CS5760: Topics in Cryptanalysis **2025**

Lecture 3: 22 January 2025

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

3.1 Cryptanalysis of DES Reduced to 8 Rounds

DES reduced to 8 rounds uses a 5-round characteristic with probability approximately $\frac{1}{10486}$ as shown in Figure 3.1.

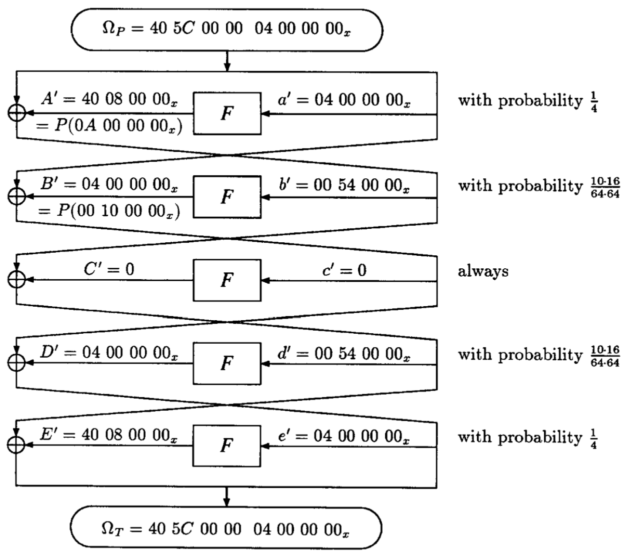

Figure 3.1: 5 round characteristic used to cryptanalyze DES reduced to 8 rounds.

From the characteristic, it is evident that

$$f' = d' \oplus E' = b' \oplus A' = L' = \texttt{40 5C 00 00}. \tag{3.1}$$

Thus, for a right pair, five S boxes S2, S5, ..., S8 have zero input XORs in the sixth round. Using

$$H' = l' \oplus g' = l' \oplus e' \oplus F' \tag{3.2}$$

and the fact that $h' = r'$, we can count on $5 \cdot 6 = 30$ key bits of $K8$. The signal to noise ratio is $S/N = \frac{2^{30}}{4^5 \cdot 10486} \approx 100$. However, due to the large memory requirement of 2^{30} locations, we count on fewer key bits. Further, due to the small probability of the characteristic, we require many plaintexts, which makes the clique method slow. Notice that each S box discards 20 % of wrong pairs. Thus, counting on 24 key bits has $S/N = \frac{2^{24}}{4^4 \cdot 0.8 \cdot 10486} \approx 7.8$ and counting on 18 key bits has $S/N = \frac{2^{18}}{4^3 \cdot 0.8^2 \cdot 10486} \approx 0.6$.

3.1.1 Modifying the Characteristic

By reducing the number of key bits to count, we can also choose which key bits are to be counted in order to improve the signal to noise ratio. Notice that

$$e' = \texttt{04 00 00 00} \rightarrow E' = P(\texttt{0W 00 00 00}) = \texttt{X0 0Y Z0 00} \tag{3.3}$$

where $W \in \{0,1,2,3,8,9,A,B\}$, $X, Z \in \{0,4\}$, $Y \in \{0,8\}$. Hence, we have $f' = d' \oplus E' = \texttt{X0 5V Z0 00}$ where $V = Y \oplus 4$. If $Z = 0$, then necessarily $E' = \texttt{40 08 00 00}$ and this happens with probability $\frac{16}{64}$. All other combinations involving $Z = 4$ occur with probability $\frac{20}{64}$.

Although we cannot count on $S5_{Kh}$, one can check $S5'_{Eh} \rightarrow S5'_{Oh}$ which is satisfied by approximately 80 % of the pairs. Thus, the modified probability of $e' \rightarrow E'$ is $\frac{16}{64} + 0.8\frac{20}{64} = \frac{1}{2}$. This doubles the probability of the characteristic Ω_P to $\frac{1}{5243}$ and consequently doubles the S/N for counting on 24 bits and 18 bits of $K8$ to 15.6 and 1.2 respectively.

Counting on 24 subkey bits, we only require about five right pairs due to the high S/N. This gives us approximately 25000 plaintext pairs. For 18 subkey bits, we need about 150000 pairs. The average count per key is $\frac{150000 \times 4^3 \times 0.8^2}{2^18} = 24$ and the right key is counted an additional $\frac{150000}{5243} = 29$ times, giving a total count of $24 + 29 = 53$ for the right key.

However, this finds us 18 subkey bits, say entering S6, S7 and S8. To find the other 12 subkey bits entering S2 and S5 in the eighth round, we filter the pairs that correspond to the subkey values in S6, S7 and S8. The expected number of pairs is then 53. Counting on the remaining 12 bits using these right pairs leads to a higher S/N which can filter more pairs.

Now, using the known 30 subkey bits of $K8$, we can find the dependence of the bits of S_{Eg} and S_{Kg} on $K8$, shown in Figure 3.2.

Into S box number	g bits S_{Eg}	Key bits S_{Kg}
S1	+ 4 + + + +	3 + . . 4 +
S2	+ + 3 + + 1	1 3 4 3 3 3
S3	+ 1 4 + + +	+ 1 + 4 1 +
S4	+ + + + 3 1	1 1 . . 1 +
S5	3 1 + + 4 +	+ + + . + +
S6	4 + + 1 3 +	+ . + . + +
S7	3 + 4 + + +	+ + + . + +
S8	+ + 3 1 + 4	+ + + + + +

Figure 3.2: Dependence of bits at the seventh round on those of the eighth round. '+' indicates dependence on known key bits, '.' indicates dependence on other key bits and a number indicates dependence on unknown key bits that enter the corresponding S box in the eighth round.

By checking using the formula $G' = f' \oplus h'$ for S2, S3 and S8, we can brute force the remaining 18 key bits of $K8$. This equation holds for all filtered pairs. A faster way is to count on the 12 bits entering S1 and S4 in the eighth round, since they compute $S3'_{Og}$. After further filtration, we count on the remaining 6 subkey bits to get $K8$ completely. Brute-force on the remaining 8 bits unused in $K8$ will give us the master key.

3.1.2 Speeding Up the Attack

Post every step of filtration, wrong pairs can be discarded. Counting on 24 bits will reduce the 25000 pairs to $25000 \times 0.8^5 \approx 7500$ pairs. However, this is not so good for counting on 18 bits. The authors devised another criterion based on a weighting function and a threshold. This weighting function is the product of the number of possible keys of each of the five countable S boxes. A right pair would suggest more possible keys than a wrong pair at an S box, thus a carefully chosen threshold can discard the wrong pairs. Experimentally, setting a threshold of 8192 discards about 97 % of right pairs. This reduces the number of pairs analyzed from 150000 to 7500 and greatly speeds up the attack.

3.1.3 Enhanced Characteristics

The authors list two ways to boost the probability of characteristics and enhance signal-to-noise ratio.

1. By exploiting possible input and output XORs in S boxes, we can eliminate some possibilities. For instance, Figure 3.3 shows that for $08_x \rightarrow A_x$, the bits at positions 2 and 6 are always equal. Thus, we can use plaintexts which cause these bits to be equal. We can see that both bits equal 0 with probability $\frac{12}{16}$ and both equal 1 with probability $\frac{4}{16}$. This improves the probability of the characteristic to $\frac{1}{2}$, doubling the S/N.

$S2_I$ 123456	$S2_I^*$ 123456	$S2_O$ 1234	$S2_O^*$ 1234
000010	001010	0001	1011
000110	001110	1110	0100
010001	011001	1100	0110
010101	011101	0001	1011
100000	101000	0000	1010
100010	101010	1110	0100
100100	101100	0111	1101
100110	101110	1011	0001

Figure 3.3: Possible instances for $08_x \rightarrow A_x$ by S2.

2. In case the key bits at those positions are known, then we could choose the $\frac{12}{16}$ case which triples the S/N.

3.1.4 Extension to Nine Rounds

We concatenate the following characteristic with the one in Figure 3.1 to cryptanalyze DES reduced to 9 rounds.

The entire six-round characteristic has probability $\approx 10^{-6}$. Thus, counting on 30 subkey bits gives $S/N = \frac{2^{30}}{4^5 \cdot 10^6} \approx 1$. After finding these 30 subkey bits, a similar process is followed by exploiting the relations between

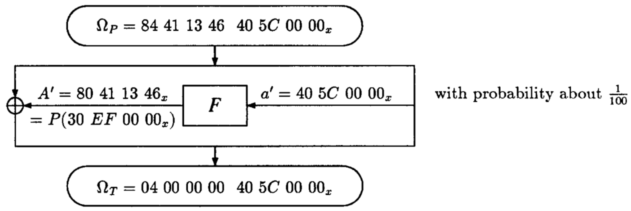

Figure 3.4: Characteristic to be concatenated to cryptanalyze DES reduced to 9 rounds.

bits in the eighth and ninth round to get the other 18 bits of $K9$. Due to the low S/N, we require about 30 million pairs.

3.2 DES with an Arbitrary Number of Rounds

3.2.1 Iterative Characteristics

To cryptanalyze DES reduced to an aribitrary number of rounds, we make use of an *iterative* characteristic. Such a characteristic can be concatenated with itself to generate longer characteristics. An iterative characteristic is shown in Figure 3.5.

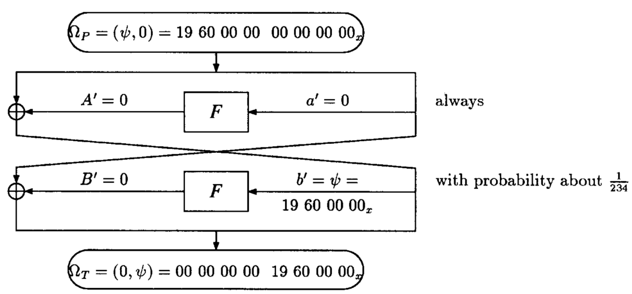

Figure 3.5: Iterative characteristic with probability $\frac{1}{234}$. Another value for ψ could be `1B 60 00 00`.

This iterative characteristic has probability $\approx 2^{-56}$ when extended to 15 rounds. Thus, using this characteristic to cryptanalyze the entire DES performs worse than exhaustive search.

Depending on the additional number of rounds in the cryptosystem that are outside of the characteristic, we can categorize attacks into four types. In most cases these additional rounds are the last rounds of the cryptosystem.

3.2.2 3R-Attacks

These have 3 additional rounds in the cryptosystem. DES reduced to 4, 8 or 9 rounds can be cryptanalyzed with this kind of attack. For DES reduced to 8 rounds, using the iterative characteristic with probability about $\frac{1}{234^2} = \frac{1}{55000}$, counting on 24 key bits gives $S/N = \frac{2^{24}}{4^4 \cdot 0.8 \cdot 55000} \approx 1.5$ and counting on 30 key bits gives $S/N = \frac{2^{30}}{4^5 \cdot 55000} \approx 19$, reducing the number of pairs to $(1 - 0.8^5) = 67\%$ of the original.

For a fixed cryptosystem, 3R attacks have shorter characteristics with better probability, thus they are the most useful.

3.2.3 2R-Attacks

These have 2 additional rounds in the cryptosystem. To boost the S/N, possibility checks can be performed for all previous round S boxes, that is, predicting whether an input-output XOR pair is possible.

For example, in DES reduced to 9 rounds, we can use the iterative characteristic with probability 2^{-24} for seven rounds. The iterative characteristic gives

$$h' = \psi \to H' = i' \oplus g' = r' \tag{3.4}$$
$$i' = r' \to I' = h' \oplus l' = \psi \oplus l' \tag{3.5}$$

For $h' \to H'$, five S boxes have zero input XOR. A wrong pair can pass through this S box with probability $\frac{1}{16}$. For the other three S boxes this probability is 0.8. Hence, counting on all 48 bits of $K9$ has $S/N = \frac{2^{48} \cdot 2^{-24}}{4^8 \cdot 0.8^3 \cdot 16^{-5}} \approx 2^{29}$. Counting on 18 bits has $S/N = \frac{2^{18} \cdot 2^{-24}}{4^3 \cdot 0.8^5 \cdot 0.8^3 \cdot 16^{-5}} \approx 2^{11}$. Counting on just 6 key bits has $S/N = \frac{2^6 \cdot 2^{-24}}{4 \cdot 0.8^7 \cdot 0.8^3 \cdot 16^{-5}} \approx 10$. By checking with the previous round S boxes, we are left with $0.8^3 \cdot 16^{-5} = 2^{-24}$ wrong pairs. Since the characteristic has probability 2^{-24}, we require 2^{26} pairs for cryptanalysis.

Similar analyses can be carried out for DES reduced to 11, 13 and 15 rounds. However, more plaintext pairs are required for cryptanalysis which makes the attacks unrealistic.

3.2.4 1R-Attacks

These have only one additional round in the cryptosystem. Here, we can only verify the value of r' and perform possibility checks on the S boxes of the last round only. The input XOR to the last round is constant, thus we cannot single out a subkey value for each S box. Instead, we have to exhaustively search these key values (which are reduced in number due to the input-output XOR pair).

For example, DES reduced to 10 rounds can be broken with the 9 round characteristic where

$$i' = 0 \to I' = 0 \tag{3.6}$$
$$j' = \psi \to J' = l' \oplus i' = l' \tag{3.7}$$

Right pairs satisfy $r' = \psi$ and the 20 bits in l' going out of S4, ..., S8 are zero. This holds for $2^{-32} \cdot (2^{-4})^5 = 2^{-52}$ of the wrong pairs. For the other three S boxes, we count on the 18 key bits to get $S/N = \frac{2^{18} \cdot 2^{-32}}{4^3 \cdot 2^{-52}} = 2^{32}$. Thus, we require 2^{34} pairs.