Differential Cryptanalysis

Çetin Kaya Koç

Oregon State University

Differential cryptanalysis is a method for breaking certain classes of cryptosystems

It was invented in 1990 by Israeli researchers **Eli Biham** and **Adi Shamir**

However, apparently the IBM researchers who designed DES knew about differential cryptanalysis, as was indicated by **Don Coppersmith** of TJ Watson Research Center

Differential cryptanalysis is efficient when the cryptanalyst can choose plaintexts and obtain ciphertexts (chosen plaintext cryptanalysis)

The known plaintext differential cryptanalysis is also possible, however, often the size of the known text pairs is very large

The method searches for plaintext, ciphertext pairs whose **difference** is constant, and investigates the differential behavior of the cryptosystem

The difference of two elements P_1 and P_2 is defined as $P_1 \oplus P_2$ (bit-wise XOR operation) for DES

The difference may be defined differently if the method is applied to some other cryptosystem

Differential cryptanalysis is applicable to the iterated ciphers with a weak round function (so-called Feistel ciphers)

The summary of the technique:

- Observe the difference between the two ciphertexts as a function of the difference between the corresponding plaintexts

- Find the highest probability differential input (called **characteristic**) which can be traced through several rounds

- Assign probabilities to the keys and locate the most probable key

Notation

- P denotes plaintext, T denotes ciphertext

- (P, P^*) is a pair of plaintexts which XOR to a specific value P', i.e., $P' = P \oplus P^*$

- (T, T^*) is a pair of ciphertexts which XOR to a specific value T', i.e., $T' = T \oplus T^*$

- Primed values are always differential: P', T', a', A', etc. For example, $a' = a \oplus a^*$

DES (DEA):
Data Encryption Standard (Algorithm)

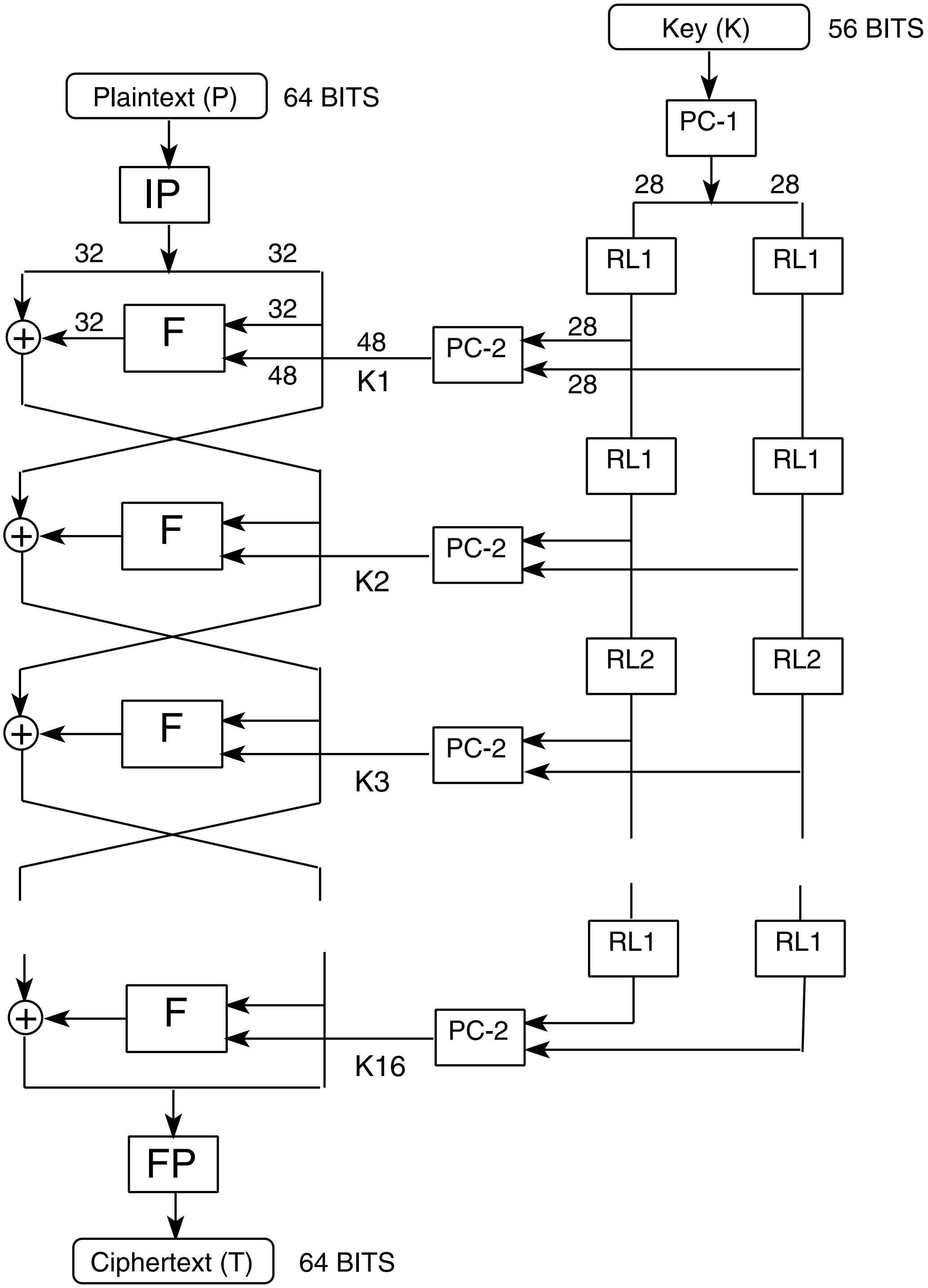
DES was designed by a group at IBM TJ Watson Research Center at the request of the US NIST for the protection of sensitive unclassified data

DES has become a US federal standard in 1976 to be reviewed every 5 years. It was reaffirmed in 1987. In 1992, after some controversy, it was recertified for another 5 years.

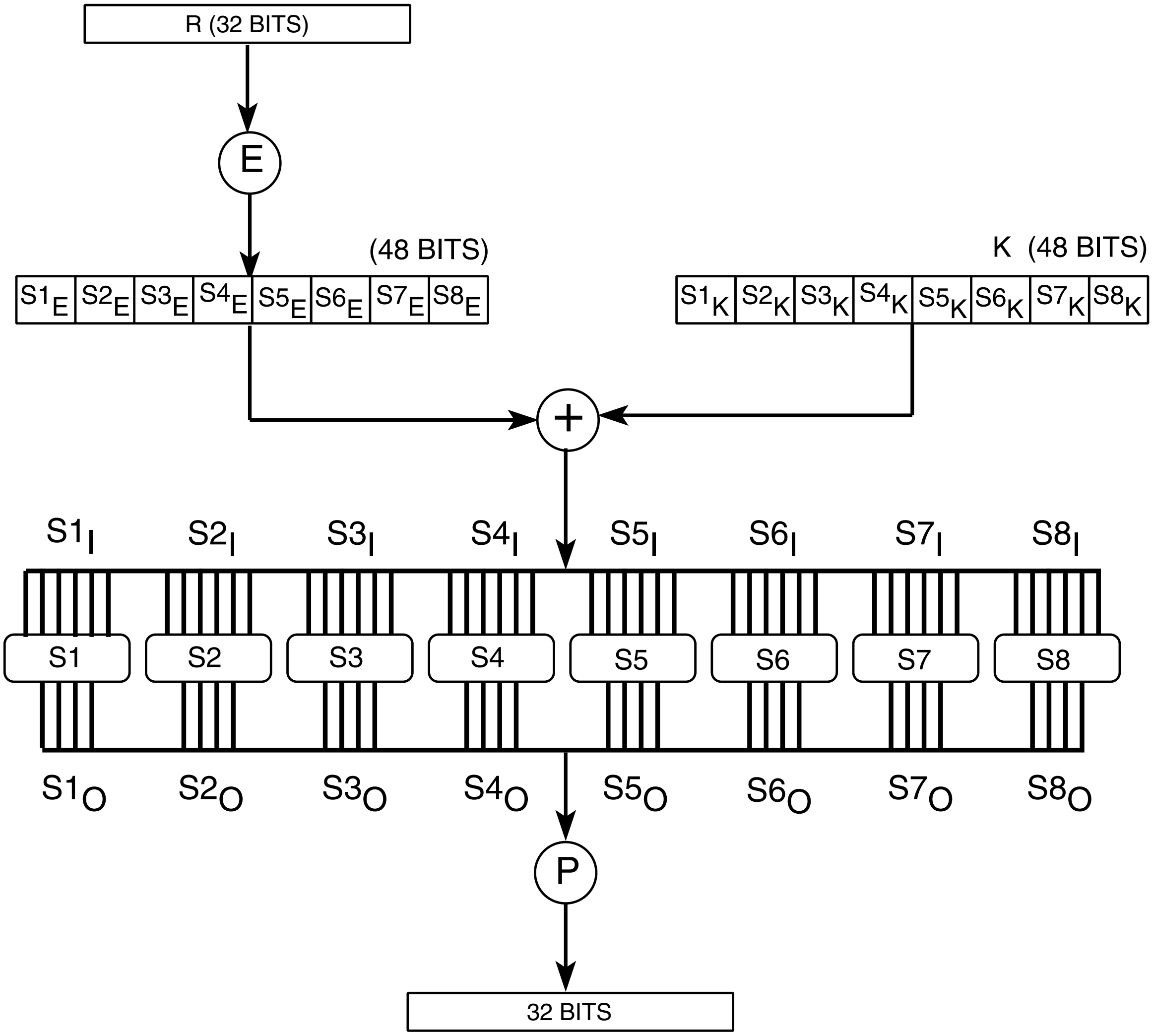
DES is a block cipher operating on a 64-bit plaintext to produce a 64-bit ciphertext with a key size of 56 bits

The fundamental building block is a substitution followed by a permutation on the text, based on the key. This is called a **round** function. DES has 16 rounds.

Outline of DES



The round function of DES


R (32 BITS)
E
(48 BITS)
S1E S2E S3E S4E S5E S6E S7E S8E
K (48 BITS)
S1K S2K S3K S4K S5K S6K S7K S8K
+
S1I S2I S3I S4I S5I S6I S7I S8I
S1 S2 S3 S4 S5 S6 S7 S8
S1O S2O S3O S4O S5O S6O S7O S8O
P
32 BITS

The Expansion 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

Differential Cryptanalysis of DES

A cryptosystem should be a good pseudorandom generator in order to foil key clustering attacks

DES was designed so that all distributions are as uniform as possible

For example, changing 1 bit of the plaintext or the key causes the ciphertext to change in approximately 32 of its 64 bits in a seemingly unpredictable and random manner

Biham and Shamir observed that with a fixed key, the **differential behavior** of DES does **not exhibit pseudorandomness**

If we fix the XOR of two plaintexts P and P^* at P' then T' (which is equal to $T \oplus T^*$) is **not uniformly distributed**

In contrast, the XOR of two uniformly distributed random numbers would itself be uniformly distributed

S-box Non-Differential Uniformity

If the input to an S-box is a uniformly distributed random number, its output will be a uniformly distributed random number

$S1$

E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

Assuming the 56-bit key is chosen according to a uniform probability distribution, the input to any S-box in any round will be uniformly distributed over all 64 possible values

The output of any S-box in any round therefore also uniformly distributed over its 16 possible values (0 to F) since each occurs 4 times in the S-box, once in each row

S-box Differential Non-Uniformity

Consider the differential behavior of an S-box, in which there are $64^2 = 4,096$ possible input pairs (x, x^*)

As the 6-bit quantities x, x^*, and $x' = x \oplus x^*$ each vary over their 64 possible values, the 4-bit quantities $y = S(x)$, $y^* = S(x^*)$, and $y' = y \oplus y^* = S(x) \oplus S(x^*)$ each vary over their 16 possible values

The distribution on the differential output y' can be computed for each of the eight S-boxes by counting the number of times each value y' occurs as (x, x^*) varies over its 4,096 possible values

$S1$ **Differential Distribution Table**

Input	Output y'															
x'	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
02	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
03	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
⋮																
0C	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
⋮																
34	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
⋮																
3E	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
3F	4	4	4	2	4	0	2	4	4	2	4	8	8	6	2	2

The 6-bit differential input x' takes 64 values: 00 (hex) to 3F (hex)

The 4-bit differential output y' takes 16 values: 0 (hex) to F (hex)

Each row sums to 64 because each differential input x' occurs for 64 of the 4,096 (x, x^*) pairs

The first row has zeros in all but the first column, because when $x' = x \oplus x^* = 0$, the same input occurs twice. Therefore, the same output must also occur both times and $y' = y \oplus y^* = 0$

The later rows are more interesting:

For example, when $x' = 01$, five of the sixteen possible y' values 0, 1, 2, 4, 8 occur with zero probability (i.e., never occurs)

A occurs with probability 16/64

9 and C occur with probability 10/64

This is **a highly non-uniform distribution**

This differential non-uniformity is observed in all of the S-boxes $S1, S2, \ldots, S8$

Consider the input XOR 34. The possible output XORs are

Output:	1	2	3	4	7	8	D	F
Occurs:	8	16	6	2	12	6	8	6

34 → 4 has two occurrences. These input pairs are duals: (α, β) and (β, α)

When we construct the differential distribution table for $S1$, we discover these inputs as 13 and 27

$$\begin{aligned} 13 &= 01\ 0011 \\ 27 &= 10\ 0111 \\ 13 \oplus 27 &= 11\ 0100 \\ &= 34 \\ S1(13) &= 0110 \\ S1(27) &= 0010 \\ S1(13) \oplus S1(27) &= 0100 \\ &= 4 \end{aligned}$$

List of possible input values for $S1$ box with input XOR 34

34 → 1: 03, 0F, 1E, 1F, 2A, 2B, 37, 3B

34 → 2: 04, 05, 0E, 11, 12, 14, 1A, 1B, 20, 25, 26, 2E, 2F, 30, 31, 3A

34 → 3: 01, 02, 15, 21, 35, 36

34 → 4: 13, 27

34 → 7: 00, 08, 0D, 17, 18, 1D, 23, 29, 2C, 34, 39, 3C

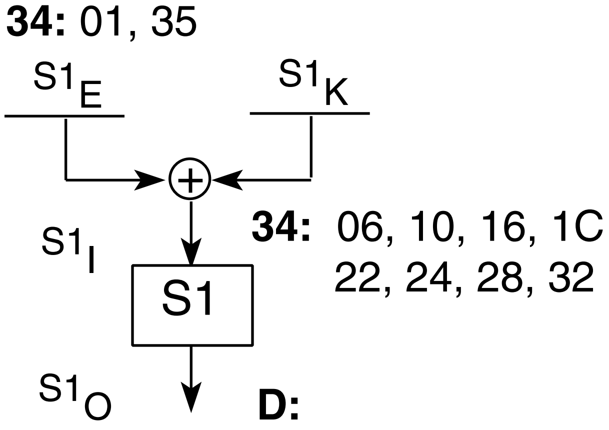
34 → 8: 09, 0C, 19, 2D, 38, 3D

34 → D: 06, 10, 16, 1C, 22, 24, 28, 32

34 → F: 07, 0A, 0B, 33, 3E, 3F

Determination of the key:

Suppose we know two inputs to $S1$ as 01 and 35 which XORs to 34, and the output XOR as D



The input XOR is 34, regardless of the value of the key because

$$\begin{aligned} S1'_I &= S1_I \oplus S1^*_I \\ &= (S1_E \oplus S1_K) \oplus (S1^*_E \oplus S1_K) \\ &= S1_E \oplus S1^*_E \\ &= S1'_E \end{aligned}$$

Also since

$$S1_I = S1_E \oplus S1_K$$

we have

$$S1_K = S1_I \oplus S1_E$$

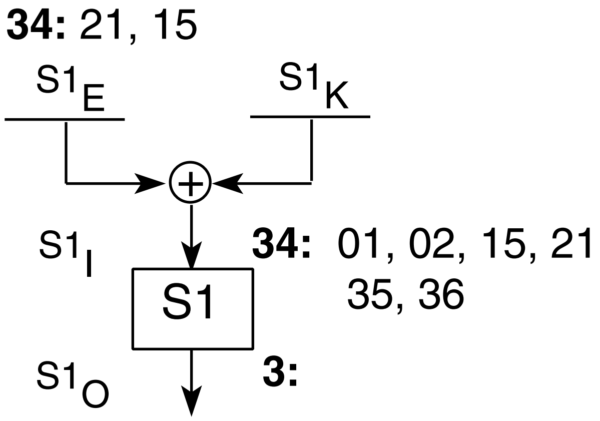
which gives

$$\begin{array}{rcl@{\qquad}rcl}
06 \oplus 01 & = & 07 & 06 \oplus 35 & = & 33 \\
10 \oplus 01 & = & 11 & 10 \oplus 35 & = & 25 \\
16 \oplus 01 & = & 17 & 16 \oplus 35 & = & 23 \\
1C \oplus 01 & = & 1D & 1C \oplus 35 & = & 29 \\
22 \oplus 01 & = & 23 & 22 \oplus 35 & = & 17 \\
24 \oplus 01 & = & 25 & 24 \oplus 35 & = & 11 \\
28 \oplus 01 & = & 29 & 28 \oplus 35 & = & 1D \\
32 \oplus 01 & = & 33 & 32 \oplus 35 & = & 07
\end{array}$$

Thus, possible keys are:

$$\{07, 11, 17, 1D, 23, 25, 29, 33\}$$

Furthermore, suppose we know two inputs to $S1$ as 21 and 15 which XORs to 34, and the output XOR as 3



This gives the key values:

$$\begin{array}{rcl}
01 \oplus 21 & = & 20 \\
02 \oplus 21 & = & 23 \\
15 \oplus 21 & = & 34 \\
21 \oplus 21 & = & 00 \\
35 \oplus 21 & = & 14 \\
36 \oplus 21 & = & 17
\end{array}
\qquad
\begin{array}{rcl}
01 \oplus 15 & = & 14 \\
02 \oplus 15 & = & 17 \\
15 \oplus 15 & = & 00 \\
21 \oplus 15 & = & 34 \\
35 \oplus 15 & = & 29 \\
36 \oplus 15 & = & 23
\end{array}$$

as

$$\{00, 14, 17, 20, 23, 34\}$$

The correct key value must appear in both of these sets:

$$\{07, 11, 17, 1D, 23, 25, 29, 33\}$$

$$\{00, 14, 17, 20, 23, 34\}$$

Intersecting these two sets, we obtain

$$\{17, 23\}$$

Thus, the key value is either 17 or 23

In order to determine which one of these is the correct value, we need more input/output XORs

Characteristic

The differential input with the highest probability, which can be traced through several rounds

Two observations:

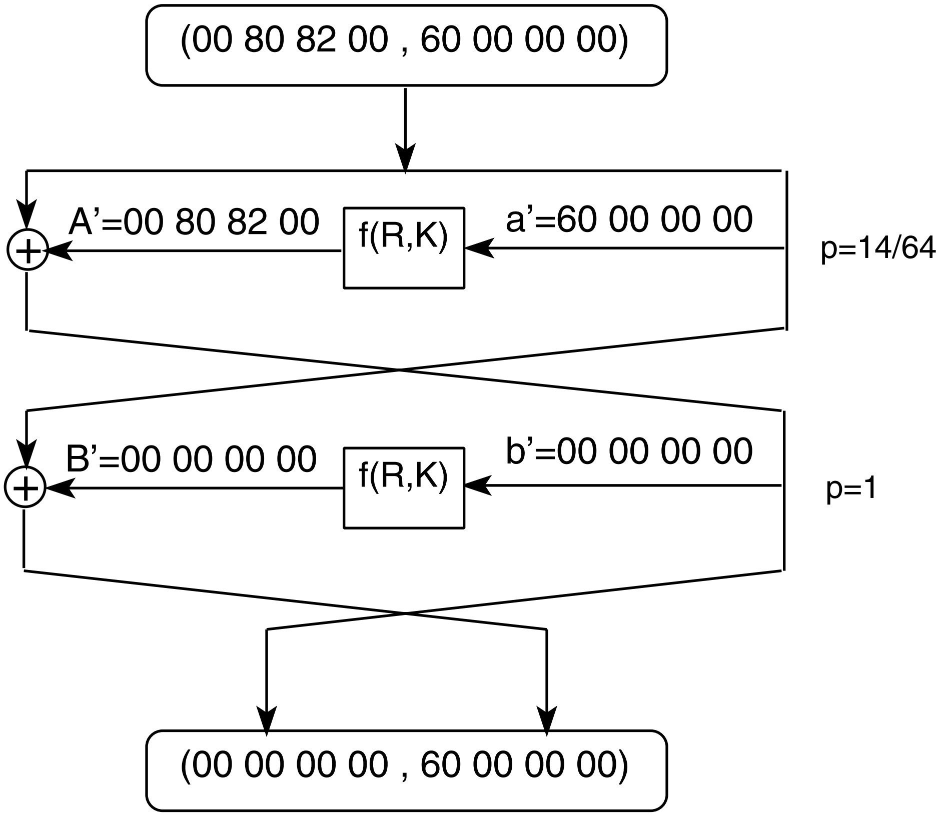
The XOR of pairs is linear in the E expansion:

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

The XOR of pairs is independent of the key:

$$\begin{aligned} S_I &= S_E \oplus S_K \\ S_I^* &= S_E^* \oplus S_K \\ S_I \oplus S_I^* &= S_E \oplus S_K \oplus S_E^* \oplus S_K \\ S_I' &= S_E \oplus S_E^* \\ S_I' &= S_E' \end{aligned}$$

A 2-Round Characteristic



The differential input to F in the first round is $a' = 60\ 00\ 00\ 00$

The expansion operation puts these half bytes into the middle four bits of each S-box in order

$6 = 0110$ goes to $S1$ and $0 = 0000$ goes to $S2, \ldots, S8$

Since all the edge bits are zero, $S1$ is the only S-box receiving non-zero differential input

$S1$'s differential input is $0\ 0110\ 0 = 0C$ while the differential inputs of $S2, \ldots, S8$ are all zero

Looking in $S1$'s differential distribution table, we find that when $x' = 0C$, the highest probability differential output y' is $E = 1110$, which occurs with probability 14/64

All the other S-boxes have $x' = 0$ and $y' = 0$ with probability 1

The S-box outputs go through the permutation P before becoming the output $f(R, K)$

As shown, the differential output of $f(R, K)$ is

$$A' = P(E0\ 00\ 00\ 00) = 00\ 80\ 82\ 00$$

$A' =$ 00 80 82 00 is then XORed with $L' =$ 00 80 82 00 to give 00 00 00 00

Thus, in the second round all S-boxes receive their differential inputs as zero, producing the differential outputs as zero

The ouput of $f(R, K)$ in the second round is zero, giving the differential output as depicted: (00 00 00 00 , 60 00 00 00)

Differential Cryptanalysis of 2-Round DES

This analysis assumes the initial (IP) and final (FP) permutations are removed from the DES algorithm

Step 1: Generate a plaintext pair (P, P^*) such that

$$P' = P \oplus P^* = \text{00 80 82 00 60 00 00 00}$$

This is done by generating a random P and XORing it with

$$\text{00 80 82 00 60 00 00 00}$$

to generate P^*

Step 2: Give the plaintext pair (P, P^*) to your opponent who enciphers it and gives you the ciphertext pair (T, T^*)
(chosen plaintext cryptanalysis)

Step 3: Compute $T' = T \oplus T^*$ and see whether it is equal to

00 00 00 00 60 00 00 00

If it does not, the characteristic has not occurred and this pair is not used. Go to Step 1 and generate a new plaintext pair.

If T' is equal to

00 00 00 00 60 00 00 00

then the characteristic has occurred, and we know the values of A' and B'. Go to Step 4.

Step 4: Since $S2, \dots, S8$ have their differential inputs equal to zero, no information can be gained about $S2_K, \dots, S8_K$

Because, in the differential distribution table of $S1$, we have $0C \to E$ with probability 14/64, only 14 of 64 possible $S1_K$ values allow

$$a' = 60\ 00\ 00\ 00$$

to produce

$$A' = 00\ 80\ 82\ 00$$

These 14 allowable values can be determined by XORing each possible $S1_K$ with the corresponding six bits of $S1_E$ and $S1^*_E$, computing $S1$'s differential output $S1'_O$ and checking if it is equal to E

Put these 14 values of $S1_K$ in a table

Step 5: Compute the intersection of these tables

Since the correct key value must occur in each table, it will be in the intersection

If more than one $S1_K$ value results, we do not have enough plaintext, ciphertext differential pairs to uniquely determine $S1_K$. Go to Step 1 and generate additional data

The number of plaintext, ciphertext differential pairs needed is approximately equal to the inverse of the probability of the characteristic used; in this case $64/14 \approx 5$ pairs are needed

If a single $S1_K$ value results, it is correct. Go to Step 6

Step 6: At this point we have recovered the 6 bits of the key comprising $S1_K$

Use similar characteristics to recover the 6 bits of key which are XORed with $S2$ through $S8$'s inputs in the first round

Step 7: At this point we have 48 bits of the key which comprise S_K, or equivalently $S1_K$ through $S8_K$

Find the remaining 8 bits of K by exhaustive search over the 64 possible values

Probabilistic Cryptanalysis

Remove Step 3 and assume that the characteristic occurs for **every** pair of encipherments

The probability of this characteristic to occur is $14/64 \cdot 1 = 14/64$

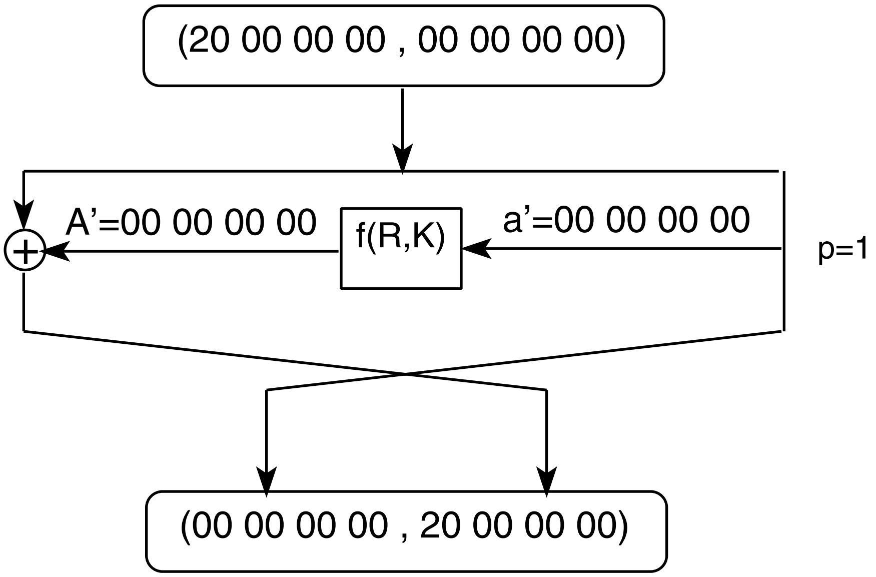
Thus, we will be **wrong** for 50/64 of the pairs

The correct value of $S1_K$ need not occur in every table and we should look for the most frequent $S1_K$ value

The correct value occurs in 14/64 of the tables and the remaining 63 values occurs with approximately equal (and smaller) probability

4-Round Differential Attack

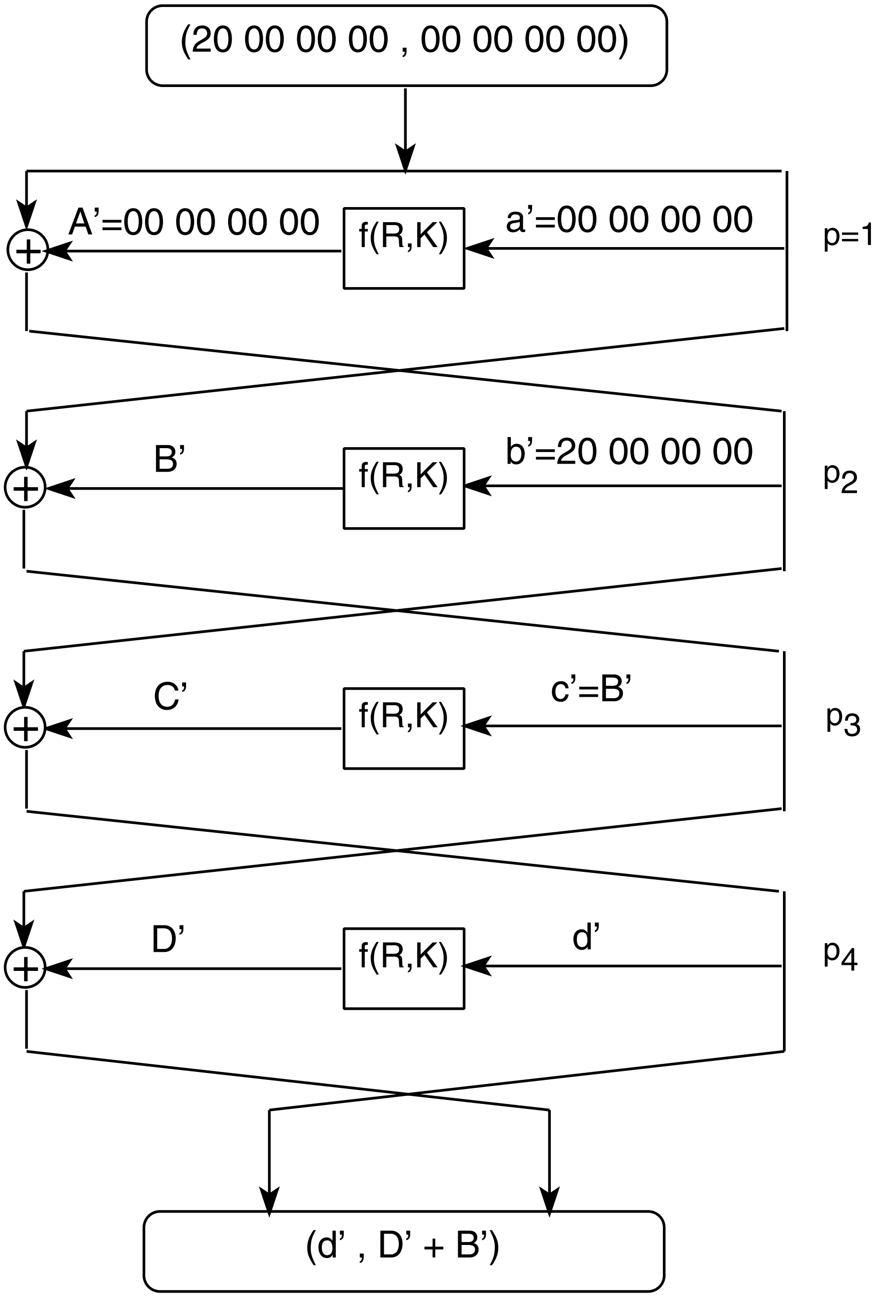
The following 1-round characteristic is used to cryptanalyze the 4-round DES



Biham and Shamir developed a method where one uses an n-round characteristic to break an $(n+3)$-round DES

They call this method a **3R attack**

Differential Cryptanalysis of 4-Round DES



Observations:

We know the inputs x and x' for all S-boxes in the last round since d and d' are the left halves of the ciphertext T and T'

To recover the 6-bit subkeys Si_K in the last round, we need to learn the differential outputs y' from some S-boxes

We know the values of d' and $D' \oplus B'$ since we know the ciphertext pair causing this characteristic

In order to get D', we need to obtain B'

Note that $b' = 20\ 00\ 00\ 00$ causes the differential inputs to $S2$ through $S8$ in the second round to be all zeros in their middle four bits

$2 = 0010$ is input to $S1$'s middle four bits and the seven zeros are inputs to $S2, S3, \ldots, S8$

The expanded edge bits that go from $S1$ to $S8$ and $S2$ are both zero; they do not disturb the zero inputs to $S2, S3, \ldots, S8$

Thus, B' have $7 \cdot 4 = 28$ zeros in its representation; the places of the zeros can be found by tracing back the permutation used at the output of $f(R, K)$

Therefore, we know 28 bits of D'

We can now obtain $6 \cdot 7 = 42$ bits of the key using our analysis technique; the remaining 14 bits can be obtained using exhaustive search

Differential Cryptanalysis of 8-Round DES

DES with 8 rounds can be broken using a 5-round characteristic

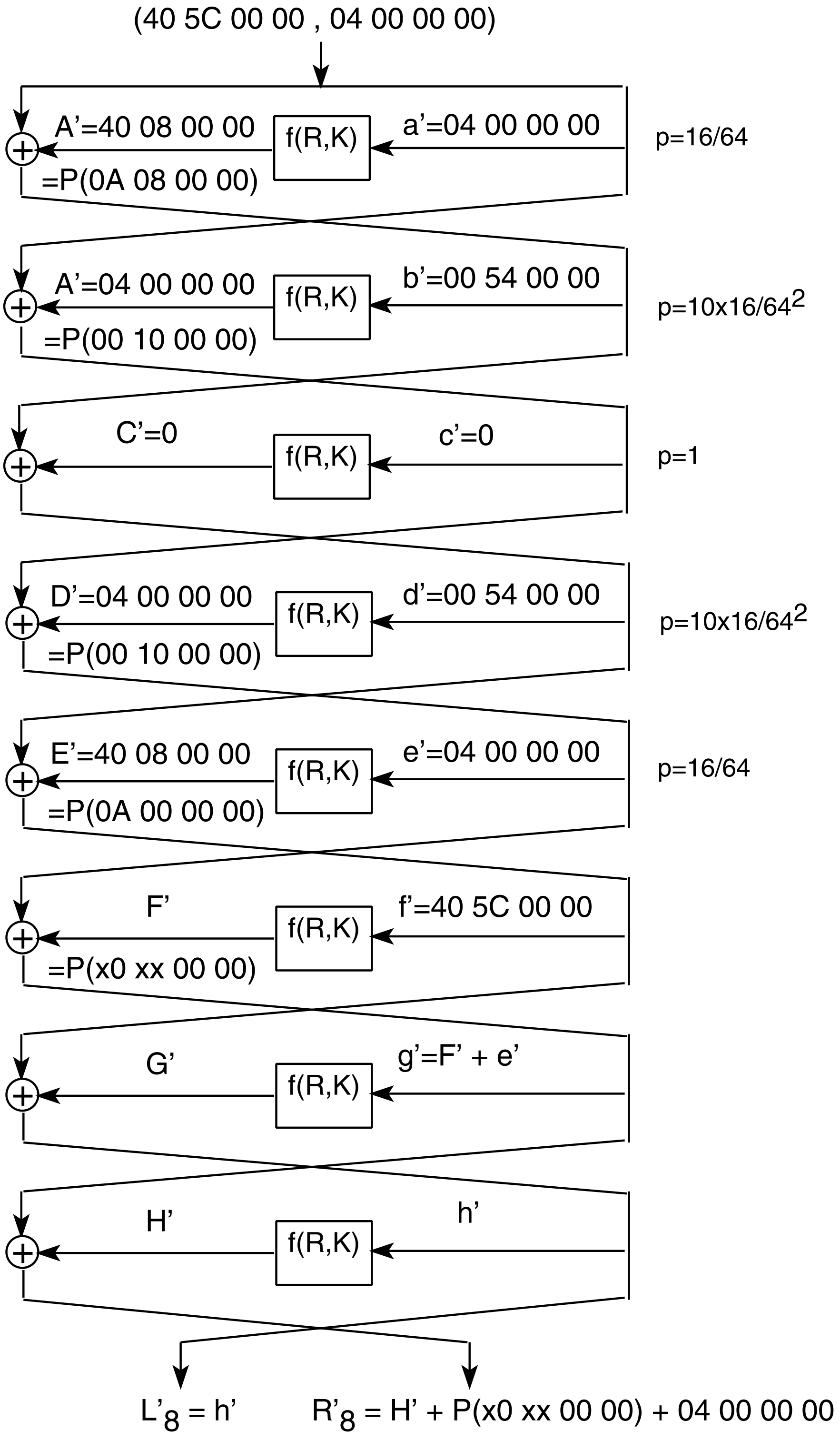
The probability of the characteristic is

$$\frac{16}{64} \cdot \frac{10 \cdot 16}{64^2} \cdot \frac{16}{64} \cdot \frac{10 \cdot 16}{64^2} \approx 9.5 \cdot 10^{-5}$$

Thus, we expect approximately 10,000 (P, P^*) pairs to be needed per occurrence of the characteristic

Since we cannot completely observe input, output XORs, we cannot guarantee that the characteristic has occurred

We assume that the characteristic occurs for every differential pair of plaintexts (P, P^*)


(40 5C 00 00 , 04 00 00 00)
A’=40 08 00 00
=P(0A 08 00 00)
f(R,K)
a’=04 00 00 00
p=16/64
A’=04 00 00 00
=P(00 10 00 00)
f(R,K)
b’=00 54 00 00
p=10x16/64^2
C’=0
f(R,K)
c’=0
p=1
D’=04 00 00 00
=P(00 10 00 00)
f(R,K)
d’=00 54 00 00
p=10x16/64^2
E’=40 08 00 00
=P(0A 00 00 00)
f(R,K)
e’=04 00 00 00
p=16/64
F’
=P(x0 xx 00 00)
f(R,K)
f’=40 5C 00 00
G’
f(R,K)
g’=F’ + e’
H’
f(R,K)
h’
L’$_8$ = h’
R’$_8$ = H’ + P(x0 xx 00 00) + 04 00 00 00

We are right only one time in 10,000; we need several times this number of differential pairs

Biham and Shamir claim that 150,000 pairs are needed

Step 1: Generate the pair (P, P^*) whose differential $P' = P \oplus P^*$ is equal to
40 5C 00 00 04 00 00 00

Step 2: Obtain the ciphertext pair (T, T^*)

Step 3: Assume the characteristic has occurred and compute the differential outputs of S2, S5, S6, S7, and S8 in the 8th round using $P^{-1}(H')$ which is equal to

$$P^{-1}(R_8' \oplus 04\ 00\ 00\ 00) \oplus (x0\ xx\ 00\ 00)$$

Step 4: Test each of the 64 possible 6-bit subkeys $K_{8,2}$ associated with $S2$ in the 8th round to see which case the observed (x, x^*) to produce the y' computed for $S2$ in Step 3

Put those subkeys that produce y' in a table $\{K_{8,2}\}$

Repeat this step to produce tables of possible subkeys $\{K_{8,5}\}$, $\{K_{8,6}\}$, $\{K_{8,7}\}$, and $\{K_{8,8}\}$ for $S5$, $S6$, $S7$, $S8$, respectively

Step 5: If any of the five tables produced in Step 4 is empty, the characteristic could not have occurred

In that case, discard all 5 tables, return to Step 1 and try a new differential plaintext pair

Step 6: If each of the 5 tables is nonempty, the characteristic may have occurred

In that case, generate all possible 30-bit portions of K_8 associated with $S2$, $S5$, $S6$, $S7$, and $S8$ by choosing one 6-bit from each table

If n_2, n_5, n_6, n_7, and n_8 denote the number of 6-bit subkeys in the tables $\{K_{8,5}\}$, $\{K_{8,6}\}$, $\{K_{8,7}\}$, and $\{K_{8,8}\}$, then the number of 30-bit values is $N = n_2 n_5 n_6 n_7 n_8$

Let $\mathcal{K}$ denote such a 30-bit value

Step 7: For each of the $\mathcal{K}$'s generated in Step 6, increment a counter corresponding to that value

If any counter reaches a count of 10, the associated $\mathcal{K}$ value is probably correct

(the value 10 is obtained using some heuristic arguments and test results suggest that it is a suitable constant)

If no counter reaches 10, return to Step 1 and generate additional differential plaintext pairs

Known-Plaintext Attack

We have assumed a chosen plaintext attack in which the cryptanalyst can obtain ciphertext of any selected plaintext

It is possible to perform a known plaintext attack by allowing the cryptanalyst to pick from a larger set of plaintext, ciphertext pairs

Suppose the chosen plaintext attack needs m pairs, and that we are given

$$2^{32}\ \sqrt{2m}$$

random plaintext, ciphertext pairs.

These form

$$\frac{(2^{32}\ \sqrt{2m})^2}{2} = 2^{64}m$$

possible pairs of plaintexts.

Each pair has an XOR. Since the block size is 64, there are 2^{64} possible plaintext XOR values, and thus there are about

$$\frac{2^{64}m}{2^{64}} = m$$

pairs creating each plaintext XOR value.

In particular, with high probability there are about m pairs with each one of the several plaintext XOR values needed for differential cryptanalysis.

Results

No. of	Find	Charac		Chosen	Known
Round	Bits	Ln	Pr	Plains	Plains
4	42	1	1	2^{4}	2^{33}
6	30	3	2^{-4}	2^{8}	2^{36}
8	30	5	$2^{-13.5}$	2^{16}	2^{40}
10	18	9	$2^{-31.5}$	2^{35}	2^{49}
16	18	15	$2^{-55.1}$	2^{58}	2^{61}

Improved with heuristics

No. of	Chosen	Known	Complexity
Round	Plaintexts	Plaintexts	
8	2^{14}	2^{38}	2^{9}
10	2^{24}	2^{43}	2^{15}
12	2^{31}	2^{47}	2^{21}
14	2^{39}	2^{51}	2^{29}
16	2^{47}	2^{55}	2^{37}

Summary of the Results

- DES reduced to 6 rounds can be broken by a chosen plaintext attack in less 0.3 seconds on a PC using 240 ciphertexts; the known plaintext version requires 2^{36} ciphertexts

- DES reduced to 8 rounds can be broken by a chosen plaintext attack in less than 2 minutes on a PC by analyzing about 2^{14} ciphertexts; the known plaintext attack needs about 2^{38} ciphertexts

- Full DES can be broken by analyzing 2^{36} ciphertexts from a larger pool of 2^{47} chosen plaintexts using 2^{37} time

- The above is true even if the keys are frequently changed and the collected data are derived from different keys

- The effort is almost independent of the key size; breaking DES with a 56-bit key requires almost the same amount of effort as breaking DES with 16 different 48-bit keys

- Differential cryptanalysis confirmed the importance of **the number of rounds** and the method by which the S-boxes are constructed

- Variations on DES turn out to be easier to cryptanalyze than the original DES; for example, GDES (Generalized DES) scheme of Schaumuller-Bich is much more easily cryptanalyzed (using only 6 ciphertexts in less than 0.2 seconds)

- Certain changes in the structure of DES may have catastrophic results:

Modified Versions of DES

Modified Operation	Chosen Plaintexts
Full DES (No change)	2^{47}
P permutation:	
Random	2^{47}
Identity	2^{19}
Order of S-boxes	2^{38}
Change XOR by Addition	2^{31}
S-boxes:	
Random	2^{21}
Random Permutation	$2^{44} \sim 2^{48}$
One Entry	2^{33}
Uniform	2^{26}
Eliminate Expansion E	2^{26}
Order of E and subkey XOR	2^{44}