



Cryptanalysis

Andreas Klappenecker
Texas A&M University

How secure is a cipher?

Typically, we don't know until it is too late...



Typical Attacks against Encryption Algorithms

Ciphertext only attack: The attacker knows just the encrypted messages

Known plaintext attack: The attacker has access to a collection of plaintext/ciphertext pairs

Chosen plaintext attack: The attacker can choose the plaintexts and read the ciphertexts

Chosen ciphertext attack: The attacker can select her own ciphertexts and observe the corresponding messages for them



Goal

Explain the basics of differential cryptanalysis.

In a nutshell:

Differential cryptanalysis explores relationships of the form: If the input bits x_0 , x_1 , and x_4 change, then the output bits y_0 and y_2 are changed [with probability p].



Differential Cryptanalysis

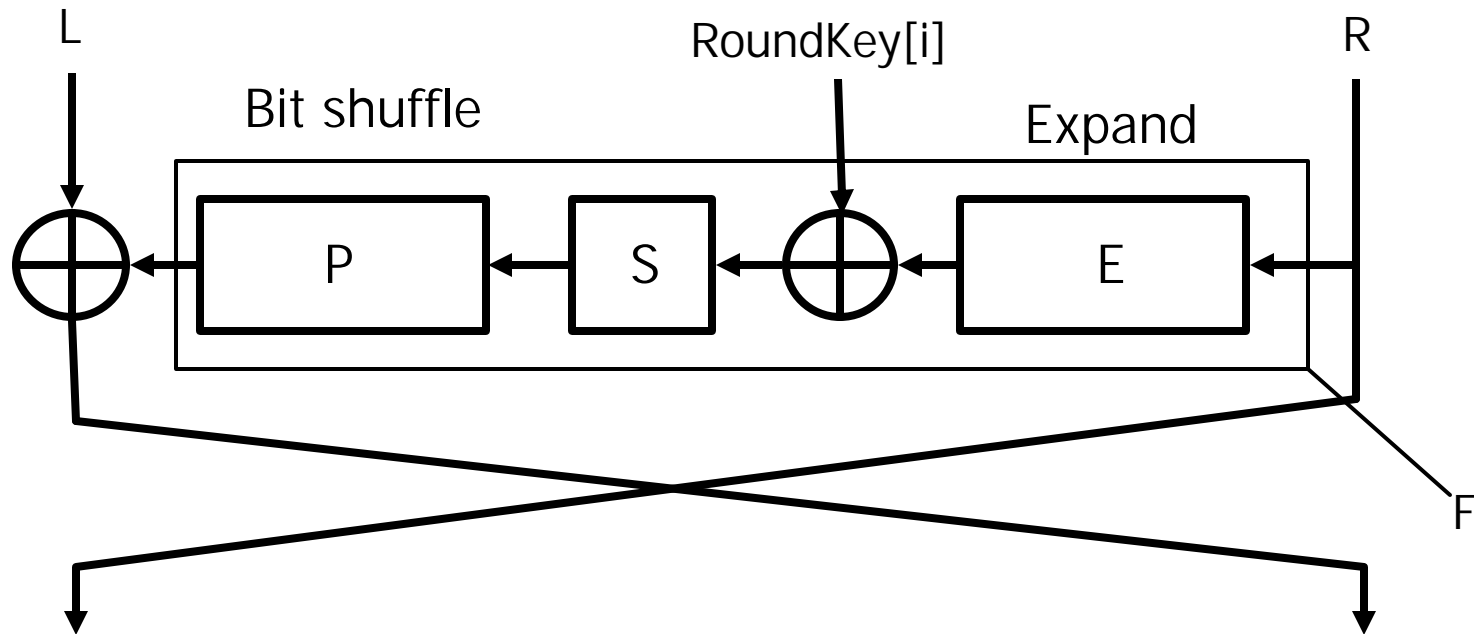
Biham and Shamir invented differential cryptanalysis in 1990, improving upon work by Murphy.

It is a chosen plaintext attack.

The attack is not necessarily practical, for instance, $2^{47.2}$ chosen plaintexts are needed to mount an attack on 16 round DES. In general, many ciphers are vulnerable to this attack.

The inventors of DES spread the rumor that they were aware of differential cryptanalysis. Supposedly, they made DES just strong enough to withstand such an attack. It is irrelevant whether or not this is true, since they did not publish these results in time.

One Round of DES



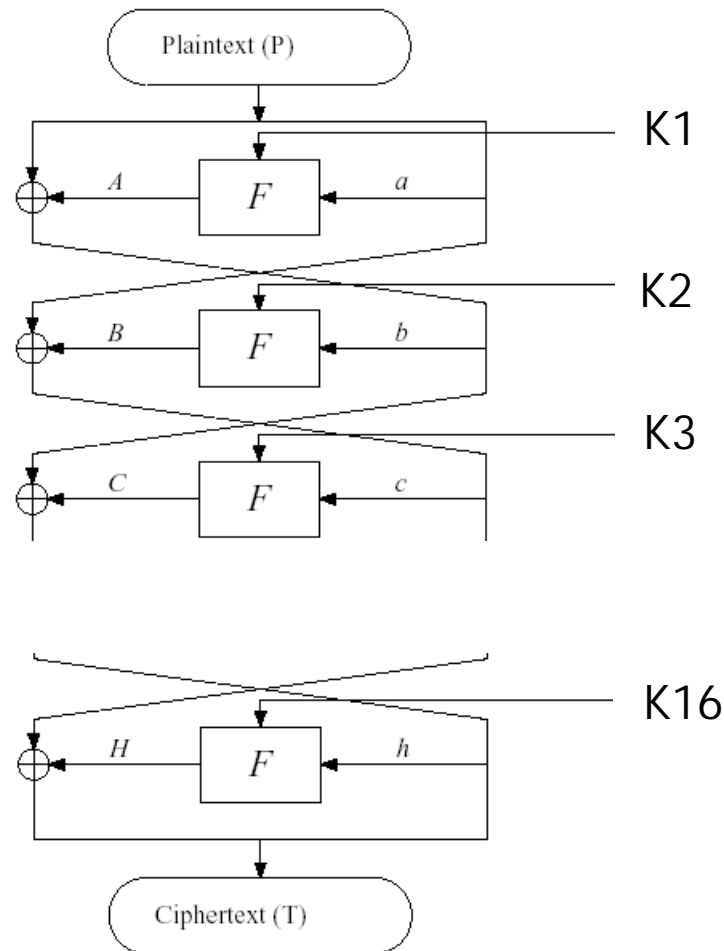
One plaintext block is 64 bits, split into two equal parts L and R. The Expand function duplicates some bits to produce 48 bits, Roundkey[i] is XORed. The S-box is a nonlinear function with 32 bits of output. These bits are shuffled before they are XORed to L.

DES repeats this operation 16 times.

Structure of DES

We omitted cryptographically irrelevant initial and final permutations.

48bit round keys are derived from one 56bit key.





Structure of DES

Take two initial message halves m_0 and m_1 . Then compute

$$m_2 := f(m_1, k_1) \oplus m_0$$

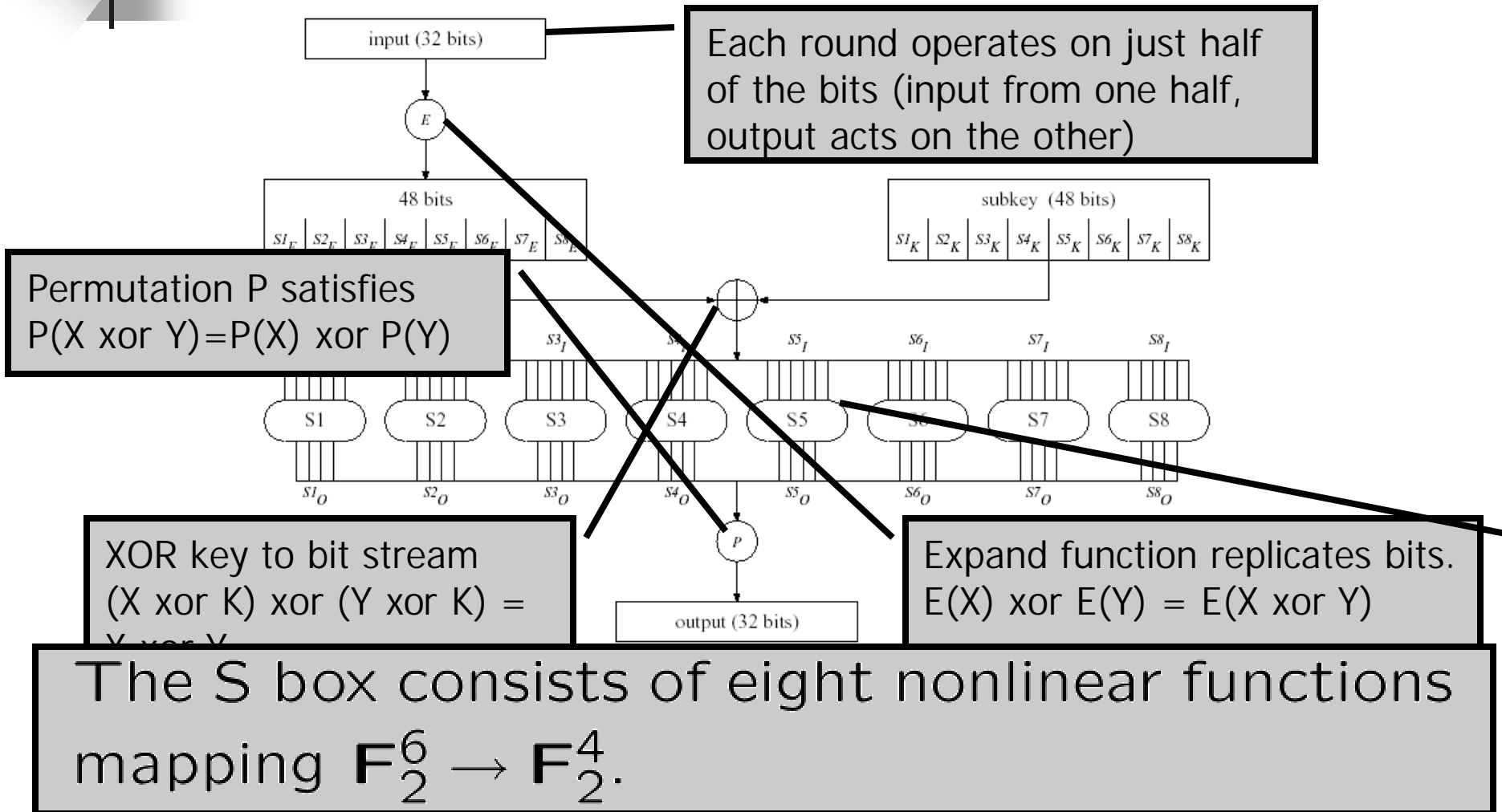
$$m_3 := f(m_2, k_2) \oplus m_1$$

\vdots

$$m_{16} := f(m_{15}, k_{15}) \oplus m_{14}$$

$$m_{17} := f(m_{16}, k_{16}) \oplus m_{15}$$

Details of one DES Round





Observations

The following functions are linear:

Expand

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

Key

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

Bit shuffle

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



Some Properties of S-Boxes

- 1) An S-box is not linear nor affine
- 2) Changing one input bit changes at least 2 output bits
- 3) $S(X)$ and $S(X \oplus 001100)$ differ in at least 2 bits
- 4) $S(X) \neq S(X \oplus 11ef00)$ for any choice of e and f

XOR Profile and S-Boxes

Distribution of input differences
and output differences

Tells you which input
bits have changed

$$D_{\delta}^{\Delta} = \left\{ \underbrace{(X, X^*)}_{\delta = X \oplus X^*} \mid \Delta = S(X) \oplus S(X^*) \right\}$$

We tabulate the size $|D_{\delta}^{\Delta}|$.

For each S-box, this is a 64×16 table

Tells you which output
bits have changed

Set of all pairs (X, X^*) that differ in the bits
set in δ and lead to output difference Δ

XOR Profile of S1

Input XOR	0 _x	1 _x	2 _x	3 _x	4 _x	5 _x	6 _x	7 _x	8 _x	9 _x	A _x	B _x	C _x	D _x	E _x	F _x
0 _x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1 _x	0	0	0	0	0	2	4	4	0	10	12	4	10	6	2	4
2 _x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3 _x	0	0	0	0	0	0	0	2	6	4	4	0	2	2	2	0
4 _x	0	0	0	0	0	0	0	0	0	4	4	0	12	2	4	6
5 _x	0	0	0	0	0	0	0	0	0	4	4	2	4	2	0	12
6 _x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
7 _x	0	0	0	0	0	0	0	0	0	6	6	4	6	2	2	0
8 _x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9 _x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A _x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B _x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C _x	0	0	0	0	0	6	6	0	0	6	6	4	6	6	2	2
D _x	0	0	0	0	4	8	2	6	0	6	4	6	0	2	0	2
E _x	0	0	0	0	6	6	4	0	6	6	4	0	0	4	0	8
F _x	0	0	0	0	4	6	4	2	4	8	2	2	2	6	8	8
									⋮							
31 _x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32 _x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33 _x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34 _x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35 _x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36 _x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37 _x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38 _x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39 _x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
3A _x	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
3B _x	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
3C _x	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
3D _x	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
3E _x	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
3F _x	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

Differential Cryptanalysis uses entries with large values, particularly 0 -> 0.

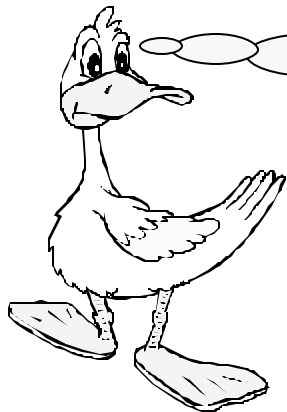
Each row sums to 64. Probability distribution for $|D_{0x34}^\Delta|/64$ is nonuniform.

14

What can we learn?

Suppose we know δ and Δ

Input to S-box must occur
in some tuples of D_δ^Δ .



Oh, right, the definition
just contained pairs of
possible inputs

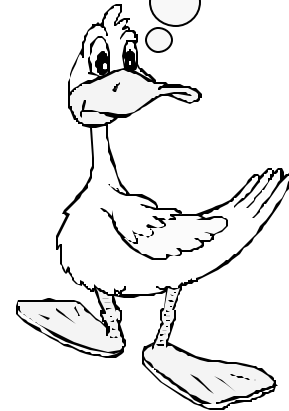
What can we learn?

So we have eight inputs.
How do they look like?

Suppose we know that
 $S1_E = 0x1$, $S1_E^* = 0x35$
 $\Delta = 0xD$

Goal Find key value $S1_K$

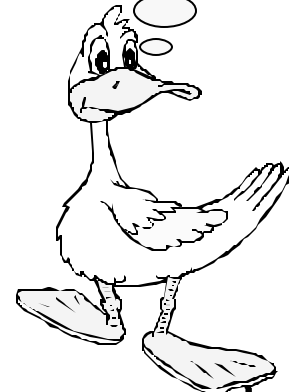
Table shows that $D_{0x34}^{0xD} = 8$



What can we learn?

OK. Now we know the input, but what about the keys?

$$D_{0x34}^{0xD} = \{ (06, 32), (10, 24), (16, 22), (1C, 28), \text{and the pairs swapped} \}$$



We have 8 possible inputs

$$\mathcal{I} = \{06, 10, 16, 1C, 22, 24, 28, 32\}$$

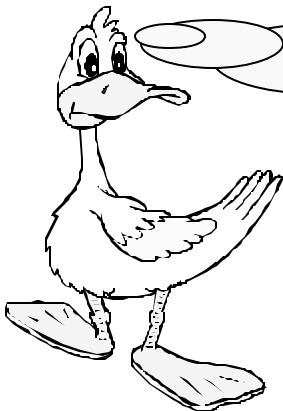
What can we learn?

Possible input values of $S1$ for $0x34 \rightarrow 0xD$
 $\mathcal{I} = \{06, 10, 16, 1C, 22, 24, 28, 32\}$

The key must be contained in

$$\begin{aligned} S1_E \oplus \mathcal{I} &= 0x01 \oplus \mathcal{I} \\ &= \{07, 11, 17, 1D, 23, 25, 29, 33\} \end{aligned}$$

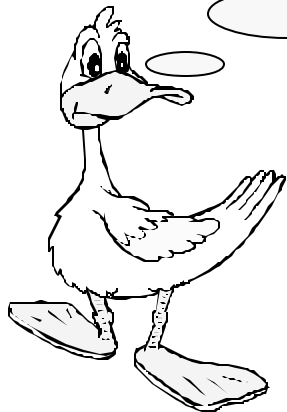
Why?



Right, the output of the expand function E is xored with the key. And this gives the input to the S-box. I get it, the input xored with the result of E gives the key,

Wait a Minute...

If this worked for one input pair, then why don't we repeat this for another one. I guess we might get a different set... Oh, and it contains the key as well...



Another Difference Pair

Suppose we know that

$$S1_E = 0x21, S1_E^* = 0x15, \Delta = 0x3$$

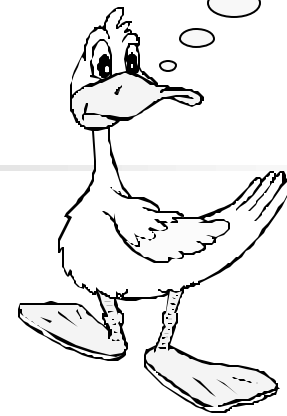
$$D_{0x34}^{0x3} = \{(01, 35), (02, 36), (15, 21), (35, 01), (36, 02), (21, 15)\}$$

Potential input and keys

$$\mathcal{I}_2 = \{01, 02, 15, 21, 35, 36\}$$

$$\mathcal{I}_2 \oplus 0x21 = \{20, 23, 34, 00, 14, 17\}$$

Putting it together



The potential keys are

$$\mathcal{I} \oplus 0x01 \cap \mathcal{I}_2 \oplus 0x21 = \{0x17, 0x23\}$$

We need a pair with another δ to discriminate between the two.



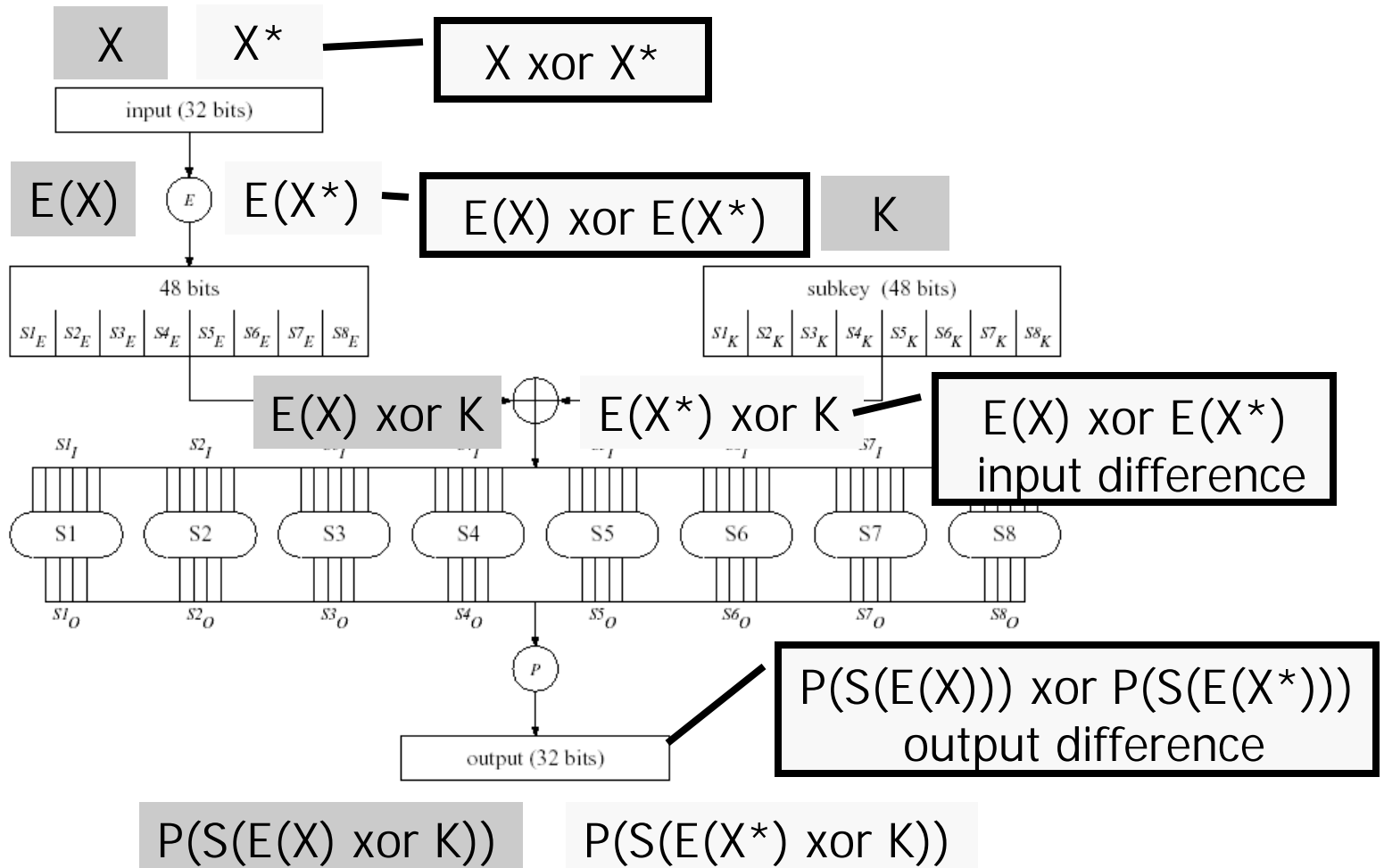
Summary of Attack on S-Box

The XOR profile D_{δ}^{Δ} does not depend on the key.

Occurrence of differences constrains the potential inputs to S-boxes.

Noting a few difference patterns allows to infer the key settings.

Review





Remarks

A single round of DES is cryptographically weak.

We can easily crack one round by looking at the differences between two encryptions.

Differential cryptanalysis explores such weaknesses.

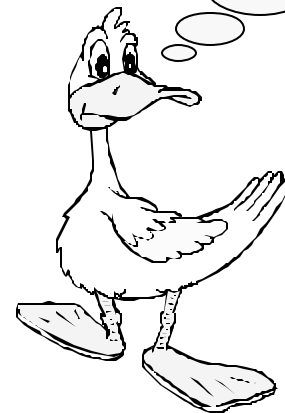
Accomplishment



3-Boxes and single
round ciphers

Overview

- Simple Attack on DES with 3 rounds
- Characteristics
- Basic Algorithm
- DES with 4 rounds



Finally, we get to see this method in action

An Attack on 3-round DES

Suppose that we have DES reduced to 3 rounds

Input difference

$P' = 0x\ 01\ 96\ 00\ 18\ 00\ 00\ 00\ 00$

Output difference

$T' = 0x\ 41\ 96\ 40\ 1A\ 48\ 00\ 00\ 00$

Cryptograms

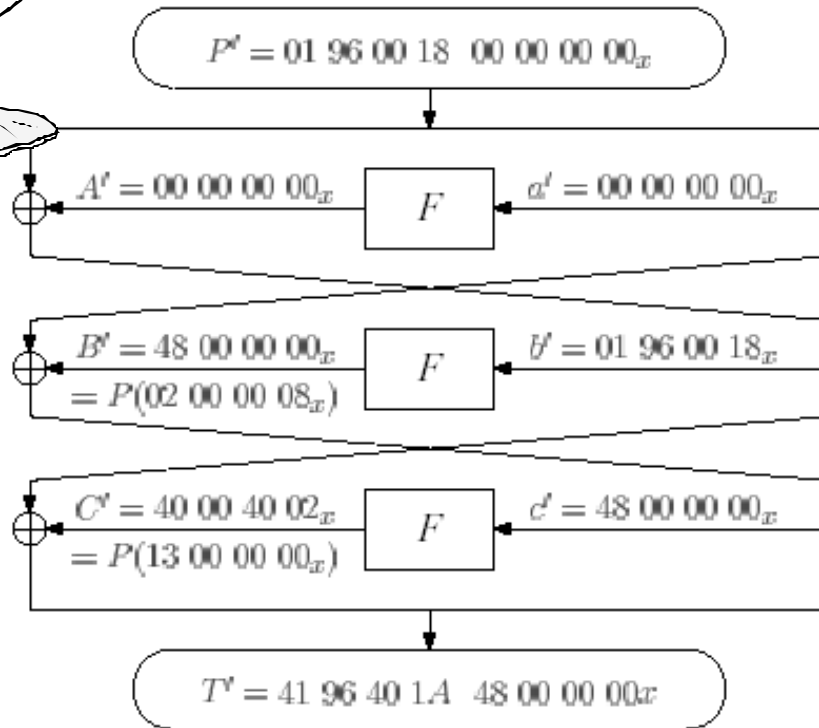
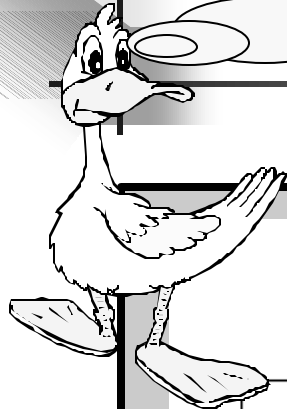
$T = 0x\ 00\ 00\ 00\ 00\ 00\ 08\ 00\ 00\ 00$

$T^* = 0x\ 41\ 96\ 40\ 1A\ 40\ 00\ 00\ 00$



So we simply look again at some differences. But how do we know that a difference has occurred in an intermediate step?

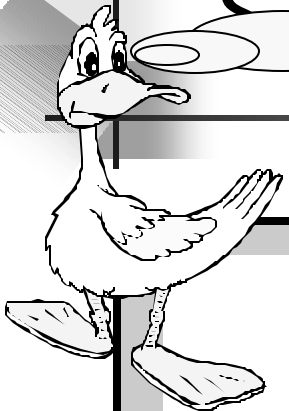
Round DES



Annotate the diagram by input/output differences, similar to our analysis of S-boxes.

A characteristic of this cipher is one particular annotation.

The differences need to be consistent with the S-box characteristics.



Aha, we know C' because the ciphertext T'_L is available, and the input to the last xor is P'_L . That was easy.

and DES

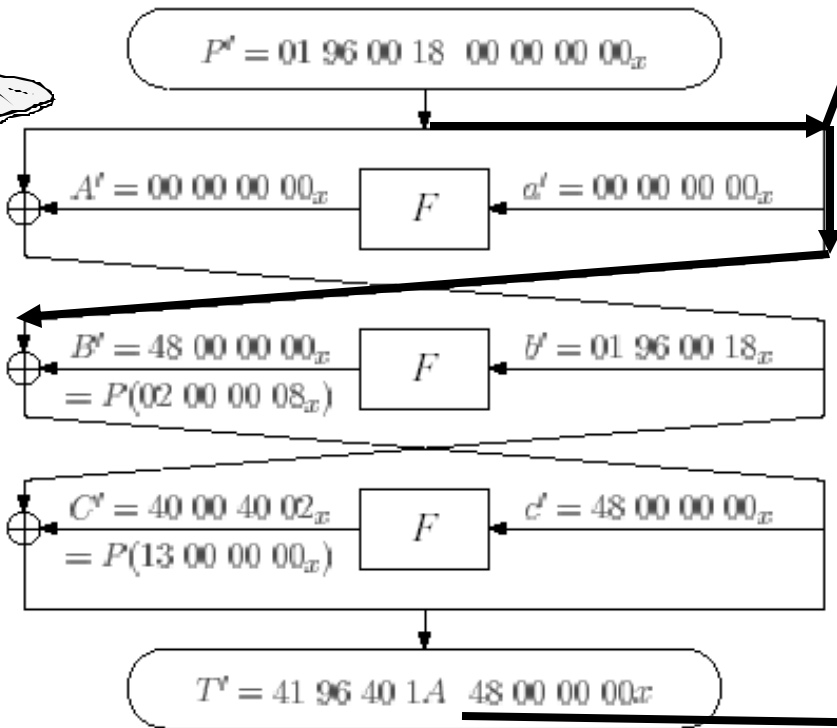
Nothing happens here. The right parts of the two plaintexts do not differ.

We look at the last round.

The S-box S1 gets the bits 32 1 2 3 4 5 as inputs, where MSB=1, LSB=32.

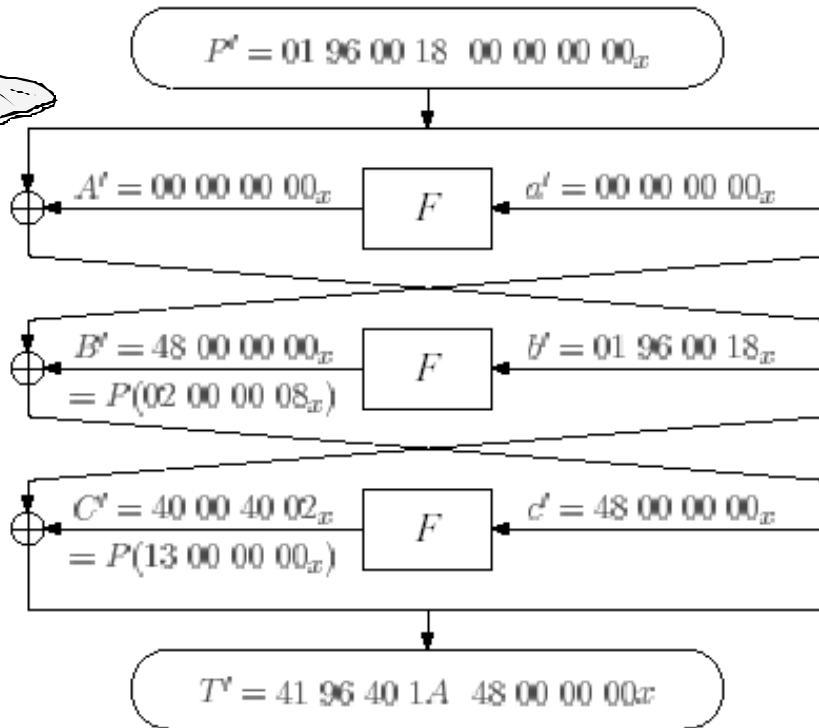
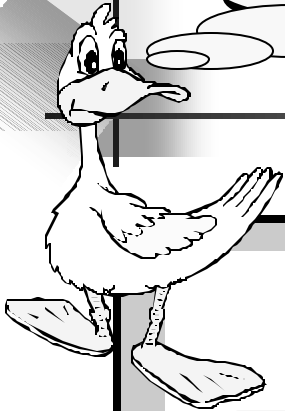
The difference $c' = 0x48\ 00\ 00\ 00$ fed into the expansion function E yields the input 0x9 for the S-box S1, and the output is 0x1.

We know c' because that is T'_R .



So this works almost like the single round scheme. But what happens if we have more rounds?

3-round DES



The input/output differences $0x9 \rightarrow 0x1$ of S1 yield

$$S1_E \text{ xor } S1_K = 0x33 \text{ or } 0x3A$$

$$S1^*_E \text{ xor } S1_K = 0x33 \text{ or } 0x3A$$

We know from the ciphertexts T and T* that

$$S1_E = 0x01$$

$$S1^*_E = 0x08$$

Hence, $S1_K = 0x32 \text{ or } 0x3B$

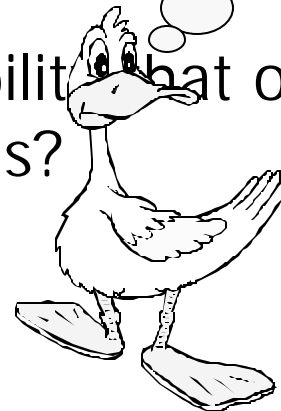
The Next Step



In a cipher with many rounds, we take a characteristics which hold more than the cipher.

We might not even be able to find the output difference. So we look at the input difference and a

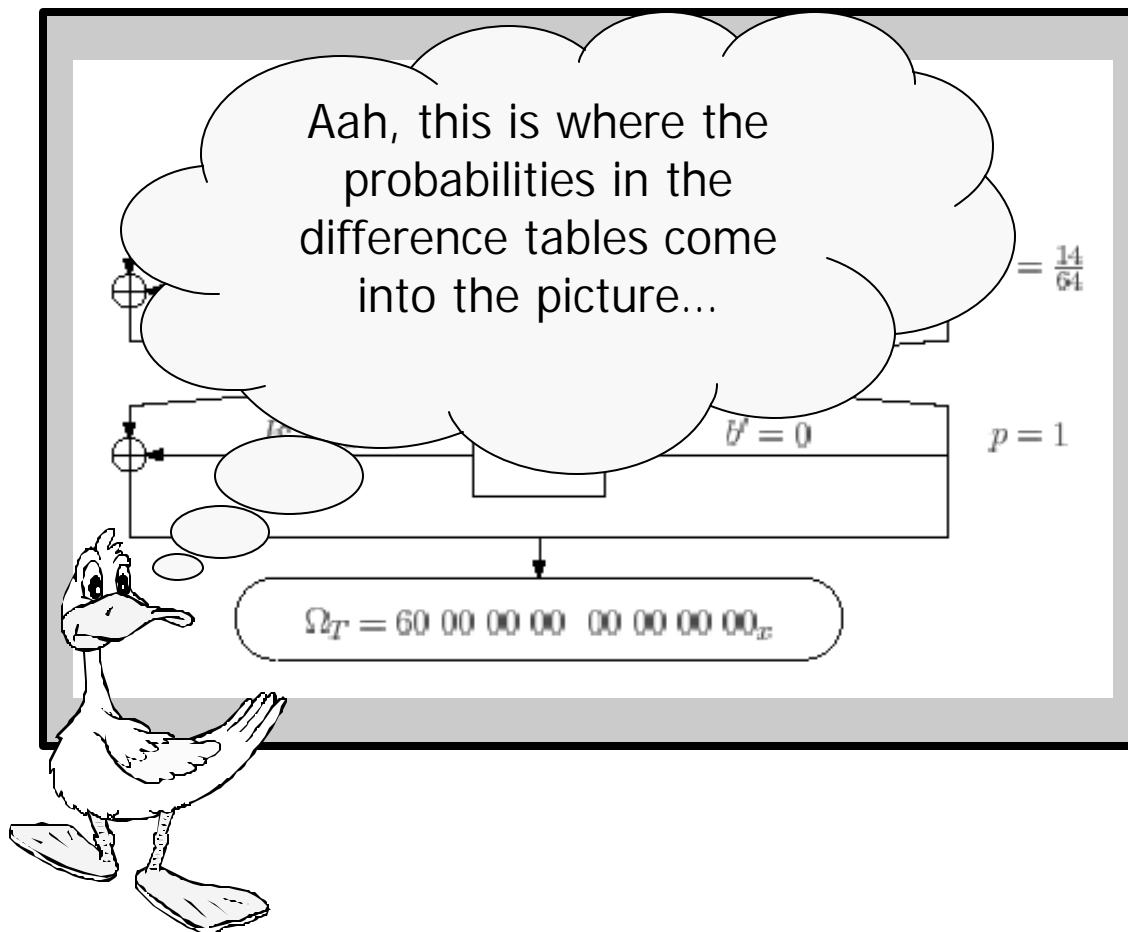
What is the probability that our characteristics holds?



"Probably", this is not as difficult as it sounds...

How about those pancakes...

Characteristics



Given the plaintext difference, we would like to know some statistical information of the differences found in intermediate rounds.

Give the characteristics some probabilities.

S1: $0xC \rightarrow 0xE$
has probability $14/64$



Characteristics

A pair P, P^* of plaintext is admissible with respect to a characteristic Ω and a key K , when Ω has input difference $\Omega_p = P \text{ xor } P^*$ and all subsequent differences are as predicted by the characteristics.

The pair is called inadmissible if it is not admissible.

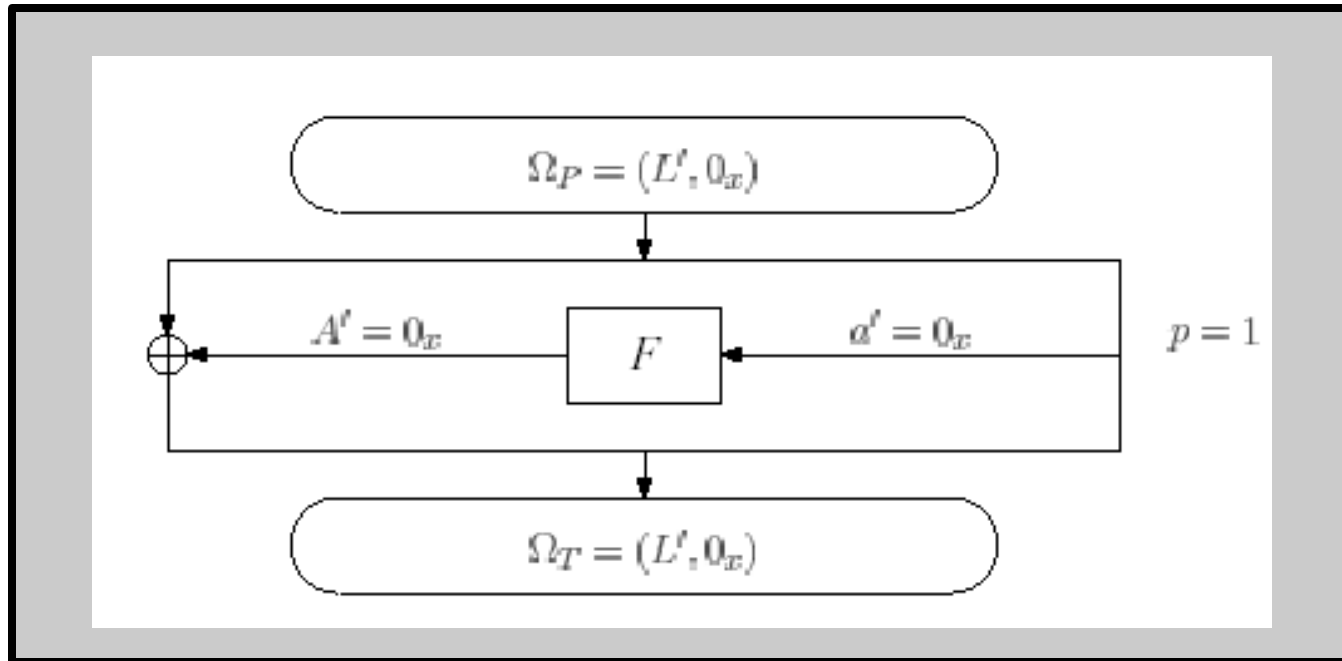
The probability of a characteristic is the probability that a random pair P, P^* with chosen input difference

$$\Omega_p = P \text{ xor } P^*$$

is an admissible pair, assuming that the round keys are chosen independently and uniformly at random.*

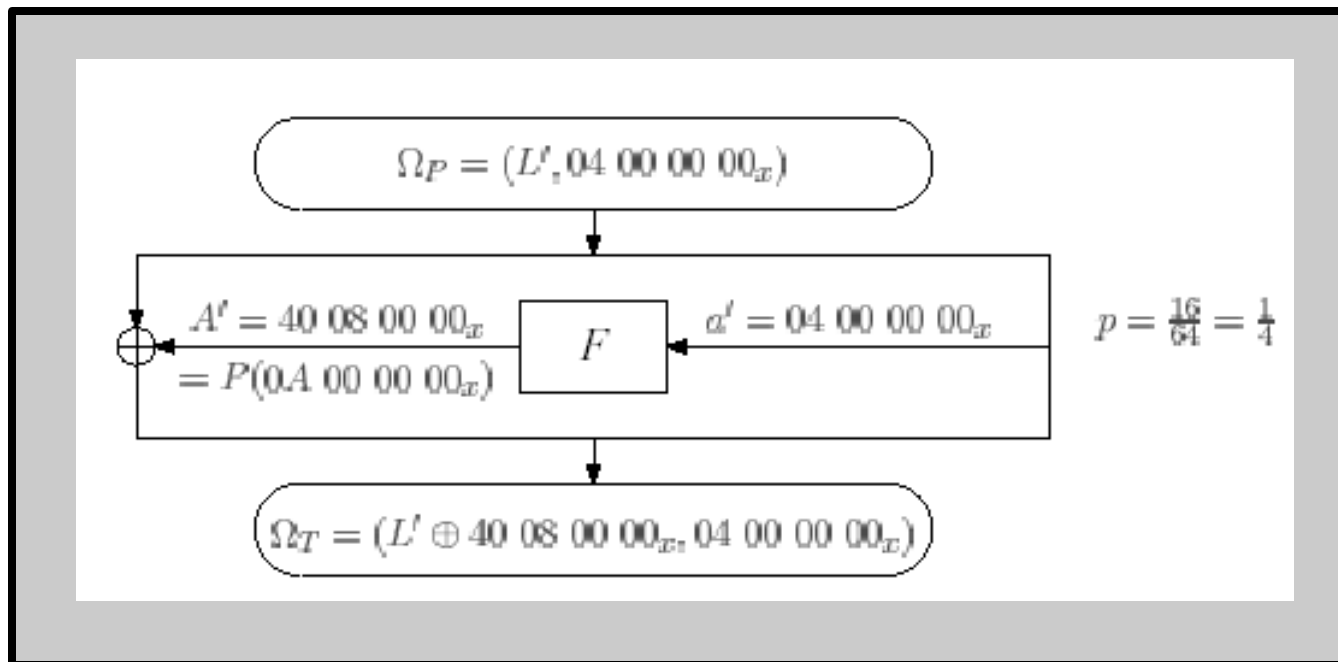
* The latter assumption is not realistic, but makes the math tractable.

Single Round Characteristics



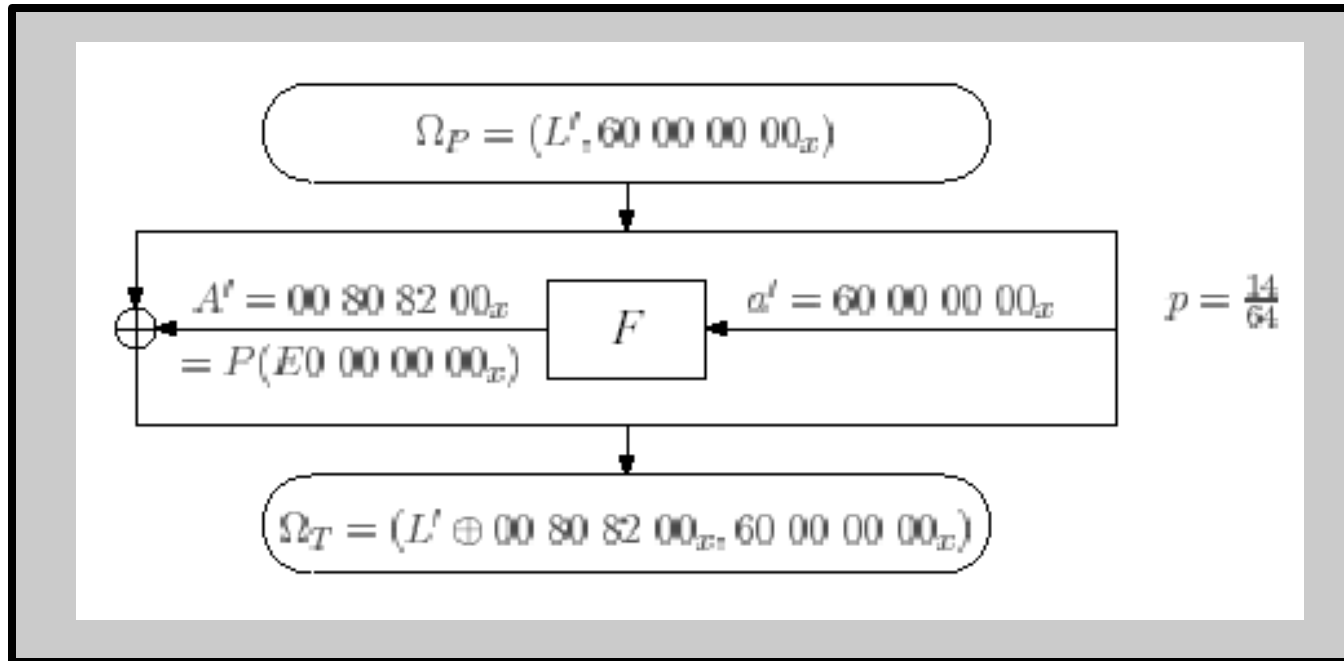
The number 0x 00000000 is always mapped to itself, yielding a characteristic with probability 1.

Another Single Round Characteristics



The second best characteristics has probability 1/4.
Only S2 is active.

Another Single Round Characteristics



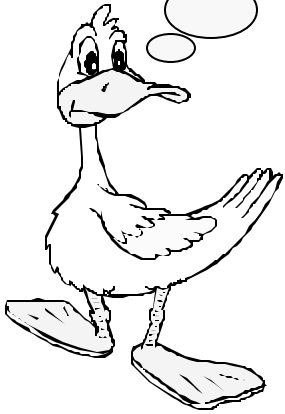
The next best characteristics has probability $14/64=21.88\%$

Problem

We cannot determine with certainty that a pair is admissible or inadmissible. That an inadmissible pair produces a difference.

So I guess set intersections cannot be used to find the key. Is there anything we can count on in this world?

It is possible that the intersection of sets with potential key settings will be empty if many pairs are used, since inadmissible pairs might not yield the key.





Solution

Remark The key occurs in all sets derived from admissible pairs. The probability that it occurs is roughly the probability of the characteristics. Incorrect keys will have a much lower probability.

Count the number of occurrences of a suggested key. The key suggested most often is likely the correct one.

Basic Algorithm

Choose $m = O(1/p)$ random pairs P, P^* such that

$$\Omega_P = P \text{ xor } P^*.$$

Compute cryptograms T, T^* under the unknown key K .

Keep the pairs satisfying $\Omega_T = T \text{ xor } T^*$, discard others.
The expected number of remaining pairs is about

$$m(p + 1/2^{64})$$

where mp is the expected number of admissible pairs,
and $m/2^{64}$ are the expected number of inadmissible
pairs that happen to yield Ω_T



Basic Algorithm II

For a pair of such cryptograms T and T^* with desired output difference $\Omega_T = T \text{ xor } T^*$, find values of the last roundkey.

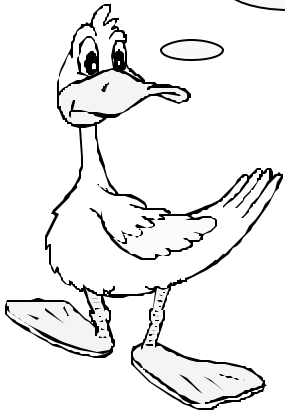
Add one to the count of appearances of each such value of the round key.

After m messages have been tested, then we take those key values that have been suggested most often.

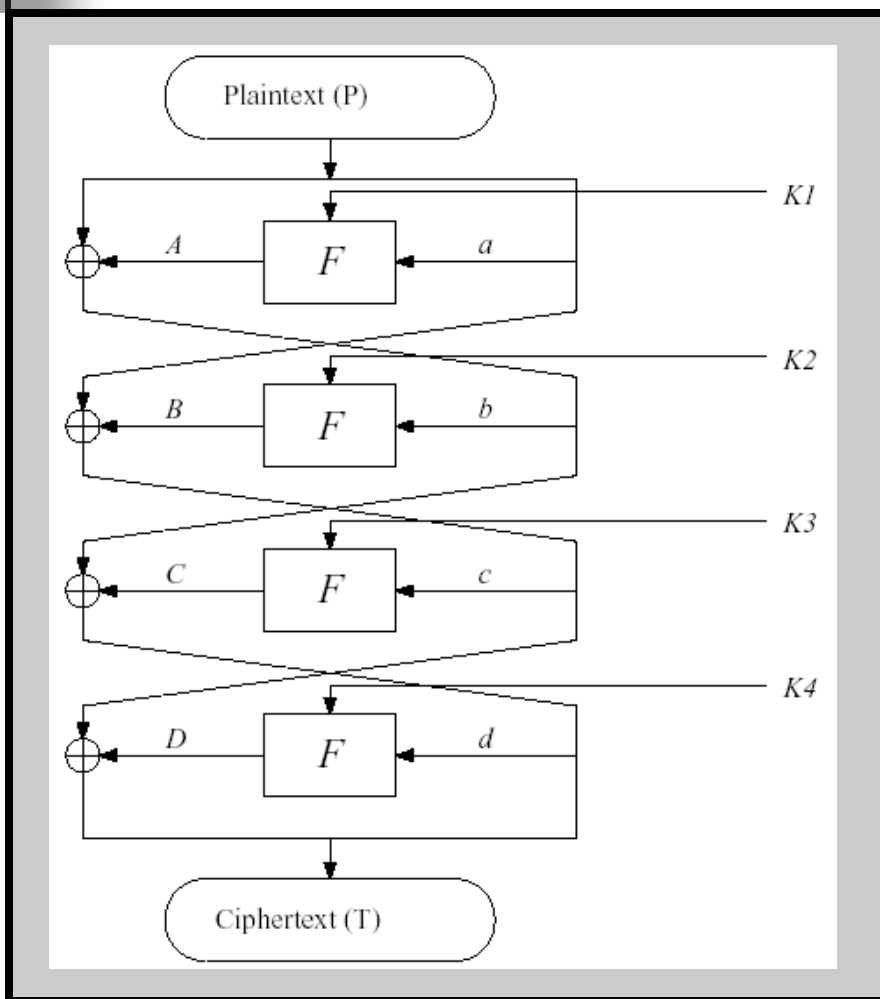
[Sometimes there will remain several possibilities that we have to be tested.]

Failures

If $p \gg 1/2^{64}$ then we will likely get admissible pairs. But what if that does not hold?



Four Round DES

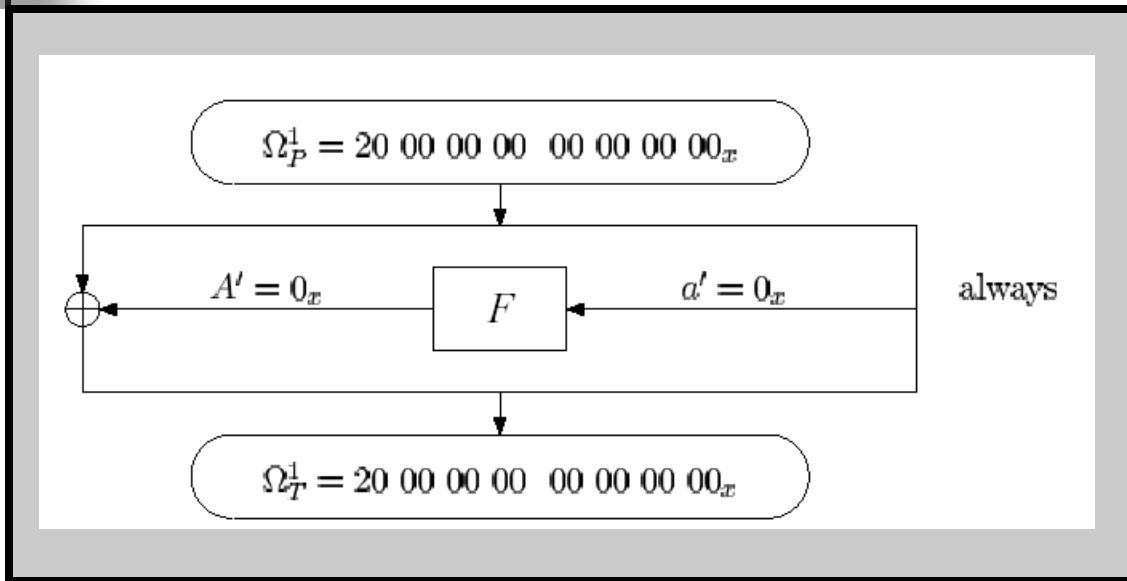


Use a characteristic with input difference $(L,0)$ in the first round, where L has just one bit set.

This is a single round characteristics with probability 1.

We use a so-called 3R attack that extends three rounds beyond this characteristic.

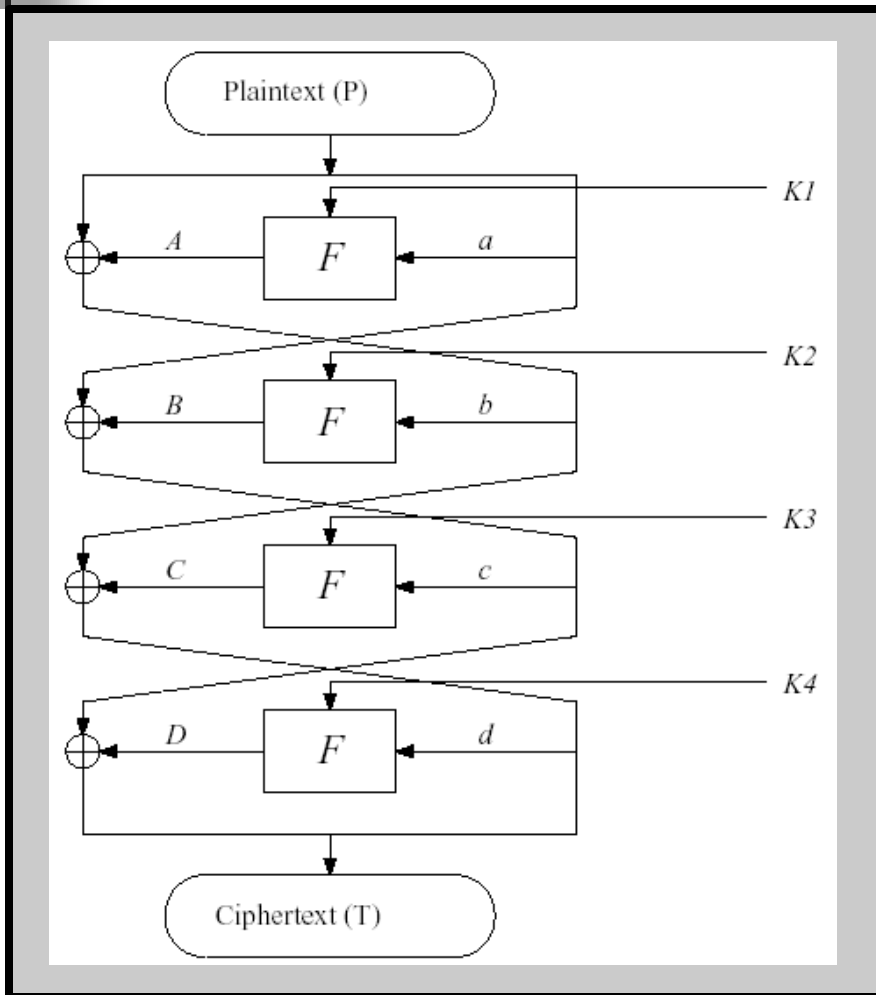
The First Round



The single bit difference plays a role in the second round in S1.

The input differences of S2,...,S8 in the second round is 0.

Four Round DES



The output difference of $S2, \dots, S8$ in B' is 0 since their input difference is 0.

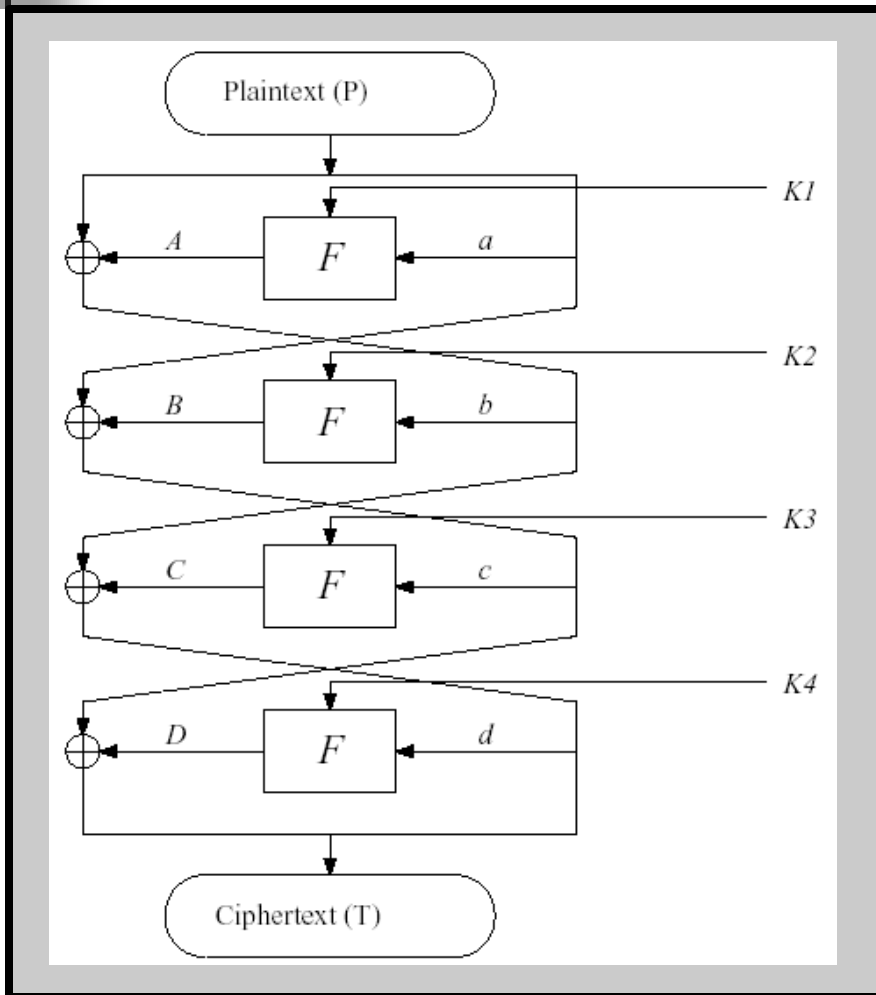
$$a' \text{ xor } B' = c' = D' \text{ xor } T'_L$$

$$\text{Hence } D' = a' \text{ xor } B' \text{ xor } T'_L$$

But $d' = T'_R$ is known.

We know a' , T'_L and 28 bits of B' , hence we know 28 bits of D' .

Four Round DES



These 28 known bits of D' are the output XORs of the S-boxes S_2, \dots, S_8 .

We know S_{Ed}, S_{Ed}^* from the ciphertexts T_R and T_R^* and S_{Od} of seven S-boxes.

Given the encrypted pairs, we use a separate counting procedure for each of the seven S-boxes.

Four Round DES

Try all 64 key values of S_{Kd} and check

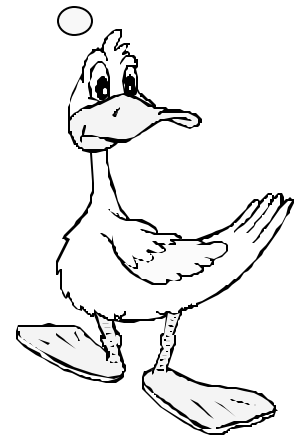
$$S_{Id} = S_{Ed} \text{ xor } S_{Kd}$$

$$S_{Id}^* = S_{Ed}^* \text{ xor } S_{Kd}^*$$

$$\text{yield } S_{Od}' = S_{Od} \text{ xor } S_{Od}^*$$

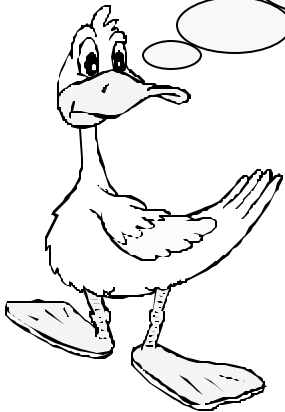
For each key, we count the number of pairs for which the test succeeds. The correct value is suggested by all pairs since the characteristic has probability 1, so each pair is admissible.

So the wrong 63 key values will occur less often, because they are not suggested by all pairs.



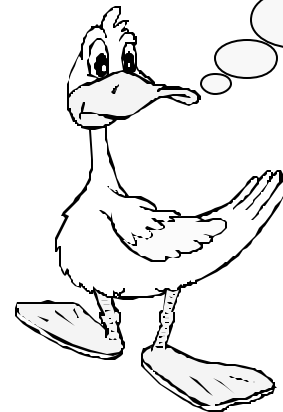
Con Fuocco

We get $7 \cdot 6 = 42$ bits of the last round key. These are 42 bits of the actual 56 bit key. So trial and error with the remaining 2^{14} possibilities cracks the cipher...



Beyond Differential Cryptanalysis

- Conditional characteristics
- Higher order differential cryptanalysis
- Truncated differentials
- Impossible differentials
- Boomerang, rectangle attacks
- Linear cryptanalysis



We never came
back to those
pan cakes...



References

Eli Biham, Adi Shamir: *Differential Cryptanalysis of DES-like Cryptosystems*, Crypto '90

<http://www.cs.technion.ac.il/~biham/Reports/Weizmann/cs90-16.ps.gz>

A thorough exposition of differential cryptanalysis. This paper contains all the details that we have omitted in our presentation. You should study the more elaborate examples so that you get exposed to all features of this method.



References

Xuejia Lai, James Massey, Sean Murphy: *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology - EUROCRYPT '91.

http://www.isi.ee.ethz.ch/archive/publications/massey_cd/pdf/BI320.pdf

An excellent exposition of differential cryptanalysis. The probabilistic aspects of the method are treated more thoroughly than in the original papers.