

# M2 Cybersecurity (Univ. Grenoble Alpes/Grenoble INP)

## Cryptographic Mechanisms (Part 3) The Post-Quantum Cryptography Era

v1.1, December 2016

Philippe Elbaz-Vincent



## Review of the DES

**DES** (Data Encryption Standard) is a Feistel cipher with  $n = 64$  bits, producing ciphertext of 64 bits. The **size of the key is 56 bits** with **8 supplementary bits used for parity tests**. If  $L_{i-1}$  and  $R_{i-1}$  are the half-block of 32 bits produced at the step  $i - 1$ , we build  $L_i$  and  $R_i$  as follows :

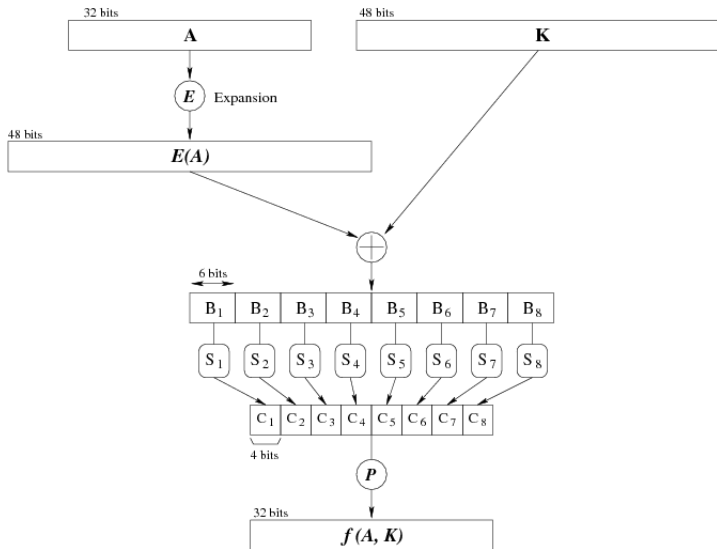
$$\begin{aligned}L_i &= R_{i-1} , \\R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) , \\f(R_{i-1}, K_i) &= P(S(E(R_{i-1}) \oplus K_i)) ,\end{aligned}$$

where  **$E$**  is the expansion function transforming  $R_{i-1}$  in a word of 48 bits. The function  **$P$**  is a permutation of 32 bits ( **$P$ -box**) and  **$S$**  is an  **$S$ -box**. The number of steps (a.k.a., rounds) is 16.

In order to add some diffusion, we perform an **Initial Permutation** (often called  **$IP$** ) on the 64 bits input and a **Final Permutation** on the 64 bits output. This final permutation is given as the **inverse of the initial permutation** (i.e., it is  $IP^{-1}$ ).

☞ *In the DES, the Feistel function  $f$  is a complicated function designed in order to mask the subkeys.*

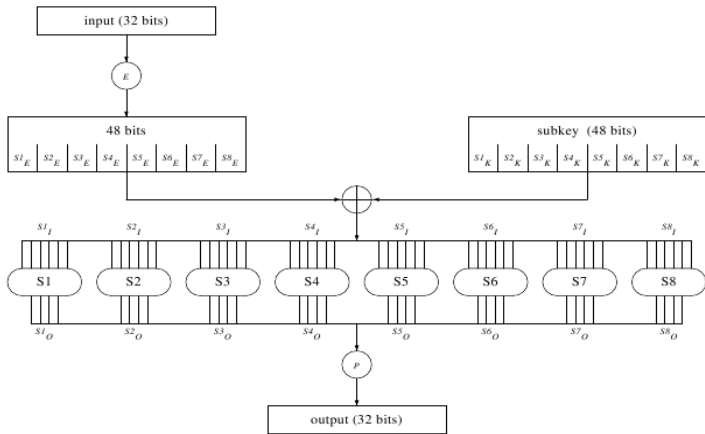
# DES : Feistel function General Chart



## DES : zoom on the function $f$

- $f(A, K) = P \circ S(E(A) \oplus K)$  (with  $A$  either  $L$  or  $R$ ),
- $A$  and  $f(A, K)$  are 32 bits= $8 \times 4$ ,
- $E(A)$  and  $K$  (subkey used in the current round) are 48 bits= $8 \times 6$ ,
- $E$  is the expansion map (it is a "hidden permutation"),
- and  $P$  is a permutation.

## The DES chart revisited at the level of the S-boxes



Let  $S$  be a given S-box. Then the input of  $S$ , denoted  $S_I$  is given by  $S_I = S_E \oplus S_K$ , where  $S_K$  are the 6 bits of (sub)key for  $S$  and  $S_E$  are the 6 bits of expansion (from the initial input) for  $S$ .

## The DES permutations (Part I)

The expansion map  $E : \{1, \dots, 32\} \rightarrow \{1, \dots, 48\}$ , is given by the following table :

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

## The DES permutations (Part II)

The permutation  $P : \{1, \dots, 32\} \rightarrow \{1, \dots, 32\}$  and its inverse are given by :

P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

$P^{-1}$							
9	17	23	31	13	28	2	18
24	16	30	6	26	20	10	1
8	14	25	3	4	29	11	19
32	12	22	7	5	27	15	21

## DES : S-Boxes (Part I)

- $S = S_1, \dots, S_8$  : pack of 8 substitution boxes,
- arrays with 4 lines and 16 columns,
- one use to transform a 6 bits input

$$B = b_1 b_2 b_3 b_4 b_5 b_6$$

to the element  $C$  in the line  $i$  and the column  $j$  :

$$i = b_1 b_6, \quad j = b_2 b_3 b_4 b_5$$

- Example for  $S_1$  : 7 in the 2nd line and the 3rd column corresponds to  $i = 10$ ,  $j = 0011$ , and so to the input  $B = 100101$ .

S1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



## DES : S-Boxes (Part II)

S1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

## DES : S-Boxes (Part III)

S5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

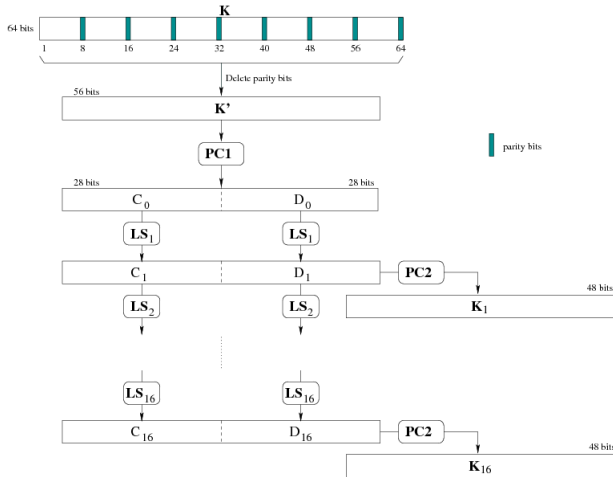
S8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

## DES : Key schedule

One set  $v_i = 1$  for  $i = 1, 2, 9, 16$  and  $v_i = 2$  otherwise. We get blocks  $C_i$  and  $D_i$  of 28 bits long.

- ① We take  $(C_0, D_0) = PC1(K)$ ,
- ② For each round  $i$  from 1 to 16 :
  - ① We obtain  $C_i$  from  $C_{i-1}$  by an “offsetting offshifting”  $v_i$  to left,
  - ② We obtain  $D_i$  from  $D_{i-1}$  by an “offsetting offshifting”  $v_i$  to left,
  - ③ We take  $K_i = (PC2(C_i, D_i))$ .

# DES : Key schedule chart



## DES : Key schedule - PC1

The choose and permute tables PC1 and PC2 (“permuted choice”) used in the keys schedule are :

$PC1 : \{1, \dots, 64\} \setminus \{8, 16, 24, \dots, 64\} \rightarrow \{1, \dots, 56\} :$

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

## DES : Key schedule - PC2

$PC2 : \{1, \dots, 56\} \rightarrow \{1, \dots, 48\}$ .

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

## DES : Sample running of a round

- Key : 01000111 01001001 01001100 01001100 01000001 01010010  
01000100 00100000
- after pc1 : 00000000 01111111 10000000 00100010 00010100  
11010000 11100000
- offset : 00000000 11111111 00000000 01000100 00101001 10100001  
11000000
- Subkey : 10100000 10010010 10100010 10010011 00010100  
00001000
  
- Plain text : 01010000 01101111 01110101 01110010 01110001  
01110101 01101111 01101001
- After IP : 11111111 00111101 01100110 11110110 00000000  
11111110 11000010 01001010
- E input : 00000000 11111110 11000010 01001010
- E Output : 00000000 00010111 11111101 01100000 01000010  
01010100
- Sub Key : 10100000 10010010 10100010 10010011 00010100  
00001000
- xor : 10100000 10000101 01011111 11110011 01010110 01011100
- output of the boxes : 1101 0110 0101 ....
- after P : ....
- Round Input : 11111111 00111101 01100110 11110110 00000000  
11111110 11000010 01001010
- Right half : 00110011 10111100 11000010 10000100
- Left half : 00000000 11111110 11000010 01001010

## Some examples of pairs plaintext/ciphertext for particular keys

<i>Key</i>	<i>Plaintext</i>	<i>Ciphertext</i>
0000000000000000	0000000000000000	8CA64DE9C1B123A7
FFFFFFFFFFFFFFFF	FFFFFFFFFFFFFFFF	7359B2163E4EDC58
3000000000000000	1000000000000001	958E6E627A05557B
1111111111111111	1111111111111111	F40379AB9E0EC533
0123456789ABCDEF	1111111111111111	17668DFC7292532D
1111111111111111	0123456789ABCDEF	8A5AE1F81AB8F2DD
FEDCBA9876543210	0123456789ABCDEF	ED39D950FA74BCC4
7CA110454A1A6E57	01A1D6D039776742	690F5B0D9A26939B
0131D9619DC1376E	5CD54CA83DEF57DA	7A389D10354BD271
07A1133E4A0B2686	0248D43806F67172	868EBB51CAB4599A
3849674C2602319E	51454B582DDF440A	7178876E01F19B2A
04B915BA43FEB5B6	42FD443059577FA2	AF37FB421F8C4095
0113B970FD34F2CE	059B5E0851CF143A	86A560F10EC6D85B
0170F175468FB5E6	0756D8E0774761D2	0CD3DA020021DC09
43297FAD38E373FE	762514B829BF486A	EA676B2CB7DB2B7A
07A7137045DA2A16	3BDD119049372802	DFD64A815CAF1A0F
04689104C2FD3B2F	26955F6835AF609A	5C513C9C4886C088
37D06BB516CB7546	164D5E404F275232	0A2AEAE3FF4AB77
1F08260D1AC2465E	6B056E18759F5CCA	EF1BF03E5DFA575A
584023641ABA6176	004BD6EF09176062	88BF0DB6D70DEE56
025816164629B007	480D39006EE762F2	A1F9915541020B56



## Differential cryptanalysis : A summary

This technic was known from the NSA and the DES team in 1977 ; it was rediscovered and published in 1987 by E. Biham and A. Shamir.

The principle is to select plaintexts with specific differences and find from this plaintexts, corresponding ciphertexts who also have some specific differences. This would reveal information on the key. DES has been strengthened against this attack. The amount of ciphered data to mount this attack is around  $2^{47}$  blocks (1024 Terabytes) in order to get few bits of the key (then we can eventually switch to exhaustive key search).

However, it is possible to perform a differential cryptanalysis on reduced version of the DES (with say  $r$  rounds, and  $r \leq 9$ ).

## Linear cryptanalysis : A summary

This cryptanalysis is due to Matsui (1993). The idea is to construct a linear equation involving certain bits of plaintext, ciphertext and the key, which is true with a probability different from  $1/2$ . The attacker analyses a large number of pairs plaintext/ciphertext in order to retrieve the “most likely key” (i.e., the key with the higher probability). In the case of DES, we need  $2^{43}$  random pairs of plaintexts/ciphertexts in order to get 22 bits of the key. The remaining bits can be found from exhaustive search. Nevertheless, in the DES case, the amount of plaintexts/ciphertexts is too unrealistic !

However, as for differential cryptanalysis, it is possible to perform a linear cryptanalysis on reduced version of the DES (with say  $r$  rounds, and  $r \leq 9$ ).

## Invariants for Linear and Differential cryptanalysis

A substitution function  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$  used in a block cipher is (in general) the only non linear part in it.

If  $x = (x_0, \dots, x_{n-1}) \in \mathbb{F}_2^n$ , let  $y = (y_0, \dots, y_{m-1}) = F(x)$ . We now introduce the quantities  $\delta_F$  and  $\lambda_F$  related to differential and linear cryptanalysis that measure the non-linearity of  $F$ .

☞ **They should be small.**

For instance the AES substitution is exceptionally good with  $(\delta_F, \lambda_F) = (4, 16)$ .

## Differential invariant

The differential invariant  $\delta_F$  measures the deviation from a linear function verifying  $F(a \oplus x) = F(a) \oplus F(x)$  where  $\oplus$  is the XOR operator (notice that XOR=+ in  $\mathbb{F}_2^\ell$ ).

It is defined by

$$\delta_F = \max_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, a \neq 0} (\{\delta_F(a, b)\}),$$

with  $\delta_F(a, b) = \#\Delta_F(a, b)$  and

$$\Delta_F(a, b) = \{x \in \mathbb{F}_2^n, F(x) \oplus F(a \oplus x) = b\} = \{x \in \mathbb{F}_2^n, F(a \oplus x) = b \oplus F(x)\}.$$

Note that  $\delta_F$  is by construction an even number  $\geq 2$ .

Besides, if  $F$  is linear, then for all  $x \in \mathbb{F}_2^n$ ,  $y \in \mathbb{F}_2^m$ , we have  $F(x) \oplus F(a \oplus x) = F(a)$ . So  $\delta_F(a, b) = 2^n$  if  $b = F(a)$ . Otherwise  $\delta_F(a, b) = 0$ .

# Comments on what we measure with $\Delta_F(a, b)$ and $\delta_F(a, b)$

## [1]

We are looking for pairs  $(a, a^*)$  with  $a, a^* \in \mathbb{F}_2^n$  and pairs  $(b, b^*)$  with  $b, b^* \in F_2^m$ , such that  $b = F(a)$ ,  $b^* = F(a^*)$  and

$$F(a \oplus a^*) = b \oplus b^*.$$

The XOR values  $a \oplus a^*$  and  $b \oplus b^*$  are respectively the input and output XOR differences. We are looking at pairs such that the output XOR correspond to the encryption of the input XOR. In fact, the set  $\Delta_F(a, b)$  is, at first look, more general than that and restrict the search to one parameter. But they are intimately related.

## Comments on what we measure with $\Delta_F(a, b)$ and $\delta_F(a, b)$

[2]

For any  $\delta_I \in \mathbb{F}_2^n$  and  $\delta_O \in \mathbb{F}_2^m$ , we define

$$\Delta'_F(\delta_I, \delta_O) = \{(x_1, x_2; y_1, y_2), y_1 = F(x_1), y_2 = F(x_2), x_1, x_2 \in \mathbb{F}_2^n, \\ y_1, y_2 \in \mathbb{F}_2^m, x_1 \oplus x_2 = \delta_I, y_1 \oplus y_2 = \delta_O\}.$$

The  $\delta_I$  and  $\delta_O$  are the input and output XOR differences (also called the XORed input and output).

Then we have a bijection between  $\Delta'_F(a, b)$  and  $\Delta_F(a, b)$ .

Consider the maps

$$\iota : \Delta'_F(a, b) \rightarrow \Delta_F(a, b) \\ (x_1, x_2; y_1, y_2) \mapsto x_1,$$

and

$$\iota' : \Delta_F(a, b) \rightarrow \Delta'_F(a, b) \\ x \mapsto (x, x \oplus a; F(x), F(x \oplus a)).$$

## Comments on what we measure with $\Delta_F(a, b)$ and $\delta_F(a, b)$

### [3]

First, both maps are well defined. Indeed, if

$(x_1, x_2; y_1, y_2) \in \Delta'_F(a, b)$  then  $x_1 \oplus x_2 = a$  and  $F(x_1) \oplus F(x_2) = b$ .

Thus,  $x_2 = x_1 \oplus a$  and  $F(x_1) \oplus F(x_1 \oplus a) = b$ . Showing that  $x_1 \in \Delta_F(a, b)$ .

Now, if  $x \in \Delta_F(a, b)$ , we have  $F(x) \oplus F(x \oplus a) = b$ , which again shows that  $(x, x \oplus a; F(x), F(x \oplus a)) \in \Delta'_F(a, b)$ . Second, we can immediately check that both maps are inverse of each other.

Hence, the set  $\delta_F(a, b)$  measure the number of pairs (plaintexts and ciphertexts, i.e. transformed by  $F$ ) with prescribed XORed input and output and  $\Delta_F(a, b)$  gives the explicit list of possible pairs.

Notice also that when  $x \in \Delta_F(a, b)$ , you immediately have a pair  $(x, x^*)$  of prescribed XOR input (and corresponding XOR output), since  $x \oplus x^* = a$  means that  $x^* = x \oplus a$ .

## Linear invariant

The linear invariant  $\lambda_F$  indicates whether there exist linear relations between input bits and output bits. Only a likely relation would be useful for an attack.

It is defined by

$$\lambda_F = \max_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, b \neq 0} (\{\lambda_F(a, b)\}),$$

with

$$\lambda_F(a, b) = \left| -2^{n-1} + \#\{x \in \mathbb{F}_2^n, \langle a, x \rangle \oplus \langle b, F(x) \rangle = 0\} \right|,$$

where  $\langle x, y \rangle = \sum_{i=0}^{\ell-1} x_i y_i$  is the "scalar product" in  $\mathbb{F}_2^\ell$ .




## Cartography of the DES S-boxes

We can compute the differential and linear invariants for the 8 S-boxes of the DES. We will also give detailed (pairs XOR) distribution tables for each S-boxes w.r.t.  $\delta$  and  $\lambda$ .

The values of the pairs  $(\delta, \lambda)$  for each S-box is given below

S-box number	$(\delta, \lambda)$
1	(16,18)
2	(16,16)
3	(16,16)
4	(16,16)
5	(16,20)
6	(16,14)
7	(16,18)
8	(16,16)

 **Notice, as we will see later, that there is a link between the max value of  $\delta$  and the number of rounds for DES...** See the DES invariant tables at the end of this slide.

## Revisiting differential cryptanalysis (after Biham and Shamir) [1]

Recall that Differential cryptanalysis is a method which analyses the effect of particular differences in plaintext pairs on the differences of the resultant ciphertext pairs.

These differences can be used to assign probabilities to the possible keys and to locate the *most probable* key.

This method usually works on many pairs of plaintexts with the same particular difference using only the resultant ciphertext pairs.

For DES-like cryptosystems the difference is chosen as a fixed XORed value of the two plaintexts.

## Revisiting differential cryptanalysis (after Biham and Shamir) [2]

In the following we will denote by  $F$  the DES function and even  $F_r$  the DES reduced to  $r$  rounds. The initial and final permutations will be ignored (they have no significance on the attack).

At any intermediate point during the encryption of pairs of messages,  $X$  and  $X^*$  are the corresponding intermediate values of the two executions of the algorithm and  $X'$  is defined by

$$X' = X \oplus X^*.$$

## Revisiting differential cryptanalysis (after Biham and Shamir) [3]

Given the XOR value of an input pair to the  $F$  function we determine its XOR value after the expansion by the formula :

$$E(X) \oplus E(X^*) = E(X \oplus X^*).$$

The XOR with the key does not change the XOR value in the pair, i.e., the expanded XOR stays valid even after the XOR with the key, by the formula :

$$(X \oplus K) \oplus (X^* \oplus K) = X \oplus X^*.$$

The output of the S-boxes is mixed by the  $P$  permutation and thus the XOR of the pair after the  $P$  permutation is the permuted value of the S-boxes output XOR, by the formula

$$P(X) \oplus P(X^*) = P(X \oplus X^*).$$

## Revisiting differential cryptanalysis (after Biham and Shamir) [4]

The output XOR of the  $F$  function is linear in the XOR operation that connects the different rounds :

$$(X \oplus Y) \oplus (X^* \oplus Y^*) = (X \oplus X^*) \oplus (Y \oplus Y^*).$$

The XOR of pairs is thus invariant in the key and is linear in the  $E$  expansion, the  $P$  permutation and the XOR operation.

The S-boxes are known to be non linear. Knowledge of the XOR of the input pairs cannot guarantee knowledge of the XOR of the output pairs. Usually several output XORs are possible.

A special case arises when both inputs are equal, in which case both outputs must be equal too. However, a crucial observation is that for any particular input XOR not all the output XORs are possible, the possible ones do not appear uniformly, and *some XORed values appear much more frequently than others* (this is the motivation for the “differential distribution tables”).

# The principle of differential cryptanalysis illustrated on a DES S-box [1]

For the first box (i.e.,  $S_1$ ), we get :

$$\Delta_1(54, 1) = \{4, 7, 12, 49, 50, 58\} . \quad (0.1)$$

and therefore :  $\delta_1(54, 1) = 6$  (for simplicity we will write  $\Delta_i$  and  $\delta_i$  instead of  $\Delta_{S_i}$  and  $\delta_{S_i}$ ).

Here is the list of corresponding pairs  $(x, x^*)$  :

$(4, 50); (7, 49); (12, 58); (49, 7); (50, 4); (58, 12)$  Notice that here  $x^* = x \oplus 54$  (since  $a = 54$ ).

## The principle of differential cryptanalysis illustrated on a DES S-box [2]

Now, perform a one round analysis on DES. Recall that the DES round function is given by

$$f(D, K) = P \circ S(E(D) \oplus K)$$

Observe that we have the following linear relations :

$$E(D \oplus D^*) = E(D) \oplus E(D^*) \quad (0.2)$$

$$(E(D) \oplus K) \oplus (E(D^*) \oplus K) = E(D) \oplus E(D^*) \quad (0.3)$$

$$P(C \oplus C^*) = P(C) \oplus P(C^*) \quad (0.4)$$

$$\text{Ditto for } P^{-1} \quad (0.5)$$

# The principle of differential cryptanalysis illustrated on a DES S-box [3]

## How to find the possible keys?

Reminder :  $f(D, K) = P \circ S(E(D) \oplus K)$ .

Working from a pair  $(D, D^*)$  with expansion image  $(E, E^*)$  and setting :

$$F = f(D, K); F^* = f(D^*, K); C = P^{-1}(F); C^* = P^{-1}(F^*)$$

The XOR  $C'$  and  $E'$  concatenates 8 strings  $C'_j$  and  $E'_j$  related to the different S-boxes. Thus, for the S-box  $S_j$  :

$$B_j := E_j \oplus K_j \in \Delta_j(E'_j, C'_j).$$

We then deduce that

$$K_j \in E_j \oplus \Delta_j(E'_j, C'_j) = \{E_j \oplus x; x \in \Delta_j(E'_j, C'_j)\}. \quad (0.6)$$

We set  $\text{Test}_j(E_j, E_j^*, C'_j) := E_j \oplus \Delta_j(E'_j, C'_j)$ .



## The principle of differential cryptanalysis illustrated on a DES S-box [4]

Let's illustrate it with a concrete "toy example" : For the first box, we have found

$$\Delta_1(54, 1) = \{4, 7, 12, 49, 50, 58\} . \quad (0.7)$$

and therefore if  $E_1 = 5 = 101$ ,  $E'_1 = 0 \times 36 = 110110$ ,  $E_1^* = 110011$ ,  
and  $C'_1 = 1$   $K_j \in 5 + \{4, 7, 12, 49, 50, 58\}$   
 $= 101 + \{100, 111, 1100, 110001, 110010, 111010\}$   
 $= \{1, 10, 1001, 110100, 110111, 111111\}$   
 $= \{1, 2, 9, 52, 55, 63\}.$

$4 = 100$ ;  $7 = 111$ ;  $12 = 1100$ ;  $49 = 32 + 16 + 1 = 110001$ ;  $50 =$   
 $32 + 16 + 2 = 110010$ ;  $58 = 32 + 16 + 8 + 2 = 111010$

## Revisiting differential cryptanalysis (after Biham and Shamir) [5]

We want to emphasise on the usual design principles of the DES S-boxes (it is known as the "strict avalanche criterion") :

- No S-box is a linear or affine function of its input.
- Changing one input bit to an S-box results in changing *at least* two output bits.
- $S(X)$  and  $S(X \oplus 001100)$  must differ in *at least* two bits.
- $S(X) \neq S(X \oplus 11b_2b_300)$  for any choice of  $b_2$  and  $b_3$ .
- The S-boxes were chosen to minimise the differences between the number of 1's and 0's in any S-box output when any single bit is held constant.

## Revisiting differential cryptanalysis (after Biham and Shamir) [6]

In DES any S-box has  $4096 = 64 \times 64$  possible input pairs, and each one of them has an input XOR and an output XOR. There are only  $1024 = 64 \times 16$  possible tuples of input and output XORs. Therefore, each tuple results in average from four pairs. However, not all the tuples exist as a result of a pair, and the existing ones do not have a uniform distribution. Very important properties of the S-boxes are derived from the analysis of the tables that summarise this distribution.

**Definition (Biham/Shamir) :** A table that shows the distribution of the input XORs and output XORs of all the possible pairs of an S-box is called *the pairs XOR distribution table of the S-box*. The entries count the number of possible pairs with such an input XOR and an output XOR.

For simplicity, we will call such table a **differential distribution table**.

## Revisiting differential cryptanalysis (after Biham and Shamir) [7]

**Definition (Biham/Shamir) :** Let  $X$  be a six bit value and  $Y$  be a four bit value. We say that  $X$  *may cause*  $Y$  *by an S-box* if there is a pair in which the input XOR of the S-box equals  $X$  and the output XOR of the S-box equals  $Y$ . If there is such a pair we write  $X \rightarrow Y$  (or even  $X \rightarrow_S Y$ , if we want to emphasise the S-box), and if there is no such pair we say that  $X$  *may not cause*  $Y$  *by the S-box* and write  $X \nrightarrow Y$  (or  $X \nrightarrow_S Y$ ).

**Example :** Consider the input XOR 32 of  $S_8$ . It has only five possible output XORs. The possible output XORs are : 2, 4, 6, 14, 16. Therefore, the input XOR 32 for  $S_8$  may cause output XOR 2 ( $32 \rightarrow_{S_8} 2$ ), also  $32 \rightarrow_{S_8} 4$ , but  $32 \nrightarrow_{S_8} 9$ .

☞ Analysis of the tables demonstrate that for a fixed input XOR, the possible output XORs do not have a uniform distribution.

**Exercise :** Are the following claims true?  $33 \rightarrow_{S_5} 1$ ,  $34 \rightarrow_{S_6} 2$ ,  $2 \rightarrow_{S_2} 8$ ,  $52 \rightarrow_{S_1} 1$ ,  $54 \nrightarrow_{S_3} 7$ .

## Revisiting differential cryptanalysis (after Biham and Shamir) [8]

**Defintion (Biham/Shamir) :** We say that  $X$  may cause  $Y$  with probability  $p$  by an S-box if for a fraction  $p$  of the pairs in which the input XOR of the S-box equals  $X$ , the output XOR equals  $Y$ .

**Example :**  $52 \rightarrow_{S_1} 2$  results from 16 out of the 64 pairs, so with probability  $\frac{1}{4}$ , while  $52 \rightarrow_{S_1} 4$  results only from two out of 64 pairs, thus with probability  $\frac{1}{32}$ .

Different distributions appear in different lines of the table. In total between 70% and 80% of the entries are possible and between 20% and 30% are impossible. The exact percentage for each S-box is shown in the following table :

$S_1$	$S_2$	$S_3$	$S_4$	$S_5$	$S_6$	$S_7$	$S_8$
79.4	78.6	79.6	68.5	76.5	80.4	77.2	77.1

## Revisiting differential cryptanalysis (after Biham and Shamir) [9]

The pairs XOR distribution tables let us find the possible input and output values of pairs given their input and output XORs. The following example shows a simple case :

**Example :** Consider the entry  $52 \rightarrow_{S_1} 4$  in the pairs XOR distribution table of  $S_1$ . Since the entry  $52 \rightarrow_{S_1} 4$  has value 2, only two pairs satisfy these XORs. These pairs are duals. If the first pair is  $X_I, X_I^*$  then the other pair is  $X_I^*, X_I$ . By looking at the following table, we see that these inputs must be 19 and 39 whose corresponding outputs are 6 and 2 respectively (check it!).

Output XOR ( $X'_O$ )	Possible inputs ( $X_I$ )
1	03, 0F, 1E, 1F, 2A, 2B, 37, 3B
2	04, 05, 0E, 11, 12, 14, 1A, 1B, 20, 25, 26, 2E, 2F, 30, 31, 3A
3	01, 02, 15, 21, 35, 36
4	13, 27
7	00, 08, 0D, 17, 18, 1D, 23, 29, 2C, 34, 39, 3C
8	09, 0C, 19, 2D, 38, 3D
D	06, 10, 16, 1C, 22, 24, 28, 32
F	07, 0A, 0B, 33, 3E, 3F

(values are in hexadecimal)

## Revisiting differential cryptanalysis (after Biham and Shamir) [10]

Next we show how to find the key bits using known input pairs and output XOR of an S-box in the  $F$  function.

Again consider  $S_1$  and assume that the input pair is  $X_E = 1$  and  $X_E^* = 53 = x35$  (note that  $xNN$  means that  $NN$  is given in hexadecimal) and the value of the corresponding six key bits is  $X_K = 35 = x23$ . Then the actual inputs of  $S_1$  (after XORing the input and key bits) are  $X_I = 34 = x22$ ,  $X_I^* = 22 = x16$  and the outputs are  $X_O = 1$  and  $X_O^* = 12 = xC$ . The output XOR is  $X'_O = 13 = xD$ .

## Revisiting differential cryptanalysis (after Biham and Shamir) [11]

Assume we know that  $X_E = 1$ ,  $X_E^* = x35$ ,  $X_O' = xD$  and we want to find the key value  $K_1$  (subkey at the level of  $S_1$ ). The input XOR is  $X_E' = X_I' = x34$  regardless of the actual value of  $K_1$ . By consulting the distribution table of  $S_1$  we can see that the input to the S-box has eight possibilities. These eight possibilities make eight possibilities for the key (by “Key value = Expansion  $\oplus$  Input”) as described in the following table.

S-box input	Possible Keys
06, 32	07, 33
10, 24	11, 25
16, 22	17, 23
1C, 28	1D, 29

(values are in hexadecimal)

Each line in the table describes two pairs with the same two inputs but with the opposite order. Each pair leads to one key, so each line leads to two keys (which are  $S_E \oplus S_I$  and  $S_E^* \oplus S_I^*$ ). The right key value  $K_1$  must occur in this table.



## Revisiting differential cryptanalysis (after Biham and Shamir) [12]

Using additional pairs we can get additional candidates for  $K_1$

Lets look at the input pair  $X_E = x_{21} = 33$ ,  $X_E^* = x_{15} = 21$  (with the same  $S1_K = x_{23} = 34$ , where  $S1$  denote the first S-box). The inputs to the S-box are  $S1_I = 2$ ,  $S1_I^* = x_{36} = 58$  and the outputs are  $S1_O = 4$ ,  $S1_O^* = 7$ . The output XOR is  $S1'_O = 3$ . The possible inputs to the S-box where  $x_{34} \rightarrow 3$  (i.e.,  $S1'_I \rightarrow S1'_O$ ) and the corresponding possible keys are described in the table below :

S-box input	Possible Keys
01, 35	03, 37
02, 36	00, 34
15, 21	17, 23

(values are in hexadecimal)

## Revisiting differential cryptanalysis (after Biham and Shamir) [13]

The expected key must occur in both tables.

The only common key values in both tables are  $x_{17}$  and  $x_{23}$ . These two values are indistinguishable with this input XOR since  $x_{17} \oplus x_{23} = x_{34} = S1'_E$ , but may become distinguishable by using a pair with a different input XOR value ( $S1'_E \neq x_{34}$ ).

## Revisiting differential cryptanalysis (after Biham and Shamir) [14]

In order to extend the previous analysis to  $r$  rounds, we need to extend the definition :

**Definition (Biham/Shamir)** : Let  $X$  and  $Y$  be 32 bit values. We say that  $X$  may cause  $Y$  with probability  $p$  by the  $F$  function (or  $F_r$ ) if for a fraction  $p$  of all the possible input pairs encrypted by all the possible subkey values in which the input XOR of the  $F$  function equals  $X$ , the output XOR equals  $Y$ . If  $p > 0$  we denote this possibility by  $X \rightarrow Y$  (or even  $X \rightarrow_F Y$ ).

## Revisiting differential cryptanalysis (after Biham and Shamir) [15]

We have the following result :

**Property :** In DES, if  $X \rightarrow Y$  with probability  $p$  by the  $F$  function then every fixed input pair  $Z, Z^*$  with  $Z' = Z \oplus Z^* = X$  causes the  $F$  function output XOR to be  $Y$  by the same fraction  $p$  of the possible subkey values.

**Remark :** In other block ciphers this property does not necessarily hold.

**Corollary :** The probability  $p$  of  $X \rightarrow_F Y$  is the product of  $p_i$  in which  $X_i \rightarrow_{S_i} Y_i$  for the S-box  $S_i, i \in \{1, \dots, 8\}$ , where  $X_1 X_2 X_3 X_4 X_5 X_6 X_7 X_8 = E(X)$  and  $Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7 Y_8 = P^{-1}(Y)$ .

## Towards the differential cryptanalysis of $F$

The above discussion about finding the key bits entering S-boxes can be extended to find the subkeys entering the  $F$  function. The method is as follows :

- 1 Choose an appropriate plaintext XOR.
- 2 Create an appropriate number of plaintext pairs with the chosen plaintext XOR, encrypt them and keep only the resultant ciphertext pairs.
- 3 For each pair derive the expected output XOR of as many S-boxes in the last round as possible from the plaintext XOR and the ciphertext pair. (Note that the input pair of the last round is known since it appears as part of the ciphertext pair).
- 4 For each possible key value, count the number of pairs that result with the expected output XOR using this key value in the last round.
- 5 The right key value is the (hopefully unique) key value *suggested* by all the pairs.

### 3 rounds DES attack

Let us consider a subset of the whole DES scheme with only three Feistel rounds and no initial (or final) permutation  $IP$ .

Given a pair of inputs  $(G_0, D_0)$  and  $(G_0^*, D_0^*)$ , one sets  $D'_i = D_i \oplus D_i^*$  (respectively  $G'_i = G_i \oplus G_i^*$ ) for  $i=0,1,2,3$ .

Then, taking  $D_0^* = D_0$ , one has :

$$D'_3 \oplus G'_0 = f(G_3, K_3) \oplus f(G_3^*, K_3) \quad (1)$$

Since  $f(D, K) = P \circ S(E(D) \oplus K)$ , one sets  $C' = P^{-1}(G'_0 \oplus D'_3)$ ,  $E = E(G_3)$  and  $E^* = E(G_3^*)$ . Therefore, equation (1) becomes :

$$C' = P^{-1}(G'_0 \oplus D'_3) = S(E \oplus K_3) \oplus S(E^* \oplus K_3)$$

or

$$C' = S(E \oplus K_3) \oplus S((E \oplus K_3) \oplus E')$$

Thus,  $E_j \oplus (K_3)_j \in \Delta_j(E'_j, C'_j)$  (for all  $j \in \{1, ..8\}$ ).

One knows the value of  $E$ ,  $E'$  and  $C'$ . Hence, it is possible to recover  $K_3$ .

## 3 rounds DES attack (continued)

Why the equation (1)?

For  $i = 0, 1, 2$  we have :  $G_{i+1} = D_i$  ;  $D_{i+1} = G_i \oplus f(D_i, K_{i+1})$ .

Performing the DES scheme on the first 3 rounds, we get :

$$D_3 = G_2 \oplus f(D_2, K_3) \quad (0.8)$$

$$= D_1 \oplus f(D_2, K_3) \quad (0.9)$$

$$= G_0 \oplus f(D_0, K_1) \oplus f(D_2, K_3) \quad (0.10)$$

$$= G_0 \oplus f(D_0, K_1) \oplus f(G_3, K_3) \quad (0.11)$$

Ditto with  $(G_0^*, D_0^*)$ . Now, perform XOR operations on the two equalities :

$$D'_3 = G'_0 \oplus f(D_0, K_1) \oplus f(D_0^*, K_1) \oplus f(G_3, K_3) \oplus f(G_3^*, K_3) \quad (0.12)$$

### 3 rounds DES attack (continued)

If you choose  $D_0 = D_0^*$  this is simplified as

$$D'_3 = G'_0 \oplus f(G_3, K_3) \oplus f(G_3^*, K_3) \quad (0.13)$$

$$f(D_2, K_3) \oplus f(D_2^*, K_3) = G'_0 \oplus D'_3 \quad (0.14)$$

If you observe that you know  $G'_0$  and  $D'_3$ , we can set :

$$C' = P^{-1}(G'_0 \oplus D'_3); E = E(G_3); E^* = E(G_3^*) \quad (0.15)$$

and you break everything into 8 pieces. Then, as in (0.6)

$$K_j \in \text{Test}_j(E_j, E_j^*, C'_j) \text{ for } j = 1, \dots, 8 \quad (0.16)$$



### 3 rounds DES attack (continued)

Hence, for one chosen pair (we will use in fact 3 pairs), namely  $[(G_0, D_0), (G_3, D_3)], [(G_0^*, D_0^*), (G_3^*, D_3^*)]$ , *assuming*  $D_0 = D_0^*$ , the algorithm is :

- ①  $D'_3 \leftarrow D_3 \oplus D_3^*, G'_0 \leftarrow G_0 \oplus G_0^*$
- ②  $C' \leftarrow P^{-1}(D'_3 \oplus G'_0)$
- ③  $E \leftarrow E(G_3), E^* \leftarrow E(G_3^*)$
- ④ For  $j = 1$  to 8, compute  $\text{Test}_j(E_j, E_j^*, C'_j)$

In order to compute the intersection of the sets  $\text{Test}_j(E_j, E_j^*, C'_j)$ , we proceed as follows : If  $K$  is subkey  $K_3$ . For each  $K_j$ , at the level of the box  $S_j$ , we have 64 possible values (say from 0 to 63). We put them in a table  $T[j]$  (initialise to 0). Each time the value  $a$  appears we perform  $T[j][a] \leftarrow T[j][a] + 1$ . You notice that each table only contains zeros, 1s and a single 3 : the value of  $a$  giving this 3 provides 6 bits from the third subkey. Then using the key schedule, we can recover 48 bits of the initial key.

**Question :** what would happen if instead of 3 pairs, we used  $s$  pairs, with  $s > 3$ ?

### 3 rounds DES attack (continued)

(see Stinson, french 1st edition, p. 87-89) : We can illustrate the previous algorithm with the following example :

Plaintext pair  $0x748502CD38451097$  ,  $0x3874756438451097$

their ciphertext  $0x03C70306D8A09F10$  ,  $0x78560A0960E6D4C8$

giving  $E = 0x007E0E80680C$ ,  $E^* = 0xBF02AC054052$ ,

$C' = 0x965B5116$

For the first box you find

$$\Delta_1(E'_1, C'_1) = \{000000, 00011, 101000, 101111\}$$

$$K_1 \in \text{Test}_1(0, 101111, 1001)$$

$$= \{000000, 00011, 101000, 101111\}$$

$$= \{0, 7, 40, 47\}$$

Therefore  $T_1[a] = 1$  for  $a = 0, 7, 40$  and  $47$  and  $T_1[a] = 0$  otherwise.

## 2 rounds DES Attack

It is an easier copy of the 3 rounds attack. We ignore  $IP$ . For  $i = 0, 1$   $G_{i+1} = D_i$  ;  $D_{i+1} = G_i \oplus f(D_i, K_{i+1})$

$$D_2 = G_1 \oplus f(D_1, K_2) \quad (0.17)$$

$$= D_0 \oplus f(D_1, K_2) \quad (0.18)$$

$$= D_0 \oplus f(G_2, K_2) \quad (0.19)$$

Ditto for  $(G_0^*, D_0^*)$  ; xoring the two equalities :

$$D_2' = D_0' \oplus f(G_2, K_2) \oplus f(G_2^*, K_2) \quad (0.20)$$

## 2 rounds DES Attack (continued)

Using the knowledge of  $D'_0$  and  $D'_2$  we compute :

$$C' = P^{-1}(D'_0 \oplus D'_2); E = E(G_2); E^* = E(G_2^*) \quad (0.21)$$

and you break everything into 8 pieces. Then, as in 3 rounds DES Attack :

$$K_j \in \text{Test}_j(E_j, E_j^*, C'_j) \text{ for } j = 1, \dots, 8 \quad (0.22)$$

Therefore one gets the subkey of the 2nd round or 48 out of the 56 bits of the key  $K$  and obtains the remaining 8 bits by a fast exhaustive research.

## Going beyond 3 rounds : The notion of characteristic

We are left with the problem of pushing the knowledge of the XORs of the plaintext pairs as many rounds as possible without making them all zeroes.

☞ When the XORs of the pairs are zero, i.e., both texts are equal, the outputs are equal too, which makes all the keys equally likely.

The pushing mechanism is a *statistical characteristic* of the cryptosystem which is an extension of the single round analysis that we have seen.

## Formal definition of the characteristic [1]

A  $r$ -round characteristic is a  $r + 2$ -tuple of  $m$  bit blocks

$\Omega_P = \Omega_0, \Omega_1, \dots, \Omega_r, \Omega_{r+1} = \Omega_T$ , with  $\Omega_i = (\lambda_I^i, \lambda_O^i)$ ,  $i = 1, \dots, r$  verifying the following properties :

- $\lambda_I^1 = \text{right half of } \Omega_P$ .
- $\lambda_I^2 = (\text{left half of } \Omega_P) \oplus \lambda_O^1$ .
- $\lambda_I^r = \text{left half of } \Omega_T$ .
- $\lambda_I^{r-1} = (\text{right half of } \Omega_T) \oplus \lambda_O^r$ .
- $\lambda_O^i = \lambda_I^{i-1} \oplus \lambda_I^{i+1}$ , with  $2 \leq i \leq r - 1$ . Thus we also have  $\lambda_I^{i+1} = \lambda_I^{i-1} \oplus \lambda_O^i$

where  $m$  is the block size of the cipher (for DES  $m = 64$ ).  $\Omega_P$  represents the plaintexts XOR of the characteristic and  $\Omega_T$  its ciphertexts XOR.

## Formal definition of the characteristic [2]

More concrete within the DES framework :

**Input** : a pair of plaintexts  $(L_0, R_0)$   $(L_0^*, R_0^*)$ , a fixed key

**Output** : values of  $f$  in the  $i$  th round

$$F_i = f(R_{i-1}, K_i), F_i^* = f(R_{i-1}^*, K_i)$$

$$\text{XOR : } F'_i = F_i \oplus F_i^*, R'_{i-1} = R_{i-1} \oplus R_{i-1}^*$$

$$\text{Recursion formula : } R_i = L_{i-1} \oplus F_i = R_{i-2} \oplus F_i$$

$$\text{therefore } R'_i = R'_{i-2} \oplus F'_i$$

$$\text{Setting } \Omega_i = (R'_{i-1}, F'_i), i = 1, \dots, r$$

$$\text{we get } \Omega_0, \Omega_1, \dots, \Omega_r, \Omega_{r+1} = (L_r, R_r)$$

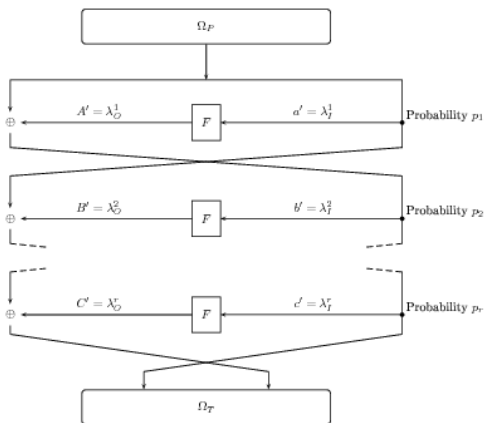
that is a characteristic as axiomatized in the previous definition. We

have  $L'_i = R'_{i-1}$  for  $i = 1, \dots, r$ . Furthermore, we often denote by

$p_i$  the probability to have  $L'_i = L_i \oplus L_i^*$  and  $R'_i = R_i \oplus R_i^*$ . The probability of the characteristic is then the product

$$p = p_1 \times \dots \times p_r.$$

# Picture of a general characteristic



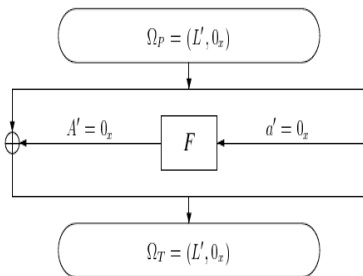


## What is a characteristic ?

Associated with any pair of encryptions are the XOR value of its two plaintexts, the XOR of its ciphertexts, the XORs of the inputs of each round in the two executions and the XORs of the outputs of each round in the two executions.

These XOR values form an  $n$ -round characteristic. A characteristic has a probability, which is the probability that a random pair with the chosen plaintext XOR has the round and ciphertext XORs specified in the characteristic. In other words ; if a pair of plaintext is chosen carefully with a given XOR value, the characteristic allows us to study the probabilistic behavior of the evolution of this XOR value during the encryption.

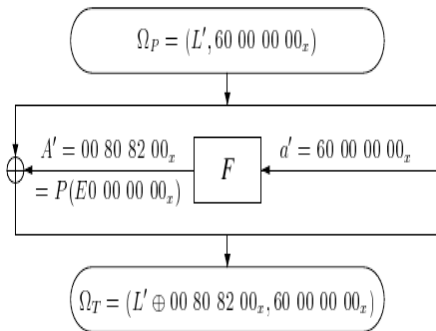
## Examples of characteristics [1]



A one round characteristic with probability 1 (for any  $L'$ )

The above example describes a one-round characteristic with probability 1 ( $F$  is the DES function). This is the only one-round characteristic with probability greater than  $\frac{1}{4}$ . This characteristic is very useful in practice. We have  $L'_0 = L' = \text{anything}$ ,  $R'_0 = 0$  and  $L'_1 = 0$  and  $R'_1 = L'_0$ . Thus the probability is indeed 1.

## Examples of characteristics [2]



A one round characteristic with probability  $\frac{14}{64}$  (for any  $L'$ )

Here we have  $L'_0 = L'$ ,  $R'_0 = 60000000_x$ ,  $L'_1 = R'_0$  and  $R'_1 = L' \oplus 00808200_x$  with probability  $p = 14/64$ .

## Comments on this one round characteristic

The XOR value of the expansion function w.r.t  $R_0$  and  $R_0^*$  (i.e.,  $E(R_0')$ ) is  $001100 \cdots 0$ . Thus the XOR input on  $S_1$  is  $001100$  and  $0$  on the other S-boxes. The corresponding output XOR for  $S_1$  is  $1110$  with probability  $14/64$  (because  $\delta_1(001100, 1110) = 14$ ). We then get

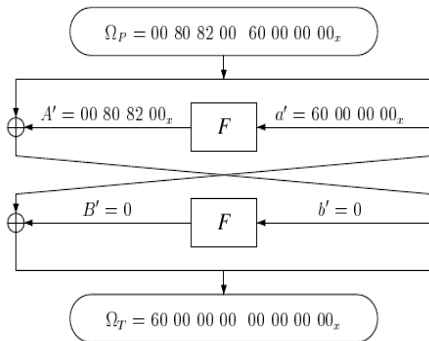
$$C' = 1110 \cdots 0.$$

Applying  $P$  we get

$$P(C') = 00000000100000000100000010 \cdots 0 = 00808200_x.$$

The idea behind this characteristic, was to put 7 input XOR of S-boxes to 0 and the remaining is chosen in order to maximize the probability that the input XOR may cause the output XOR. The choice of  $S_1$  is mainly driven by the behavior of the expansion function.

## Examples of characteristics [3]



A two round characteristic with probability  $\frac{14}{64}$

This characteristic is built from the previous one-round characteristics. **Exercise** : give an example of one-round characteristics with probability  $\frac{1}{4}$  (hint : use non zero input XOR in  $S_2$  or  $S_6$ ).

## Composing characteristics

We start with two characteristics as previously seen :

$$\Omega_P^1 = \Omega_0^1, \Omega_1^1, \dots, \Omega_r^1, \Omega_{r+1}^1 = \Omega_T^1,$$

$$\Omega_P^2 = \Omega_0^2, \Omega_1^2, \dots, \Omega_r^2, \Omega_{s+1}^2 = \Omega_T^2$$

$$\text{Condition : } \Omega_T^1 = \Omega_P^2$$

The  $r + s$  round composite is :

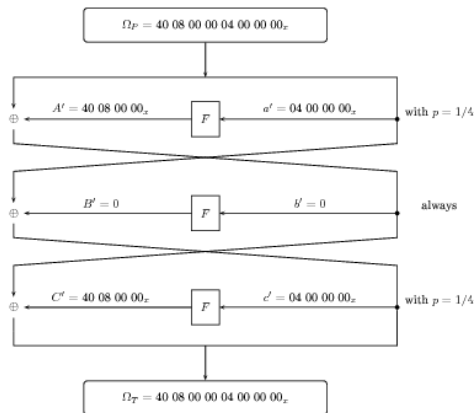
$$\Omega_P = \Omega_0^1, \Omega_1^1, \dots, \Omega_r^1, \Omega_1^2, \dots, \Omega_r^2, \Omega_{s+1}^2 = \Omega_T$$

We may use two copies of one characteristic in the case where

$$\Omega_P = \Omega_T$$

and therefore go further with several copies of the same characteristic.

First 3 rounds characteristic with probability  $\frac{1}{16}$



## Explanation

The picture summarizes the situation with  $\Omega_P = (G'_0, D'_0)$  as XOR of a pair of plaintexts.

In each round we have the XOR of inputs and the XOR of outputs of the function  $F$  with its probability displayed on the right.

The XOR of the outputs is  $\Omega_T = (G'_3, D'_3)$



## Attack on the 3 last rounds

We use the characteristic for the 3 first rounds and we use the 3 round method for the 3 last rounds, but with  $\Omega_T$  replacing the XOR of plaintexts :

$$D'_6 = G'_3 \oplus f(D_3, K_4) \oplus f(D_3^*, K_4) \oplus f(D_5, K_6) \oplus f(D_5^*, K_6) \quad (0.23)$$

It is exactly (0.12) but 3 rounds below. As  $D'_3 = 40080000_x = 0100\ 0000\ 0000\ 1000 \dots \xrightarrow{E} 001000\ 000000\ 000001\ 01000 \dots$ , the inputs of the boxes  $S_i$  are the same for  $i \neq 1, 3$  or 4 for the two elements of a pair so the corresponding bits of  $f(D_3, K_4) \oplus f(D_3^*, K_4)$  are 0.

We are in the situation of the the 3 rounds attack but only for the 30 bits of 5 boxes.

Instead of  $(G'_0)$  as in (0.12) we have now  $G'_3$  from the characteristic.

## from 3 to 6 rounds

- We use the previous method for the last 3 rounds
- We push the knowledge of the plaintext XOR to a knowledge of an intermediate XOR after 3 rounds
- The tool for that is the **characteristic**.

## Algorithm for the partial recovering of the 6 th round key

One needs around one hundred pairs with prescribed XOR  $\Omega_T$  and computes the corresponding sets  $Test_j(E_j, E_j^*, C'_j)$  with

$$C' = P^{-1}(G'_3 \oplus D'_6); E = E(G_6); E^* = E(G_6^*) \quad (0.24)$$

Here  $G'_6$  et  $D'_6$  are known as the XOR of the outputs.  $G'_3$  is just the value given by the characteristic and is the true  $G'_3$  with relatively large probability

## Good pairs

- The key  $K$  is fixed, and we take a characteristic.
- A pair of plaintexts is **good** (or **right**) if the sequence  $\Omega_i = (R'_{i-1}, F'_i)$ ,  $i = 1, \dots, r$ ,  $\Omega_T$ , computed with  $K$ , is the sequence of XOR described in the characteristic and **bad** (or **wrong**) otherwise.
- The good pairs are frequent enough among a random set of pairs (for example 1/6).
- The bad pairs spread randomly.
- We record the suggested keys (as seen in SAC lectures).

## Schedule of the Algorithm

- The sets  $Test_j$  suggest pieces of  $K_6$  :
- every good pair suggest the good key  
the bad ones have a random behaviour so that the key  $K_6$  (or the 30 bits we want to recover) pop out eventually.
- We may proceed as in the DES restricted to 3 rounds and look for the 5 pieces of 6 bits independently.
- a better method is to manage the 5 boxes together in order to use more efficiently the good pairs : see below the definition of **cliques...**

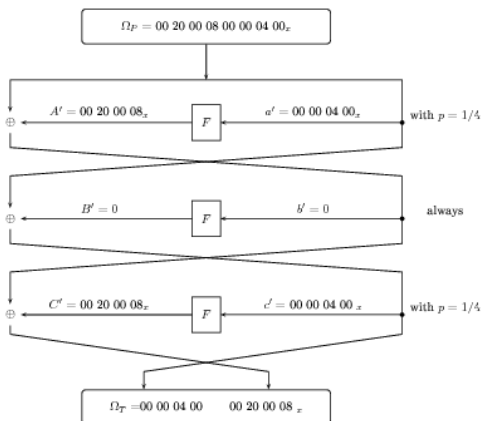
## Finishing the attack

We end by an exhaustive search on 26 missing bits or faster :

We may use a second characteristic for guessing another set of 30 bits, which has only 12 bits not already obtained. Therefore we obtain 42 bits and the exhaustive search need only to find 14 bits.

Quartet :  $P, P \oplus \Psi_1, P \oplus \Psi_2, P \oplus \Psi_1 \oplus \Psi_2$  = tool to use pairs for the two characteristics (parallelogram property).

## Second 3 rounds characteristic



## 3-R Attacks

Counter  $T_j = 64$  entry array corresponding to the allowable values of the  $j$  th piece of the round key  $K_r$ .

For each value  $a$ , one stores in  $T_j[a]$  the list of pairs suggesting  $a$ .

**Clique** : it is a set of pairs  $\cap_j T_j[a_j]$ , for  $j \in \{2, 5, 6, 7, 8\}$ , and various  $a_j$  .

The largest clique gives the piece of key.



## 2-R DES Attacks

A 2-R attack apply the method of the 2 rounds attack for the last two rounds. The input is now the output XOR of a  $(r - 2)$  round characteristic.

## iterative characteristic

iterative characteristic

= characteristic one can repeat.

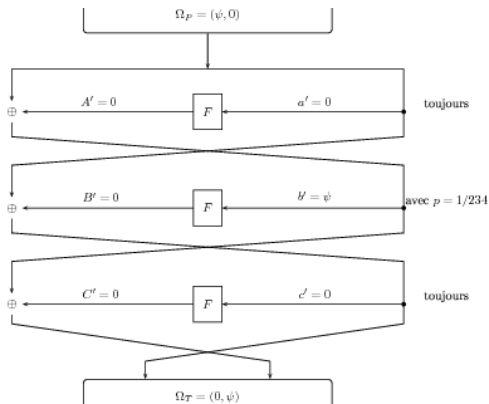
Here are the main 3 examples in 2 rounds, according to the formula :  $\Omega_0 = (\Psi, 0), \Omega_1 = (0, 0), \Omega_2 = (\Psi, 0) = \Omega_T$  .

for  $\Psi = 19\ 60\ 00\ 00$ ,  $p = 14 \times 8 \times 10/64^3 \simeq 1/234$ .

for  $\Psi = 1B\ 60\ 00\ 00$ ,  $p = 14 \times 8 \times 10/64^3 \simeq 1/234$ , and

for  $\Psi = 00\ 19\ 60\ 00$ ,  $p = 1/256$ .

## 2 round characteristics, embedded in a 3 round characteristics



## Summary of the 6 rounds attack

Let us consider the first characteristic :

*Input* :  $\Omega_P = 0x40\ 08\ 00\ 00\ 04\ 00\ 00\ 00$

*Output* :  $\Omega_T = 0x04\ 00\ 00\ 00\ 40\ 08\ 00\ 00$  (*with probability 1/16*)

We should generate enough couples of inputs

$((G_0, D_0), (G_0^*, D_0^*) = (G_0, D_0) \oplus \Omega_P)$  (between 100 and 200, we should look for the smallest set of couples).

With probability 1/16, one has  $(G_3, D_3) \oplus (G_3^*, D_3^*) = \Omega_T$ .

We set  $\Omega_P = (\Omega_P^{(1)}, \Omega_P^{(2)})$  and  $\Omega_T = (\Omega_T^{(1)}, \Omega_T^{(2)})$ .

Then, we perform the previous attack on the last 3 rounds. Namely

$$D'_6 \oplus \Omega_T^{(1)} = f(G_3, K_4) \oplus f(G_3^*, K_4) \oplus f(D_5, K_6) \oplus f(D_5^*, K_6) \quad (2)$$

One sets  $C' = P^{-1}(\Omega_T^{(1)} \oplus D'_6)$ ,  $E = E(G_6)$  and  $E^* = E(G_6^*)$ .

## The 6 rounds attack (continued)

Equation (2) can be written as follows :

$$C' = S(E(D_3) \oplus K_4) \oplus S(E(D_3^*) \oplus K_4) \oplus S(E \oplus K_6) \oplus S(E^* \oplus K_6) \quad (3)$$

If we still assume that the couple is following the first characteristic, then  $E(D_3) \oplus E(D_3^*) = E(\Omega_T^{(2)}) =$   
0x08 0x00 0x01 0x10 0x00 0x00 0x00 0x00.

Hence, for  $j \in \{2, 5, 6, 7, 8\}$ , one has  $E(G_3)_j = E(G_3^*)_j$  and

$$C'_j = S(E_j \oplus (K_6)_j) \oplus S(E_j^* \oplus (K_6)_j) \quad (4)$$

Therefore, with respect to what we have seen for the 3-rounds attack :

$$E_j \oplus (K_6)_j \in \Delta_j(E'_j, C'_j) \text{ for } j = 2, 5, 6, 7, 8$$

Thus one should be able to recover part of the subkey  $K_6$ .

## The 6 rounds attack (continued)

However, the use of the first characteristic is not enough to compute efficiently the attack since there are still 26 bits to recover by brute force (well, this can be done easily in few minutes with 64 cpus).

One should use a second characteristic instead, namely

$$\text{Input} : \Omega_P = 0x00\ 20\ 00\ 08\ 00\ 00\ 04\ 00$$

$$\text{Output} : \Omega_T = 0x00\ 00\ 04\ 00\ 00\ 20\ 00\ 08 \text{ (with probability } 1/16)$$

As an exercise, you can write the formulae for this characteristic.

We have

$$E(\Omega_T^{(2)}) = 0x00\ 0x00\ 0x04\ 0x00\ 0x00\ 0x00\ 0x01\ 0x10$$

. Hence, for  $j \in \{1, 2, 4, 5, 6\}$ , one has  $E(G_3)_j = E(G_3^*)_j$  and

$$C'_j = S(E_j \oplus (K_6)_j) \oplus S(E_j^* \oplus (K_6)_j) \quad (5)$$

Eventually, with this second characteristic, only  $(K_6)_3$  remains unknown and there are only 8 bits to brute force.

## Probabilities for characteristics

Round  $i$  of a characteristic has probability  $p_i^\Omega$  if  $\lambda_I^i \rightarrow_F \lambda_O^i$  with probability  $p_i^\Omega$ .

An  $n$ -round characteristic has probability  $p^\Omega$  if  $p^\Omega$  is the product of the probabilities of its  $n$  rounds :

$$p^\Omega = \prod_{i=1}^n p_i^\Omega .$$

**Theorem :** The formally defined probability of a characteristic  $\Omega = (\Omega_P, \Omega_A, \Omega_T)$  is the actual probability that any fixed plaintext pair satisfying  $P' = \Omega_P$  is a right pair when random independent keys are used.

## Remarks on good/bad pairs

- For 6 rounds, a characteristic gives 30 bits of the key : compare  $1/6$  to  $2^{-30}$
- We need a number of pairs in inverse ratio of the probability of the characteristic
- One can **filter** pairs by ignoring the ones giving at least one empty set
- The ratio of (independent) subkeys for which a pair  $(L_0, R_0)$  and  $(L_0^*, R_0^*)$  with XOR  $\Omega_P$  is good is equal to the probability of the characteristic.

If  $E_j$  and  $E_j^*$  are six bits and  $C_j'$  4 bits, we define

$$\text{Test}_j(E_j, E_j^*, C_j') := E_j \oplus \delta_j(E_j', C_j')$$

where  $E_j' = E_j \oplus E_j^*$ . If  $\text{Test}_j(E_j, E_j^*, C_j') = \emptyset$  for a given pair ( $E$  output from expansion,  $C'$  output of the inverse permutation of the last round), then it is a bad pair.



## Counting

We fix a characteristic  $\Omega$  with probability  $p$ .

We take a set of  $m$  pairs and wish to guess  $k$  bits of the key via the bits of a round subkey

The number of good pairs is  $mp$  and always suggest the good key.

The signal is then at least  $mp$

Note we need  $m > 1/p$  just to have  $mp > 1$ . Unfortunately, if the ratio signal/noise is small, we should take  $m$  even larger. We shall now compute that ratio.

## Signal/Noise ratio

- $\alpha$  = mean value of the number of suggested keys by a filtered pair
- $\beta$  = the ratio of filtered pair
- So we get  $m\alpha\beta$  suggested parts of key. If the part are  $k$  bits long, this parts are dispatched in  $2^k$  counters ; so the mean value of the noise is  $m\alpha\beta/2^k$ .
- The right key is counted about  $mp$  times, from the good pairs in proportion  $p$  (the probability of the characteristic)
- Therefore we find a ratio

$$S/N = \frac{2^k p}{\alpha\beta}$$

## Example

For the 6 round DES we see that  $k = 30$  bits, and that the probability of the characteristics is  $1/16$ .

Suppose we use  $b = 5$  boxes : the mean value for the distribution tables is 4. So we get  $4^b$  suggested parts of key.

$$S/N = \frac{2^{30} \times (1/16)}{4^5} = 2^{30-4-10} = 2^{-16}$$

## Table of results

The following table gives according to the round number the number of plaintexts to be chosen or analysed and the complexity (=number of necessary encryptions) from Biham/Shamir (1992); All the numbers displayed are **exponents** for numbers which are powers of 2.

rounds	Chosen Plaintexts	Analysed Plaintexts	Complexity	Time	Space
8	14	2	9	16	24
9	24	1	32	26	30
10	24	14	15	35	-
11	31	1	32	36	-
12	31	21	21	43	-
13	39	1	32	44	30
14	39	29	29	51	-
15	47	7	37	52	42
16	47	36	37	58	-

# Linear cryptanalysis of DES

This attack of DES (plaintext attack) was introduced by Matsui in 1993/94 using the linear approximations of the boxes seen in SAC. Its practical implementation uses the last round function.

☞ In the following we will set  $NL_i(a, b) = \lambda_{S_i}(a, b)$ .

## Matsui's strategy

for a block  $A$  of bits,  $A_i$  means the  $i$  th bit.

(Warning : if you look to Matsui's papers, the bits there are numbered from right to left beginning at 0 )

$$A\{i_1, i_2, \dots, i_n\} = A_{i_1} \oplus A_{i_2} \oplus \dots A_{i_n}$$

We look for relations looking as

$$M\{i_1, i_2, \dots, i_a\} \oplus C\{j_1, j_2, \dots, j_b\} = K\{k_1, k_2, \dots, k_c\} \quad (0.25)$$

verified with probability  $p$  for randomly given plaintexts (0.25) should be true 1 time over  $2^{\frac{1}{2}}$ . We are therefore interested in the deviation  $\epsilon = p - \frac{1}{2}$ .

## Method

$$\epsilon = p - \frac{1}{2}$$

is called the **effectiveness** of the relation (0.25) is  $|\epsilon| = |p - \frac{1}{2}|$ . Starting with  $N$  plaintexts  $M$  with  $T$  among them give 0 for  $M\{i_1, i_2, \dots, i_a\} \oplus C\{j_1, j_2, \dots, j_b\}$ , then the suggested value for  $K\{k_1, k_2, \dots, k_c\}$  is given by the following table :

	if $T > N/2$	si $T < N/2$	(0.26)
if $p > 1/2$	0	1	
if $p < 1/2$	1	0	

## DES Attack :

$N$  plaintexts  $P$ .

- 1 One looks for the best  $r - 1$  rounds approximation :

$$P\{i_1, \dots, i_a\} \oplus C\{j_1, \dots, j_b\} \oplus F_r(G_r, K_r)\{\ell_1, \dots, \ell_d\} = K\{k_1, \dots, k_c\} \quad (0.27)$$

This will help us to recover  $K_r$  and  $K\{k_1, \dots, k_c\}$  :

- 2 for each possible value  $K_r^{(i)}$  of  $K_r$ ,  $T_i$  = number of  $P$  so that the left side = 0 in (0.27)
- 3 Determinate the values of  $i$ ,  $min$  such that  $T_i$  is minimum and  $max$  such that  $T_i$  is maximum



## DES Attack (continued)

- If  $|T_{max} - N/2| > |T_{min} - N/2|$ , take

$$K_r = K_r^{(max)}, K\{k_1, k_2, \dots, k_c\} = 0 \text{ if } p > 1/2 \text{ or } = 1 \text{ if } p < 1/2$$

Rk : we have  $T_{max} > N/2$ , otherwise one deduces  $T_{min} - N/2 < 0$ , and  $T_{max} - N/2 < T_{min} - N/2$ , absurd

- If  $|T_{max} - N/2| < |T_{min} - N/2|$ , take

$$K_r = K_r^{(min)}, K\{k_1, k_2, \dots, k_c\} = 1 \text{ if } p > 1/2 \text{ or } = 0 \text{ if } p < 1/2$$

(One has  $T_{min} < N/2$ , otherwise  $T_{max} - N/2 > 0$  and  $T_{max} - N/2 < T_{min} - N/2$ , absurd)

# Relations

Matsui uses 5 relations deduced from the previous tables by composing with  $E$  and  $P$ .

- Relation A : From  $NL_5(16, 15) = 12$ , one gets :

$$D\{17\} \oplus f(D, K)\{3, 8, 14, 25\} = K\{26\} \text{ avec } p = 12/64 .$$

(0.28)

- Relation B : from  $NL_1(27, 4) = 22$ , one gets :

$$D\{1, 2, 4, 5\} \oplus f(D, K)\{17\} = K\{2, 3, 5, 6\} \text{ avec } p = 22/64 .$$

(0.29)

- Relation C : from  $NL_1(4, 4) = 30$ , one gets :

$$D\{3\} \oplus f(D, K)\{17\} = K\{4\} \text{ avec } p = 30/64 . \quad (0.30)$$

- Relation D : from  $NL_5(16, 14) = 42$ , one gets :

$$D\{17\} \oplus f(D, K)\{8, 14, 25\} = K\{26\} \text{ avec } p = 42/64 . \quad (0.31)$$

- Relation E : from  $NL_5(34, 14) = 16$ , one gets :

$$D\{16, 20\} \oplus f(D, K)\{8, 14, 25\} = K\{25, 29\} \text{ avec } p = 16/64 . \quad (0.32)$$

**Remark :** for comparing to Matsui one should replace  $k$  by  $48 - k$  or  $32 - k$ , according to the bit numbers.

# Relations

Matsui uses 5 relations deduced from the previous tables by composing with  $E$  and  $P$ .

- Relation A : From  $NL_5(16, 15) = 12$ , one gets :

$$D\{17\} \oplus f(D, K)\{3, 8, 14, 25\} = K\{26\} \text{ avec } p = 12/64 .$$

(0.33)

- Relation B : from  $NL_1(27, 4) = 22$ , one gets :

$$D\{1, 2, 4, 5\} \oplus f(D, K)\{17\} = K\{2, 3, 5, 6\} \text{ avec } p = 22/64 .$$

(0.34)

- Relation C : from  $NL_1(4, 4) = 30$ , one gets :

$$D\{3\} \oplus f(D, K)\{17\} = K\{4\} \text{ avec } p = 30/64 . \quad (0.35)$$

- Relation D : from  $NL_5(16, 14) = 42$ , one gets :

$$D\{17\} \oplus f(D, K)\{8, 14, 25\} = K\{26\} \text{ avec } p = 42/64 . \quad (0.36)$$

- Relation E : from  $NL_5(34, 14) = 16$ , one gets :

$$D\{16, 20\} \oplus f(D, K)\{8, 14, 25\} = K\{25, 29\} \text{ avec } p = 16/64 . \quad (0.37)$$

Remark : for comparing to Matsui one should replace  $k$  by  $48 - k$  or  $32 - k$ , according to the bit numbers.

## “Piling lemma”

**Theorem :**  $X_i=0$  ou  $1$ , random variables,  $p(X_i = 0) = \frac{1}{2} + \epsilon_i$   
Then  $p(X_1 \oplus \dots \oplus X_n) = \frac{1}{2} + \epsilon$  with  $\epsilon = 2^{n-1}\epsilon_1 \dots \epsilon_n$

Recursion proof, using the case  $n = 2$  :

The probability is

$$\begin{aligned} & p_1 \cdot p_2 + (1 - p_1)(1 - p_2) \\ &= \left(\frac{1}{2} + \epsilon_1\right)\left(\frac{1}{2} + \epsilon_2\right) + \left(\frac{1}{2} - \epsilon_1\right)\left(\frac{1}{2} - \epsilon_2\right) \\ &= 2 \times \frac{1}{2} \cdot \frac{1}{2} + 2 \times \epsilon_1 \cdot \epsilon_2 \end{aligned}$$

## Linear approximation for 3 rounds

- 1st round :  $D_0\{17\} \oplus f(D_0, K_1)\{3, 8, 14, 25\} = K_1\{26\}$   
 $D_1 = G_0 \oplus F_1 \Rightarrow F_1 = D_1 \oplus G_0$   
 $D_1\{3, 8, 14, 25\} \oplus G_0\{3, 8, 14, 25\} \oplus D_0\{17\} = K_1\{26\}$
- last round :  
 $D_2\{17\} \oplus f(D_2, K_3)\{3, 8, 14, 25\} = K_3\{26\}$   
 $D_3 = G_2 \oplus F_3 = D_1 \oplus F_3 = C_L, G_3 = D_2 = C_H$   
 $D_1\{3, 8, 14, 25\} \oplus D_3\{3, 8, 14, 25\} \oplus D_2\{17\} = K_3\{26\}$
- performing xor :  
 $G_0\{3, 8, 14, 25\} \oplus D_3\{3, 8, 14, 25\} \oplus D_0\{17\} \oplus G_3\{17\} =$   
 $K_1\{26\} \oplus K_3\{26\}$  and  
 $G_0\{3, 8, 14, 25\} \oplus D_0\{17\} \oplus G_3\{17\} \oplus D_3\{3, 8, 14, 25\} =$   
 $K_1\{26\} \oplus K_3\{26\}$
- The probability is 0,70.  $|\epsilon| = 0, 20$ .
- We compute as in (0.26) : With a number  $N > (1/\epsilon)^2 = 25$ , the success rate for the determination of  $K_1\{26\} \oplus K_3\{26\}$  is at least 97,7 % .

## Comments

N= Number of plaintexts randomly distributed.

success rate for the algorithm :

$$\frac{1}{\sqrt{2\pi}} \int_{-2\epsilon\sqrt{N}}^{\infty} \exp(-x^2/2) dx$$

Numerically :

N	$\epsilon^{-2}/4$	$\epsilon^{-2}/2$	$\epsilon^{-2}$	$2\epsilon^{-2}$
rate	84,1	92,1	97,7	99,8



## Linear approximation for 5 rounds

Set  $\alpha = \{3, 8, 14, 25\}$ ,  $\beta = \{1, 2, 4, 5\}$ ,

$\gamma = \{2, 3, 5, 6\}$  et  $\delta = \{8, 14, 25\}$

By one shift of the 3 round relation :

$$G_1\{\alpha\} \oplus D_4\{\alpha\} \oplus D_1\{17\} \oplus G_4\{17\} = K_2\{26\} \oplus K_4\{26\} \quad (0.38)$$

Using relation B :

$$D\{\beta\} \oplus F\{17\} = K\{\gamma\}$$

giving from  $F_1 = G_0 \oplus D_1$  :

$$D_0\{\beta\} \oplus G_0\{17\} \oplus D_1\{17\} = K_1\{\gamma\} \quad (0.39)$$

## 5 rounds continued

shifting by 4 :

$$D_4\{\beta\} \oplus G_4\{17\} \oplus D_5\{17\} = K_5\{\gamma\} \quad (0.40)$$

We add the 3 relations (27) (28) (29) cancelling the 2  $G_4\{17\}$  and the 2  $D_1\{17\}$  we get :

$$G_0\{17\} \oplus D_5\{17\} \oplus D_0\{\alpha, \beta\} \oplus G_5\{\alpha, \beta\} = \\ K_1\{\gamma\} \oplus K_2\{26\} \oplus K_4\{26\} \oplus K_5\{\gamma\}$$

because  $G_1 = D_0$  et  $G_5 = D_4$

## The best linear relations

r	relation	$\epsilon$	characteristic
3	$G_0\{\alpha\} \oplus D_0\{17\} \oplus D_3\{\alpha\} \oplus G_3\{17\}$ $= K_1\{26\} \oplus K_3\{26\}$	$1,56 \cdot 2^{-3}$	A-A
7	$G_0\{\delta\} \oplus D_0\{16, 20\} \oplus D_7\{\alpha\} \oplus G_7\{17\}$ $= K_1\{25, 29\} \oplus L_3 \oplus K_7\{26\}$	$1,952^{-10}$	E-DCA-A
8	$G_0\{\delta\} \oplus D_0\{16, 20\} \oplus D_8\{17\} \oplus G_8\{\alpha, \beta\}$ $= K_1\{25, 29\} \oplus L_3 \oplus K_7\{26\} \oplus K_8\{\gamma\}$	$-1,22 \cdot 2^{-11}$	E-DCA-AB
14	$D_0\{\delta\} \oplus D_{14}\{\alpha\} \oplus G_{14}\{17\}$ $= L_2 \oplus L_6 \oplus L_{10} \oplus K_{14}\{26\}$	$-1,19 \cdot 2^{-21}$	-DCA-ACD DCA-A
15	$G_0\{\delta\} \oplus D_0\{16, 20\} \oplus D_{15}\{\alpha\} \oplus G_{15}\{17\}$ $= K_1\{25, 29\} \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}\{26\}$	$1,19 \cdot 2^{-22}$	E-DCA-ACD DCA-A
16	$G_0\{\delta\} \oplus D_0\{16, 20\} \oplus G_{16}\{17\} \oplus D_{16}\{\alpha, \beta\}$ $= K_1\{25, 29\} \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}\{26\} \oplus K_{16}\{\gamma\}$	$-1,49 \cdot 2^{-24}$	E-DCA-ACD DCA-AB

Used notation :  $L_i = K_i\{26\} \oplus K_{i+1}\{4\} \oplus K_{i+2}\{22\}$

## Approximations on $r$ rounds

We generalize the above computation for producing recursively  $r$  rounds approximations .

The relation for the  $i$  th round is :

$$D_{i-1}\{\theta_i\} \oplus F_i\{\alpha_i\} = K_i\{\gamma_i\}$$

Using  $F_i = D_i \oplus D_{i-2}$  for deducing :

$$D_{i-1}\{\theta_i\} \oplus D_i\{\alpha_i\} \oplus D_{i-2}\{\alpha_i\} = K_i\{\gamma_i\}$$

Consider 3 consecutive relations including  $D_{i-1}$  :

$$D_{i-2}\{\theta_{i-1}\} \oplus D_{i-1}\{\alpha_{i-1}\} \oplus D_{i-3}\{\alpha_{i-1}\} = K_{i-1}\{\gamma_{i-1}\} \quad (0.41)$$

$$D_{i-1}\{\theta_i\} \oplus D_i\{\alpha_i\} \oplus D_{i-2}\{\alpha_i\} = K_i\{\gamma_i\} \quad (0.42)$$

$$D_i\{\theta_{i+1}\} \oplus D_{i+1}\{\alpha_{i+1}\} \oplus D_{i-1}\{\alpha_{i+1}\} = K_{i+1}\{\gamma_{i+1}\} \quad (0.43)$$

## Formulas

If one want to go trough the rounds,  $D_{i-1}$  must cancell ; as its masks are  $\theta_i, \alpha_{i-1}$  et  $\alpha_{i+1}$ .

we obtain the following recursion formula :

$$\theta_i = \alpha_{i-1} \oplus \alpha_{i+1}$$

## Attack Schedule

for the 8 rounds DES, one uses the 7 rounds approximation :

$$\begin{aligned} G_0\{\delta\} \oplus D_0\{16, 20\} \oplus D_7\{\alpha\} \oplus G_7\{17\} \\ = K_1\{25, 29\} \oplus K_3\{10\} \oplus K_4\{4\} \oplus K_5\{26\} \oplus K_7\{26\} \end{aligned}$$

for deducing via  $G_7 = F_8 \oplus D_8$  :

$$\begin{aligned} G_0\{\delta\} \oplus D_0\{16, 20\} \oplus G_8\{\alpha\} \oplus D_8\{17\} \oplus f(G_8, K_8)\{17\} \\ = K_1\{25, 29\} \oplus K_3\{10\} \oplus K_4\{4\} \oplus K_5\{26\} \oplus K_7\{26\} \end{aligned}$$

## bits recovering

- So we recover 6 bits of the key plus one supplementary relation.
- This is almost equivalent to the knowledge of 7 bits.
- Shifting upwards we find another set of 7 bits :
- we have now 42 bits to recover.
- Results :
  - $2^{20}$  plaintexts in 20 secondes : rate of succes 88%
  - $2^{21}$  plaintexts in 40 secondes : rate of succes 99%

## DES Attack

for the true DES, with a 15 rounds characteristic :

$$\begin{aligned} & G_0\{\delta\} \oplus D_0\{16, 20\} \oplus D_{15}\{\alpha\} \oplus G_{15}\{17\} \\ &= K_1\{25, 29\} \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}\{26\} \end{aligned}$$

one deduces via  $G_{15} = F_{16} \oplus D_{16}$

$$\begin{aligned} & G_0\{\delta\} \oplus D_0\{16, 20\} \oplus G_{16}\{\alpha\} \oplus D_{16}\{17\} \oplus f(G_{16}, K_{16}) \\ &= K_1\{25, 29\} \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}\{26\} \end{aligned}$$

and proceeding as before... few memory needed  
faster than exhaustive search



## Ciphertexts

Example with the 8 round DES :

One uses relation with effectivity  $\simeq 2^{-17}$  :

$$D_0\{5\} \oplus D_8\{5\} \oplus G_8\{0\} \oplus f(G_8, K_8)\{5\} =$$

$$K_2\{47\} \oplus K_3\{40\} \oplus K_4\{47\} \oplus K_6\{47\} \oplus K_7\{40\}$$

which contains  $D_0\{5\}$  = the 25 th bit of the plaintext which should be 0 for an english text :

So the above relation contains NO bit from the plaintext !

We recover 7 bits with large probability in using  $8(2^{-17})^{-2} = 2^{37}$  plaintexts. With the same effectivity  $1,83 \cdot 2^{-12}$ ,

$$D_0\{\delta\} \oplus D_8\{\delta, 18\} \oplus G_8\{17\} \oplus f(G_8, K_8)\{18\} = K_2\{26\}$$

## 16 rounds attack

One begins with the 14 round relation :

$$D_0\{\delta\} \oplus D_{14}\{\alpha\} \oplus G_{14}\{17\} = L_2 \oplus L_6 \oplus L_{10} \oplus K_{14}\{26\}$$

with a shift

$$D_1\{\delta\} \oplus D_{15}\{\alpha\} \oplus G_{15}\{17\} = L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}\{26\}$$

we expand it in both directions via  $D_1 = G_0 \oplus F_1$  and  $G_{15} = D_{16} \oplus F_{16}$ ,

$$\begin{aligned} G_0\{\delta\} \oplus f(G_0, K_1)\{\delta\} \oplus G_{16}\{\alpha\} \oplus D_{16}\{17\} \oplus f(D_{16}, K_{16})\{17\} \\ = L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}\{26\} \end{aligned}$$

This equation has 13 bits of plaintext and 12 bits of key in the first member

## Mirror relation

$$\begin{aligned} D_{16}\{\delta\} \oplus f(D_{16}, K_{16})\{\delta\} \oplus D_0\{\alpha\} \oplus G_0\{17\} \oplus f(G_0\{17\}, K_1)\{17\} \\ = L_4 \oplus L_8 \oplus L_{12} \oplus K_2\{26\} \end{aligned}$$

Actually we get the equivalence of 26 key bits

Rather than producing statistical conclusions from these 26 bits, it is better to work separately with two 13 bit packs getting therefore two orderings

Let  $(a, b)$  be a pair of packs.

Let  $r_a$  and  $r_b$  the ranks  $a$  and  $b$  in the orderings.

We give to  $(a, b)$  the rank  $(1 + r_a)(1 + r_b)$ .

We look for the remaining 30 bits by taking the first ranked  $(a, b)$ .

# Algorithm

## ① Counting

- ① Prepare  $2^{13}$  counters  $TA_t$  with 0 as initial value, each one corresponding to one bit present in the relation
- ② for  $P_i$  encrypted as  $C_i$  compute the value  $t = t_i$  of the 13 bits sequence and increase the corresponding counter  $TA_t$ .

## ② Counting for the keys

- ① Prepare  $2^{12}$  counters  $KA_k$  with 0 as initial values, corresponding to the key bits.
- ② for each  $k$ , and each  $i$  compute the first member and if it is 0, add  $TA_{t_i}$  to  $KA_k$ .

## ③ Exploitation

- ① Reorder the counters according to decreasing values of  $|KA_k - N/2|$ ,
- ② for the first in the new order take the right member to be 0 if  $KA_k - N/2 > 0$  and 1 otherwise and validate  $k$  as good value.
- ③ Complete  $k$  by using exhaustive research.
- ④ In case of failure take the 2 nd in the order

## Several linear relations

Suppose we have  $n$  linear relations with efficiency  $\epsilon_i$ , see (0.25)

$$M\{\alpha_i\} \oplus C\{\beta_i\} = K\{\gamma\} ,$$

set  $T_i$  = number of plaintext verifying the  $i$  th relation form the weighted sum  $U = \sum a_i T_i$ .

The best approximation of  $K\{\gamma\}$

is obtained by using the statistical number  $U$  with weights

$$a_i = \epsilon_i / \sum_k \epsilon_k$$

same kind of trick in case of several relations (0.27)

## DES invariant tables

# Differential distribution table for the S-box $S_1$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	64	2	8	14	4	10	6	12	8	18	2	16	6	12	6	12	6	16	12	6	12	4	8	4	6	6	6	4	4	10	2	4	
1	10	2	8	4	10	8	4	4	12	2	8	4	10	6	4	10	8	8	4	8	4	8	4	8	4	6	6	6	4	10	2	4	
2	10	2	8	12	6	6	2	10	4	6	10	4	8	2	10	2	4	8	6	2	4	8	6	10	6	2	4	2	10	4	6	10	
3	10	6	8	12	6	2	4	4	12	2	2	10	8	8	8	4	10	4	2	6	10	4	8	10	6	4	4	4	2	6	10	8	
4	10	2	4	10	10	2	8	10	2	2	2	2	4	6	4	6	10	6	2	10	2	10	2	10	8	10	4	10	6	8	14	2	
5	10	2	4	6	10	4	4	8	4	8	2	6	8	6	6	10	4	6	10	2	10	2	2	2	6	4	8	6	10	10	2	2	
6	10	4	4	4	10	4	6	8	8	6	6	4	6	2	4	4	2	8	4	4	4	4	4	10	2	4	6	6	6	10	10	2	
7	10	4	4	12	6	2	2	4	4	6	10	10	6	10	2	14	6	6	6	2	10	6	2	2	6	6	4	12	2	10	8	8	
8	10	10	6	10	6	10	8	12	10	2	6	12	10	6	4	10	4	6	2	8	6	10	4	2	10	6	6	6	10	6	6	6	
9	10	10	6	4	4	4	4	4	6	2	4	6	6	6	6	8	6	10	4	10	2	2	2	4	4	4	2	2	4	4	4	8	
10	10	12	8	4	6	4	4	8	12	8	6	12	6	4	4	2	6	6	2	6	2	10	4	6	10	4	6	10	2	10	10	2	
11	10	4	6	1	4	10	12	8	10	10	6	4	6	10	2	11	6	6	8	4	10	12	6	8	4	10	4	2	4	6	8	10	
12	10	10	12	12	2	12	4	12	8	10	4	6	6	10	2	4	6	4	4	4	10	12	6	6	6	12	4	2	2	2	6	12	4
13	10	6	6	12	8	4	10	12	10	10	4	6	6	12	4	6	6	4	10	6	8	4	6	6	6	8	4	6	10	4	6	6	4
14	10	2	4	12	6	4	10	4	12	12	2	10	14	10	10	8	10	4	4	4	6	12	2	12	4	6	4	4	14	6	6	6	4
15	10	4	10	10	12	6	12	4	4	12	10	12	12	12	8	8	6	10	6	10	10	4	6	10	2	10	8	10	10	10	10	2	4

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63		
0	10	10	10	10	12	6	10	10	12	4	12	4	6	6	2	4	8	2	4	8	2	6	2	2	6	2	4	6	10	8	8	8		
1	10	4	4	4	10	4	4	4	2	2	2	2	2	6	2	4	8	2	2	6	2	6	2	2	6	2	4	6	10	4	6	8		
2	10	2	6	4	10	4	4	4	2	2	2	4	2	2	6	2	2	6	2	6	2	16	4	2	12	2	2	6	4	4	6	2	4	
3	10	4	2	8	2	12	10	10	8	10	6	2	4	2	2	2	10	10	4	2	6	10	2	2	4	2	2	4	4	10	10	2	2	
4	10	4	10	10	2	4	10	12	10	10	10	10	4	10	8	10	2	12	2	4	10	2	8	8	12	12	6	10	10	12	2	4	2	
5	12	8	8	12	2	4	10	4	6	2	2	6	12	4	2	6	6	2	12	8	10	10	10	4	10	10	6	8	2	10	6	4	10	
6	8	10	12	6	2	4	12	12	12	4	8	6	10	4	4	8	12	2	2	4	10	10	12	4	12	4	10	4	4	10	4	2	2	
7	12	10	10	10	10	10	10	10	10	10	10	10	10	4	4	6	10	10	4	12	12	10	10	10	10	10	8	6	6	10	8	14	4	
8	10	4	12	6	12	2	4	10	10	10	10	10	2	2	4	12	8	6	6	4	6	10	4	12	4	4	4	4	2	4	6	4	4	
9	6	4	12	6	14	2	4	8	12	14	14	12	2	4	10	4	12	10	6	10	10	4	12	4	12	4	6	10	4	12	2	2	2	
10	4	10	6	12	2	2	6	10	6	10	2	6	4	6	6	4	4	12	10	4	12	10	6	6	12	4	2	6	8	4	10	10	8	
11	4	10	10	10	10	10	4	4	10	12	2	6	12	8	10	2	6	4	12	8	12	10	6	6	8	6	4	4	2	6	12	4	10	4
12	4	4	4	2	2	4	4	8	4	4	2	6	8	8	12	8	6	2	12	4	10	10	10	6	10	4	2	2	4	4	10	10	8	
13	12	10	10	4	6	2	4	8	10	6	10	4	2	2	2	2	4	12	6	8	2	4	12	6	4	6	4	4	12	8	6	4	2	
14	10	2	4	10	2	2	4	6	10	2	8	12	10	6	4	2	10	8	12	10	14	10	12	10	10	10	4	4	6	2	4	4	12	
15	12	8	10	10	4	2	10	4	2	4	2	4	6	6	4	2	4	10	6	10	4	6	10	2	10	10	10	10	10	10	10	10	4	4

# Linear distribution table for the S-box $S_1$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	2	1	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
2	3	4	1	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
3	4	5	6	1	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
4	5	6	7	8	1	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
5	6	7	8	9	10	1	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
6	7	8	9	10	11	12	1	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
7	8	9	10	11	12	13	14	1	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
8	9	10	11	12	13	14	15	16	1	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
9	10	11	12	13	14	15	16	17	18	1	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
10	11	12	13	14	15	16	17	18	19	20	1	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
11	12	13	14	15	16	17	18	19	20	21	22	1	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
12	13	14	15	16	17	18	19	20	21	22	23	24	1	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	2	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
1	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32
2	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33
3	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34
4	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35
5	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36
6	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37
7	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38
8	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39
9	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39	40
10	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39	40	41
11	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39	40	41	42
12	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39	40	41	42	43
13	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39	40	41	42	43	44
14	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39	40	41	42	43	44	45
15	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46



# Differential distribution table for the S-box $S_2$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	54	10	10	4	10	12	4	10	10	10	6	10	6	10	6	10	6	10	4	10	6	6	10	6	10	10	6	10	10	4	10	4
1	10	10	10	8	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
2	10	10	10	4	10	4	6	6	10	4	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
3	10	4	10	10	10	8	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
4	10	10	10	4	10	10	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
5	10	10	4	6	6	4	4	4	8	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
6	10	6	6	4	10	6	6	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
7	10	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
8	10	10	10	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
9	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	10	6	6	4	4	4	8	4	6	10	4	6	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
12	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
13	10	4	10	10	10	6	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
14	10	6	10	10	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
15	10	10	6	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	10	10	4	8	10	6	10	6	10	8	10	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
1	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
2	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
3	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
5	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
7	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
8	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
9	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
12	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
13	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
14	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
15	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10

# Linear distribution table for the S-box $S_2$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
1	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
2	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
3	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
4	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
5	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
6	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
7	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
8	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
9	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
10	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
11	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
12	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
13	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
14	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
15	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
1	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
2	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
3	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
4	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
5	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
6	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
7	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
8	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
9	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
10	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
11	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
12	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
13	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
14	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	
15	1	16	8	4	2	1	0	15	7	3	14	6	13	5	12	10	9	11	18	17	20	22	25	23	24	26	27	28	29	30	31	

### Differential distribution table for the S-box $S_3$

Out	In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	64	8	8	8	8	8	6	8	8	8	10	8	8	8	8	8	8	8	8	4	8	4	8	4	8	8	8	8	8	8	8	8	8	
1	8	8	8	8	6	8	2	10	8	8	2	10	6	8	8	8	4	6	8	8	2	4	6	8	6	8	8	8	8	8	10	6	8	8
2	8	8	8	8	10	8	4	6	8	8	8	8	6	8	8	8	4	6	8	2	8	12	4	2	10	6	4	4	6	8	8	8	8	
3	8	8	2	2	4	4	8	8	6	4	10	8	2	8	10	8	8	2	6	4	6	2	8	10	4	8	8	8	8	8	8	6	8	8
4	8	8	8	8	8	8	8	8	8	10	4	2	8	10	14	4	2	8	4	4	2	6	2	8	8	6	6	4	4	2	4	2	4	10
5	8	4	2	6	2	10	8	4	4	4	6	2	12	4	12	2	12	8	8	2	4	4	4	4	2	8	8	8	8	4	12	8	6	8
6	8	8	8	8	8	4	6	4	4	4	6	4	4	12	8	4	4	4	2	8	12	6	8	8	2	4	6	10	6	8	8	4	4	8
7	8	12	8	6	2	2	12	2	6	8	8	8	8	8	8	4	8	8	8	8	10	2	8	8	2	4	4	2	4	4	8	6	4	6
8	8	8	8	8	8	8	8	2	2	10	8	8	4	4	8	8	2	10	6	8	8	8	8	8	2	6	4	2	4	8	12	2	10	4
9	8	14	4	4	12	8	4	4	6	6	6	6	2	8	8	4	2	4	4	8	2	2	6	2	2	2	8	2	8	8	8	8	8	8
10	8	8	12	8	8	8	8	8	4	6	8	6	6	8	8	14	4	6	2	12	2	2	6	2	2	2	4	6	8	2	10	4	2	8
11	8	4	10	2	4	8	8	8	8	6	4	8	8	4	8	4	12	6	8	2	2	2	2	2	8	10	8	8	10	8	8	2	6	10
12	8	8	4	8	6	8	8	6	4	6	6	4	2	8	6	4	6	2	8	4	4	2	2	4	6	10	2	2	4	4	4	4	4	8
13	8	2	6	4	8	8	4	4	8	8	8	8	8	8	14	2	4	6	14	8	8	4	8	6	8	8	6	2	8	8	10	8	8	8
14	8	6	8	2	10	4	8	4	8	4	2	14	2	4	2	2	8	8	14	4	8	4	8	4	8	6	10	8	8	8	8	8	8	8
15	8	10	8	2	4	2	8	6	8	6	8	12	10	2	8	8	4	8	2	8	8	8	2	4	2	6	2	4	2	8	14	2	8	8

Out	In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0		0	18	12	2	4	6	6	0	6	0	0	10	10	4	4	8	0	2	2	4	0	4	4	4	4	0	6	2	0	4	8	2
1		0	8	6	2	8	0	0	2	2	2	6	2	4	2	0	0	10	6	4	6	6	4	8	8	6	0	2	2	6	6	6	6
2		0	8	4	10	2	0	0	4	10	8	0	6	6	4	2	0	8	2	4	6	2	10	4	2	12	4	2	6	4	8	4	4
3		0	0	4	6	12	2	0	4	16	0	4	4	6	2	4	10	0	6	0	8	8	2	10	4	4	0	0	2	6	4	4	0
4		0	8	0	0	6	8	4	8	6	0	0	2	4	4	4	0	4	12	4	2	6	16	8	0	0	2	6	4	0	12	2	0
5		4	4	4	2	4	2	4	2	4	4	4	2	2	6	4	0	4	2	8	6	2	6	2	6	2	2	4	6	4	2	10	10
6		4	2	10	4	2	0	4	6	0	4	8	2	4	10	4	4	8	4	8	4	0	2	2	6	6	6	6	4	4	4	2	8
7		8	4	2	10	10	2	0	6	4	6	6	0	2	16	4	2	12	8	4	2	2	2	4	6	6	4	4	8	6	2	2	2
8		0	0	0	4	2	8	4	10	4	4	4	4	2	2	2	0	10	2	8	2	12	6	4	2	2	8	4	4	2	10	2	2
9		2	6	4	12	2	8	2	2	2	10	8	2	10	2	6	4	4	2	4	2	2	2	10	4	4	10	2	2	2	2	2	8
10		2	6	4	4	2	2	14	4	4	4	4	2	4	0	6	6	4	2	2	6	4	0	4	8	2	4	2	4	2	6	4	6
11		4	6	12	2	4	2	0	4	8	8	4	0	4	4	2	12	6	0	8	4	0	6	4	4	12	4	6	8	8	6	2	4
12		10	0	4	6	2	4	8	0	2	4	4	2	0	4	2	4	12	2	6	12	4	2	16	4	2	12	4	4	2	4	6	2
13		16	0	4	4	0	4	10	2	2	4	2	4	2	2	0	8	10	12	2	0	10	6	10	8	4	2	4	6	4	2	2	2
14		12	2	0	8	4	10	2	8	4	4	6	6	2	4	6	6	0	0	0	2	2	6	0	8	0	6	4	4	2	10	4	0
15		2	0	2	8	6	6	2	2	2	6	6	2	6	8	6	0	6	2	2	2	8	6	8	2	4	2	2	6	10	0	2	4

# Linear distribution table for the S-box $S_3$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	
14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
1	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
2	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	
3	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	
4	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	
5	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	
6	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	
7	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	
8	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	
9	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	
10	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	
11	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	
12	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	
13	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	
14	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	
15	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	

# Differential distribution table for the S-box $S_4$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	54	1	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	
1	1	54	10	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	
2	10	6	54	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	
3	8	12	4	15	1	10	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	
4	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15
5	4	15	8	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	
6	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	
7	1	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	
8	10	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	
9	8	12	4	15	1	10	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	
10	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15
11	4	15	8	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	
12	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	
13	1	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	
14	10	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	
15	8	12	4	15	1	10	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
0	54	1	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	
1	1	54	10	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	
2	10	6	54	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	
3	8	12	4	15	1	10	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	
4	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15
5	4	15	8	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	
6	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	
7	1	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	
8	10	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	
9	8	12	4	15	1	10	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	
10	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15
11	4	15	8	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	4	6	12	2	8	15	
12	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	
13	1	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	8	12	4	15	4	10	
14	10	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	12	4	15	8	6	
15	8	12	4	15	1	10	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	8	12	4	15	1	10	

# Linear distribution table for the S-box $S_4$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32																															
1				4																												
2																																
3																																
4																																
5																																
6																																
7																																
8																																
9																																
10																																
11																																
12																																
13																																
14																																
15																																

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0																																
1																																
2																																
3																																
4																																
5																																
6																																
7																																
8																																
9																																
10																																
11																																
12																																
13																																
14																																
15																																

# Differential distribution table for the S-box $S_5$

Out	In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0		64	10	10	8	10	12	8	10	10	8	10	4	10	10	10	4	10	6	10	10	10	4	10	10	10	10	10	10	10	4	10	10	
1		10	6	10	10	10	12	10	8	10	10	6	6	4	10	4	6	4	10	6	10	10	10	6	6	10	4	10	10	10	10	4	10	
2		10	10	10	10	10	10	10	4	4	10	8	10	10	10	10	10	10	10	10	10	4	6	10	10	10	10	10	10	10	10	10	6	8
3		10	4	4	6	8	4	6	8	10	10	4	6	4	10	10	8	10	10	10	10	10	4	8	10	10	10	10	10	10	10	10	4	10
4		10	10	10	10	10	10	10	4	4	10	10	8	10	10	10	10	10	10	10	10	4	8	10	10	10	10	10	10	10	10	10	4	10
5		10	10	10	10	4	4	4	6	10	8	6	8	10	10	10	10	10	10	10	10	4	8	10	10	10	10	10	10	10	10	10	10	4
6		10	8	6	10	10	10	8	10	10	6	10	6	10	10	10	10	10	10	10	10	4	10	10	10	10	10	10	10	10	10	10	10	10
7		10	6	4	10	6	10	10	10	6	10	4	10	10	10	10	10	10	10	10	10	4	10	10	10	10	10	10	10	10	10	10	10	10
8		10	10	10	6	10	10	4	4	10	10	8	10	10	10	10	10	10	10	10	10	4	8	10	10	10	10	10	10	10	10	10	10	10
9		10	4	6	8	6	10	10	4	8	4	10	10	10	6	6	10	10	10	10	10	4	8	10	10	10	10	10	10	10	10	10	10	10
10		10	10	4	6	6	10	6	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11		10	10	10	10	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
12		10	10	10	4	4	8	10	6	10	8	6	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
13		10	10	10	10	6	10	10	10	10	10	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
14		10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
15		10	10	4	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10

Out	In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
0		10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	
1		10	10	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
2		10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
3		8	6	10	4	4	8	4	10	6	8	10	6	6	4	4	10	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
4		10	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
5		8	10	10	10	4	8	4	10	4	4	4	8	6	6	6	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
6		10	6	10	10	6	10	4	10	6	6	10	10	6	4	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
7		6	4	10	4	10	6	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
8		10	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
9		4	10	10	8	6	4	8	4	6	10	10	10	4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
10		4	10	10	8	6	10	4	8	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11		4	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
12		6	10	10	6	6	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
13		6	10	10	6	6	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
14		8	4	10	10	10	6	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
15		8	10	10	8	10	6	4	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10

# Linear distribution table for the S-box $S_5$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
1	0	0	4	0	2	2	2	2	0	-4	4	4	2	6	2	2	2	2	2	-6	4	4	0	4	6	2	2	2	0	4	-4	-4
2	0	0	0	2	2	2	2	-4	0	2	6	0	4	0	2	2	2	2	0	0	-4	0	6	-6	0	2	2	6	2	2	-8	8
3	0	0	2	6	0	-4	-6	2	6	2	0	4	2	2	0	8	0	0	2	2	0	-4	6	2	2	-6	-8	-4	2	6	0	8
4	0	0	0	0	0	0	0	0	0	0	0	6	0	0	6	0	4	2	2	0	-4	2	6	4	0	0	-6	4	-8	0	0	
5	0	0	2	2	2	0	-4	8	2	-4	-6	2	2	2	4	4	2	2	-4	4	0	4	2	6	4	310	2	4	0	2	-6	
6	0	0	-4	4	2	-6	2	6	2	-6	2	2	4	4	0	-6	2	2	2	2	0	-8	4	-4	-4	4	0	0	-6	2	-6	
7	0	0	0	-4	0	-4	0	0	-6	-6	2	2	2	10	110	2	2	-8	-4	-8	0	0	-8	4	2	2	2	2	2	2	2	
8	0	0	4	0	0	0	0	-4	2	6	2	2	2	2	2	0	4	4	4	-4	0	4	4	2	6	2	6	2	10	2	2	
9	0	0	0	0	2	2	2	6	2	2	2	2	4	0	2	4	2	6	-6	-4	0	-4	0	8	8	8	6	8	6	2	2	
10	0	0	2	2	2	2	10	4	0	2	2	2	2	2	4	8	2	2	4	4	4	-4	6	2	6	4	0	-4	-8	2	2	
11	0	0	2	6	4	0	2	-6	312	-4	2	2	-8	4	2	2	-4	0	6	2	4	4	2	2	0	4	2	2	-8	6	2	
12	0	0	0	2	-4	4	-6	2	2	2	4	0	2	-4	8	-8	-8	-6	-6	8	2	8	2	2	10	-4	2	2	4	-8		
13	0	0	0	2	2	2	2	6	-6	-4	-8	4	8	6	-6	2	-6	4	4	4	4	2	2	4	0	2	-6	2	2	4	0	
14	0	0	0	4	2	2	2	-6	-4	-8	-4	-4	-6	-6	2	10	2	-6	2	-4	0	0	0	2	2	2	2	2	0	4	0	
15	0	0	-4	-4	0	4	0	4	-4	4	0	4	0	-4	0	20	4	0	0	0	4	0	4	4	-4	-4	0	0	4	0	-4	

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63		
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
1	0	0	0	-4	0	-2	6	2	-16	4	0	0	8	2	-2	6	6	2	2	6	-6	0	-8	4	-8	2	-2	6	-2	-8	4	-4	0	
2	0	0	0	-2	0	6	-2	4	0	0	2	-4	4	-4	2	-6	-2	-2	0	0	-12	4	0	-2	-6	4	8	-10	-6	-6	2	4	-4	
3	0	0	2	2	4	4	0	-2	-2	-2	6	-8	4	-6	-2	-4	4	0	0	0	10	4	0	-6	-6	-2	0	4	-2	-2	-4	4	-4	
4	0	0	0	-2	6	0	0	-2	6	0	0	6	6	0	0	6	4	0	0	0	2	-4	8	-2	-6	0	-4	0	-10	4	2	14	0	
5	0	0	0	0	6	6	6	0	4	4	0	6	-6	-2	4	4	-6	-2	8	0	0	4	-4	0	6	-2	6	4	0	4	2	6	0	
6	0	0	0	-4	-4	-2	-2	0	6	-6	6	6	-6	0	-8	4	4	-2	-2	0	-2	4	4	8	0	4	4	4	0	-8	-2	-2	-6	
7	0	0	0	8	4	4	0	-4	-4	-2	-2	-6	6	6	-2	-2	-2	-4	0	4	-4	-8	4	4	-2	-6	-2	4	0	-2	-2	0	0	
8	0	0	0	-4	4	4	-4	4	0	0	2	6	0	-2	-10	4	4	0	4	0	0	-4	0	4	12	-2	-6	6	-10	-6	-2	2	2	
9	0	0	0	0	0	-6	-6	-2	6	-6	-2	6	-4	0	-8	4	2	-2	10	6	0	-4	-4	4	4	-4	-4	4	2	-10	-2	2	0	
10	0	0	-6	4	-2	2	4	-12	4	-8	-2	0	-2	-6	0	4	2	-2	0	0	-4	-4	0	-2	-6	-2	4	4	4	4	2	2	6	
11	0	0	6	-2	4	-8	-2	0	0	0	6	-4	-8	-2	-6	0	4	0	0	-10	0	4	-2	-2	0	4	0	0	0	0	-2	-2	0	
12	0	0	0	-2	0	6	0	2	6	-2	-8	-4	-2	-2	4	0	0	0	0	0	-4	4	6	-2	6	-2	4	0	0	0	2	4	0	0
13	0	0	0	-2	6	-14	-2	0	0	-2	-6	4	4	0	-2	2	2	2	4	4	-4	4	0	2	4	0	0	-2	2	-2	-4	0	0	
14	0	0	-16	4	2	6	-2	6	-4	0	-4	4	6	-2	-2	-2	2	2	2	0	-2	-4	-4	4	-2	-2	-2	2	4	4	0	4	-4	0
15	0	0	-12	-4	0	-4	0	-4	0	0	4	4	0	4	0	-4	4	4	0	0	0	0	4	-4	0	0	-4	4	4	4	0	4	4	0



# Differential distribution table for the S-box $S_6$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
1	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
3	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
4	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
5	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
6	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
7	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
8	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
9	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
10	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
11	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
12	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
13	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
14	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
15	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
2	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
3	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
4	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
5	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
6	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
7	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
8	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
9	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
10	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
11	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
12	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
13	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
14	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
15	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

# Linear distribution table for the S-box $S_6$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	4	4	0	0	8	0	2	2	6	2	-2	2	6	2	2	2	-2	-2	-2	18	10	6	0	4	4	8	0	4	0	-4
2	0	0	0	0	0	0	2	6	6	2	2	8	4	-8	4	0	0	0	0	-2	18	-6	6	-6	-2	6	-2	0	-4	-8	0	-4
3	0	0	-4	-4	2	2	6	10	-4	8	4	-6	-6	2	-6	10	2	2	2	4	4	4	6	4	6	-2	-2	-6	8	0	0	
4	0	0	-2	2	2	2	0	-4	4	2	18	2	-2	0	-8	0	4	2	-6	-2	-2	-4	-4	4	-4	-6	10	-2	8	0	12	
5	0	0	2	2	2	-6	4	-8	2	-6	4	4	4	-6	6	2	2	-8	0	-2	-4	6	2	4	6	2	6	2	2	4	4	
6	0	0	2	2	0	-4	6	-2	2	-6	-4	-4	-6	-6	4	4	4	0	0	-2	-4	-4	2	10	2	2	-8	-4	2	6	-4	4
7	0	0	10	6	-8	4	6	-8	0	2	0	4	-2	4	-2	-6	2	0	0	2	0	0	0	-4	-6	0	0	0	6	0	4	
8	0	0	2	-2	-2	-4	-4	-12	-2	2	-4	4	4	-4	6	18	0	0	0	2	2	18	0	-8	-2	2	0	0	-4	12	-6	-2
9	0	0	-6	-2	-2	2	0	8	4	-4	-6	-2	2	4	4	2	2	-8	4	-4	0	-6	-6	-6	-6	-4	0	0	-4	2	2	
10	0	0	-2	2	2	0	6	3	0	-4	-2	6	0	4	2	6	0	0	2	2	0	0	-6	-2	8	-4	2	-6	-4	-6	2	
11	0	0	14	-6	-4	4	-2	2	2	-2	-4	0	18	-2	0	-4	2	2	4	2	2	-4	0	0	2	2	2	-4	-4	2	2	
12	0	0	0	0	4	0	4	0	6	6	-2	6	-2	2	6	2	-4	0	-12	0	8	0	0	2	2	6	-6	-2	6	6	6	
13	0	0	0	0	0	4	4	0	12	0	4	8	-4	-4	0	-6	-2	-6	-2	2	2	2	2	2	2	2	2	6	-6	-2	2	
14	0	0	4	-4	18	-6	-6	2	4	4	4	2	2	-2	2	8	4	4	0	2	-2	2	2	2	0	4	0	-4	-2	2	2	
15	0	0	12	4	2	2	2	2	2	2	2	2	4	-8	4	0	2	2	-6	2	4	0	4	0	4	0	0	-8	-2	2	2	

## Differential distribution table for the S-box $S_7$

Out	In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
1		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
2		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
3		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
4		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
5		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
6		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
7		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
8		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
9		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
10		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
11		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
12		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
13		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
14		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
15		64	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64
Out	In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
0		10	4	18	6	4	2	6	4	14	2	2	16	6	2	2	6	8	4	2	4	6	2	2	6	6	4	16	2	6	4	14		
1		10	2	6	6	2	2	10	2	6	2	6	6	2	4	8	4	10	6	16	4	6	2	2	6	2	4	6	6	2	4	6	16	
2		10	6	10	2	6	2	6	2	6	2	6	6	4	8	4	10	6	14	6	2	2	2	6	2	16	4	6	6	2	4	6	16	
3		14	2	2	2	6	16	10	2	4	2	2	4	6	2	8	2	10	8	8	6	10	2	8	2	6	16	4	6	2	6	16		
4		10	12	4	10	8	2	10	2	4	2	4	6	8	2	10	8	6	6	2	2	10	4	4	4	8	10	2	10	2	12	2	8	
5		8	2	4	4	2	4	6	2	6	8	2	10	8	2	2	4	2	4	2	4	2	6	6	2	8	6	10	4	8	2	10	8	
6		4	4	10	6	6	4	14	2	4	8	2	2	6	8	4	2	10	2	2	2	2	2	4	4	4	2	4	2	4	4	6		
7		12	10	10	10	10	4	4	10	2	12	12	6	8	4	6	10	6	6	2	4	2	4	2	4	2	2	2	6	4	6	4	8	8
8		10	6	4	10	8	2	4	6	4	10	2	2	2	10	4	10	6	6	4	16	6	2	4	2	4	10	2	6	6	2	4	10	
9		4	4	10	4	2	8	2	6	6	6	8	2	8	4	2	6	4	10	4	2	2	10	2	2	2	4	4	6	4	10	10	2	
10		2	10	12	8	2	2	4	6	2	4	2	2	4	8	8	4	10	6	8	2	10	4	6	6	2	8	2	2	4	10	4	10	
11		8	2	2	2	10	4	6	2	2	4	4	2	2	10	4	8	6	2	2	4	2	8	2	8	6	6	10	6	2	6	6	10	
12		2	4	8	12	8	10	2	12	4	6	8	4	2	14	6	10	6	4	2	10	6	4	6	2	6	10	6	2	4	10	4	10	
13		6	10	6	2	6	4	2	10	4	4	2	6	10	6	2	10	4	6	4	2	4	16	4	4	2	10	12	4	12	4	8		
14		10	2	10	10	12	10	2	4	2	12	2	2	8	10	10	2	8	2	6	10	4	10	2	10	10	2	4	12	6	10	2	4	
15		14	2	2	10	2	2	2	4	2	4	6	10	2	4	6	6	10	2	2	4	8	2	10	10	10	2	2	4	6	10	2	4	

# Linear distribution table for the S-box $S_7$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
0	32	16	8	4	2	1	0	15	7	3	14	6	12	5	10	11	13	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
1	15	7	3	14	6	12	5	10	11	13	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6		
2	14	6	12	5	10	11	13	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9		
3	13	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
4	12	5	10	11	13	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	
5	11	13	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
6	10	11	13	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
7	9	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
8	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	
9	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
10	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	
11	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
12	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
13	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
14	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
15	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
1	0	0	0	0	0	0	-4	112	0	0	0	-4	4	4	-4	4	12	0	6	0	6	-2	-6	0	6	0	6	0	-2	-6	-2	-6	14
2	0	0	0	-2	-2	-2	-4	0	-4	0	0	10	6	2	0	-8	-2	0	0	0	-8	-2	-2	-6	-6	-4	0	8	-8	6	10	0	
3	0	0	0	-2	-2	6	-2	0	4	4	0	0	2	6	4	0	0	6	-6	0	6	4	0	-4	-2	-2	-2	-2	-2	-2	-4	4	
4	0	0	-4	0	0	0	-8	-4	-4	-2	2	2	2	2	-6	2	0	0	0	0	-4	0	-4	0	-2	-2	0	110	0	2	2	0	
5	0	0	4	0	4	-4	0	-4	-6	0	2	2	2	-6	2	2	6	-6	6	6	6	2	2	2	4	-8	4	4	4	0	-4	-4	
6	0	0	0	-6	2	2	-8	0	-6	0	0	0	0	-8	6	0	2	0	0	0	4	4	-6	0	4	-4	110	0	110	0	0	0	
7	0	0	0	-2	2	2	0	0	0	0	0	-8	12	4	2	2	0	0	4	-6	2	2	-4	0	2	2	-4	0	-4	0	0	2	
8	0	0	0	-2	-4	0	6	2	4	0	-6	6	0	0	0	0	0	0	0	0	2	-8	4	2	2	0	12	-6	-6	0	-8		
9	0	0	0	2	2	4	0	2	-8	4	2	6	0	0	0	6	8	4	2	0	4	2	2	0	-8	2	2	0	4	2	-6	0	
10	0	0	0	-4	-2	0	2	2	-4	-4	-4	-8	0	-6	2	2	4	0	0	0	0	10	2	2	4	0	-8	0	0	2	-2	10	
11	0	0	0	-8	4	6	-6	-2	8	0	4	8	2	-6	2	2	2	-6	6	2	4	0	8	0	0	-2	-2	2	4	4	0	0	
12	0	0	0	-2	4	0	0	-2	6	0	0	4	6	-6	4	-4	2	0	0	0	-6	2	-4	0	0	-4	0	0	0	0	-2	-6	
13	0	0	0	-6	0	4	-2	-2	14	6	-4	0	110	2	4	-4	4	-4	-6	0	4	0	-6	2	2	-2	4	0	0	0	4	4	
14	0	0	0	-16	-8	-2	2	-6	-2	-6	-2	2	4	4	4	-4	-4	-4	-4	0	0	6	-2	2	2	6	2	0	0	0	-4	-4	
15	0	0	0	-8	2	-2	2	2	2	2	2	2	-4	4	-4	4	2	-2	0	0	0	0	0	0	0	0	0	0	0	2	2	2	

# Differential distribution table for the S-box $S_8$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
0	64	10	6	10	4	10	6	10	8	10	2	10	6	10	8	10	10	10	4	10	10	16	10	12	6	10	6	10	10	8	10	4		
1	10	10	10	10	10	10	2	4	10	8	10	10	10	10	10	10	10	6	4	2	16	10	12	6	10	4	4	4	12	6	4	2		
2	10	10	10	2	10	6	10	8	10	10	16	10	10	4	6	4	10	4	10	2	4	6	10	2	8	6	8	6	10	8	4	10		
3	10	6	8	8	2	10	4	2	4	6	4	6	2	10	8	2	4	6	8	6	2	4	6	10	2	10	2	10	4	10	6	10		
4	10	10	10	10	10	6	8	10	10	6	10	10	2	4	2	10	10	6	8	6	6	6	6	6	8	8	8	2	6	10	8	6		
5	10	10	6	4	10	4	10	6	4	6	6	10	10	10	8	4	10	10	2	6	10	10	10	10	10	8	4	4	10	10	2			
6	10	4	4	6	6	4	6	4	4	4	4	10	10	8	10	2	8	6	8	10	10	10	10	10	4	8	4	10	10	10	4	4		
7	10	10	10	10	10	10	6	10	2	6	10	4	6	6	2	2	10	6	4	2	10	10	2	6	8	10	10	2	4	8	2	8	4	
8	10	10	6	10	4	2	4	2	4	4	10	2	4	10	2	10	2	10	4	2	14	4	2	8	6	10	10	8	2	6	10	10	2	
9	10	10	10	6	6	10	6	2	8	4	6	10	6	2	6	6	10	6	4	2	10	2	10	2	10	4	10	4	10	4	10	2	6	
10	10	6	2	6	8	4	4	10	6	6	4	10	6	6	10	4	8	4	4	2	4	2	10	6	10	4	10	8	4	2	2	2	2	
11	10	10	4	2	4	6	10	4	10	10	10	2	2	6	10	4	6	8	6	6	4	6	8	10	6	10	2	4	2	4	2	2	2	
12	10	14	8	2	10	8	4	10	8	12	10	2	10	2	6	2	10	10	10	2	4	2	10	2	4	4	4	6	10	2	10	2	10	2
13	10	6	8	10	4	2	2	10	2	10	2	6	2	2	2	10	4	4	2	2	6	6	6	4	10	6	10	2	10	8	10	10	16	
14	10	2	6	8	8	10	10	2	10	10	6	10	2	4	14	6	4	10	10	10	10	4	6	4	10	2	10	10	4	2	4	6	8	
15	10	4	2	6	10	2	6	6	12	4	10	2	10	2	2	6	4	10	4	10	4	10	6	10	8	6	6	10	10	10	10	10	10	

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

# Linear distribution table for the S-box $S_8$

Out \ In	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	32	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	
14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Out \ In	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
0	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	
1	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	
2	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	
3	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	
4	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	
5	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	
6	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	
7	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	
8	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	
9	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	8	
10	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	8	9	
11	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	8	9	10	
12	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	8	9	10	11	
13	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	8	9	10	11	12	
14	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	8	9	10	11	12	13	
15	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15