'_{Eb} = 0$, thus using a similar argument we can find $S1'_{Od}$ and apply the counting approach to get $S1_{Kd}$, which will completely find $K4$.

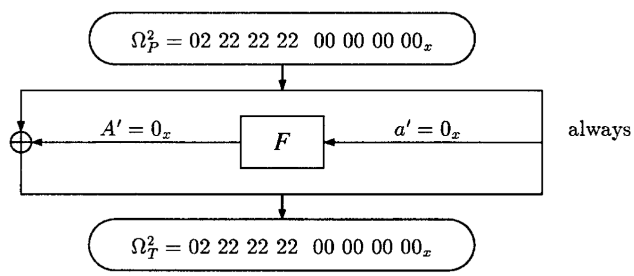

Figure 2.3: Second characteristic used to find K3 and K4 completely.

Finding $K3$ using Ω^2_P is straightforward. At this point, we can decrypt the fourth round to completely find c' and $C' = b' \oplus D'$. A similar counting argument can be used to find $K3$ completely.

To find $K1$ and $K2$ we will need to choose different characteristics, since both characteristics have $a' = 0 \rightarrow A' = 0$ and thus all keys are equally likely for $K1$. Similarly, some S boxes in the second round have zero XOR inputs and make all keys equally likely. To overcome these, we choose characteristics Ω^3_P and Ω^4_P arbitrarily such that

1. $S'_{Ea} \neq 0$ for all S boxes for both characteristics.
2. For every S box the S'_{Ea} values differ between the characteristics.

Knowing the value of b' after decryption of the third round, we can find $B' = c' \oplus a' = c' \oplus R'$. A similar counting argument will find the complete $K2$. Similarly, $A' = L' \oplus b'$ and thus the complete $K1$ can also be found. One can verify the keys have been found by encrypting plaintexts with these values and checking the outputs. This completes the cryptanalysis of DES reduced to 4 rounds. It also shows that differential cryptanalysis can work even if the round subkeys in DES are independently chosen.

For the cryptanalysis, a total of 16 encryptions are needed to find the keys with high probability: 8 pairs each of Ω^1 and Ω^2 and 4 pairs each of Ω^3 and Ω^4.

2.2 DES Reduced to 6 Rounds