

## 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.

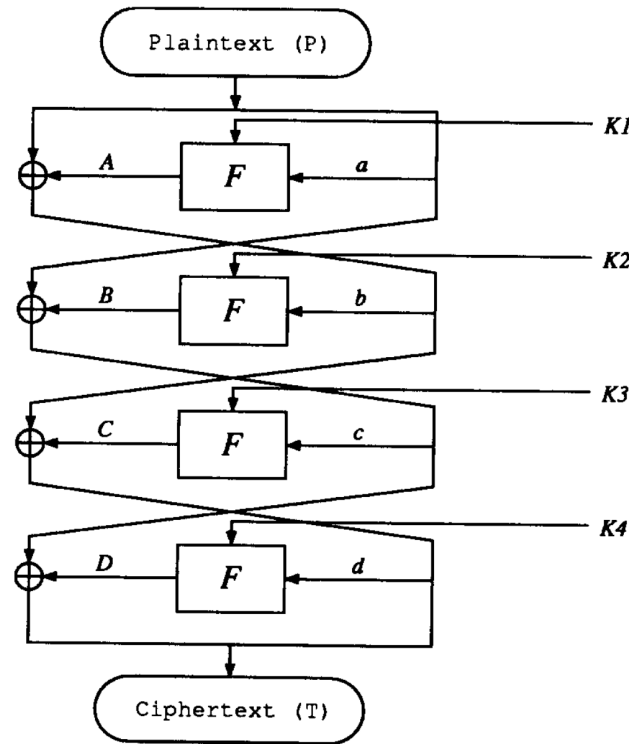


Figure 2.1: DES reduced to four rounds.

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

$$c' = D' \oplus l' = a' \oplus B' \quad (2.1)$$

$$\implies D' = l' \oplus B', \quad (2.2)$$

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

$$S(S_E \oplus S_K) \oplus S(S_E^* \oplus S_K) = S'_O. \quad (2.3)$$

Since  $\Omega_P^1$  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.

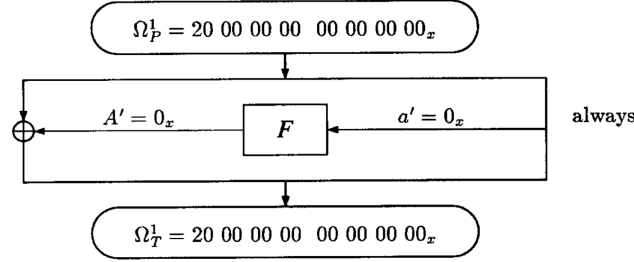


Figure 2.2: Characteristic used for cryptanalysis of DES reduced to four rounds.

### 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  $\Omega_P^2$  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  $K4$ .

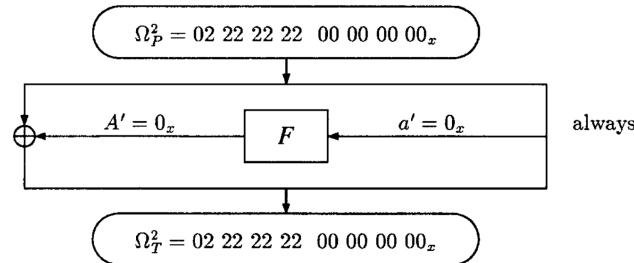


Figure 2.3: Second characteristic used to find K3 and K4 completely.

Finding  $K3$  using  $\Omega_P^2$  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  $\Omega_P^3$  and  $\Omega_P^4$  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  $\Omega^1$  and  $\Omega^2$  and 4 pairs each of  $\Omega^3$  and  $\Omega^4$ .

## 2.2 Cryptanalysis of DES Reduced to 6 Rounds

### 2.2.1 Characteristics for Recovering K6

For the cryptanalysis of DES reduced to 6 rounds, we make use of two characteristics, both with probability  $\frac{1}{16}$  as shown in Figure 2.4.

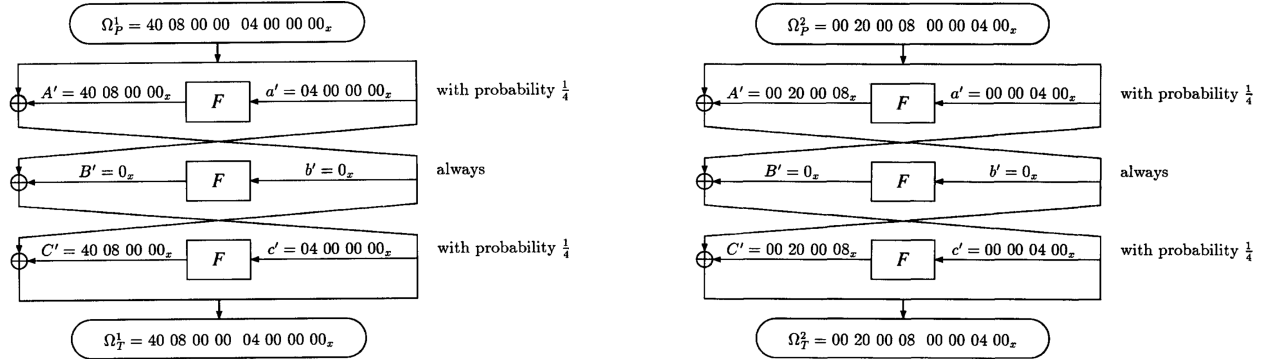


Figure 2.4: Characteristics used for cryptanalysis of DES reduced to 6 rounds.

For the characteristic  $\Omega_P^1$ , the S boxes S2, S5, ..., S8 have zero input XORs and for  $\Omega_P^2$ , the S boxes S1, S2, S4, S5 and S6 have zero input XORs in the fourth round. We write

$$e' = F' \oplus l' = c' \oplus D' \quad (2.4)$$

$$\implies F' = c' \oplus D' \oplus l' \quad (2.5)$$

### 2.2.2 Finding K6 Efficiently

From both characteristics, we can find 42 bits of  $K6$ . However, using a direct  $2^{30}$  counting approach for each characteristic is memory intensive. The authors proposed a graph-based algorithm to work around this. Consider a graph  $G = (V, E)$  where

1. Each  $v \in V$  represents a plaintext.
2. The edge  $(u, v)$  is labelled using a 64-bit mask for each S box, with each bit representing one of the possible 64 6-bit keys that enter that particular S box. Thus, each edge has five 64-bit masks associated with it.

3. We define a *clique* in  $G$  to be a set of vertices where the bitwise “and” of all edge labels for each of the five masks is nonzero.

Thus, the task is to find the largest such clique, which corresponds to the most likely values of  $S_{Kf}$  for the corresponding S boxes with zero XOR inputs. This can be done with a recursive clique finding algorithm. This works for smaller graphs with few edges as the complexity of this algorithm is exponential. Applying this algorithm for both characteristics, if the  $S_{Kf}$  values match for the common S boxes S2, S5 and S6, we have found 42 bits of  $K6$  with high probability.

### 2.2.3 Speeding up the Cryptanalysis

Though brute forcing the other 14 bits of the master key is already fast enough, we can do better by finding the other 6 key bits entering S3 in the sixth round. First, we filter out pairs satisfying (2.5), leaving us with  $\frac{1}{16}$  possibly right pairs. Then, for each possible value of  $S3_{Kf}$ , we decrypt the sixth round to get  $e$  and  $e^*$ , using which we verify the equality  $E' = d' \oplus f'$ . Specifically, we verify that  $Si'_{O_e}$  for  $i \in \{2, 3, 8\}$  match the computed value of  $E'$ . Only one of the 64 possibilities will survive with high probability since the chances of another possibility also satisfying the given inequality is  $2^{-20}$ . This works because of the dependence of  $S_{Ke}$  on the key bits in  $S_{kf}$  as shown in Figure 2.5.

Into S box number	$e$ bits $S_{Ee}$	Key bits $S_{Ke}$
S1	++++++	<b>3</b> + . . ++
S2	++ <b>3</b> +++	+ <b>3</b> + <b>3</b> <b>3</b> <b>3</b>
S3	++++++	++++++
S4	++++ <b>3</b> +	++ . . ++
S5	<b>3</b> +++++	+++ . ++
S6	++++ <b>3</b> +	+ . + . ++
S7	<b>3</b> +++++	+++ . ++
S8	++ <b>3</b> +++	++++++

Figure 2.5: Dependence of  $K5$  on bits of  $K6$ . The ‘3’ indicates dependence on  $S3_{Kf}$ , the ‘.’ indicates bits unused in  $K6$  and the ‘+’ indicates dependence on known key bits of  $K6$ .

After finding  $K6$  entirely, one can now brute force the other 8 missing key bits of the master key, leading to a faster cryptanalysis of DES reduced to six rounds.