Miss in the middle

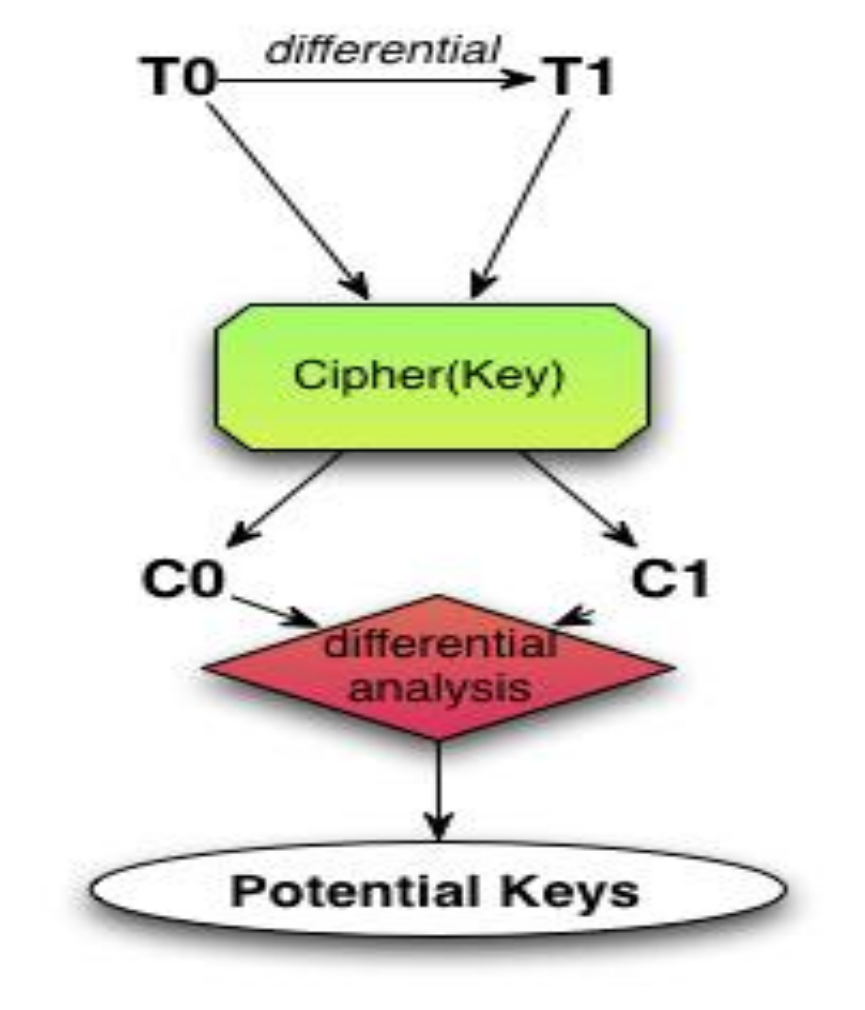
By: Gal Leonard Keret

Miss in the Middle Attacks on IDEA, Khufu and Khafre

- Written by:
  - Prof. Eli Biham.
  - Prof. Alex Biryukov.
  - Prof. Adi Shamir.

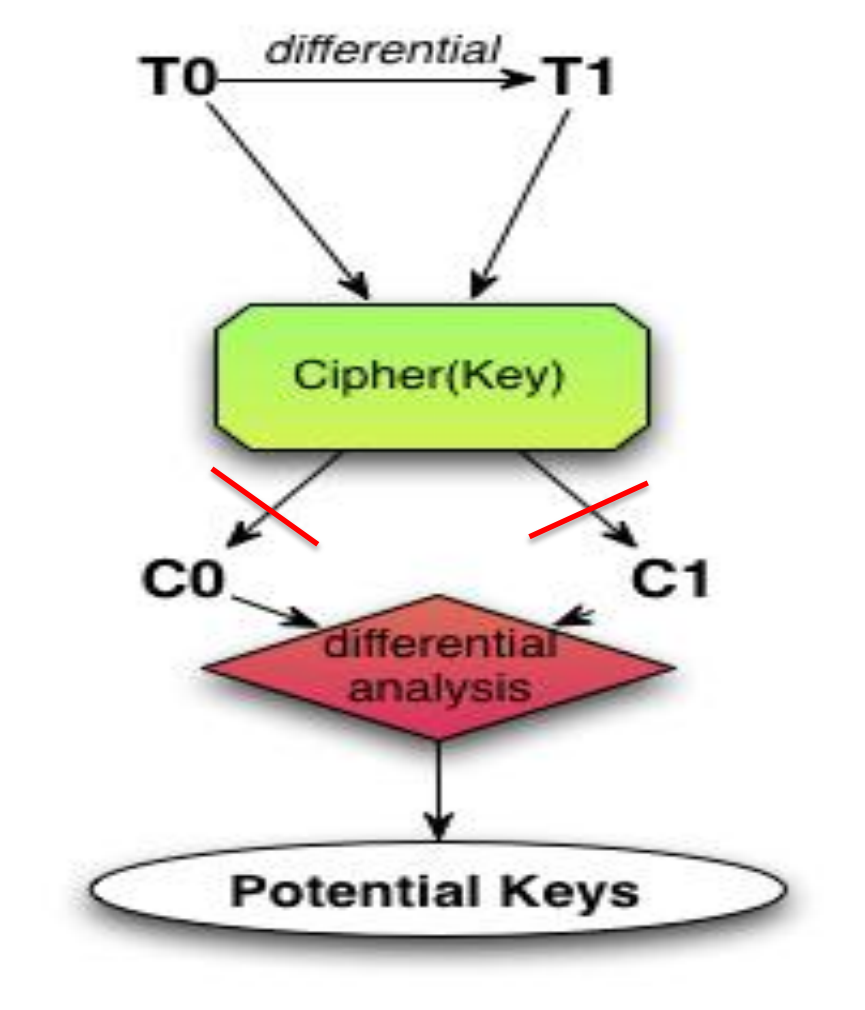
Introduction

- So far we used traditional differential which predict and detect statistical events of highest possible probability.



Introduction

- A new approach is to search for events with probability one, whose condition cannot be met together (events that never happen).



Impossible Differential

- Random permutation:

$$\sigma(M_0) = any\ C\ of\ size\ M_0.$$

- Cipher (not perfect):

$$E(M_0) = some\ C\ of\ size\ M_0.$$

- Events ($m \nrightarrow c$) that never happen distinguish a cipher from a random permutation.

Impossible Differential

- Impossible events ($m \nrightarrow c$) can help performing key elimination.
- All the keys that lead to impossibility are obviously wrong.
- This way we can filter wrong key guesses and leaving the correct key.

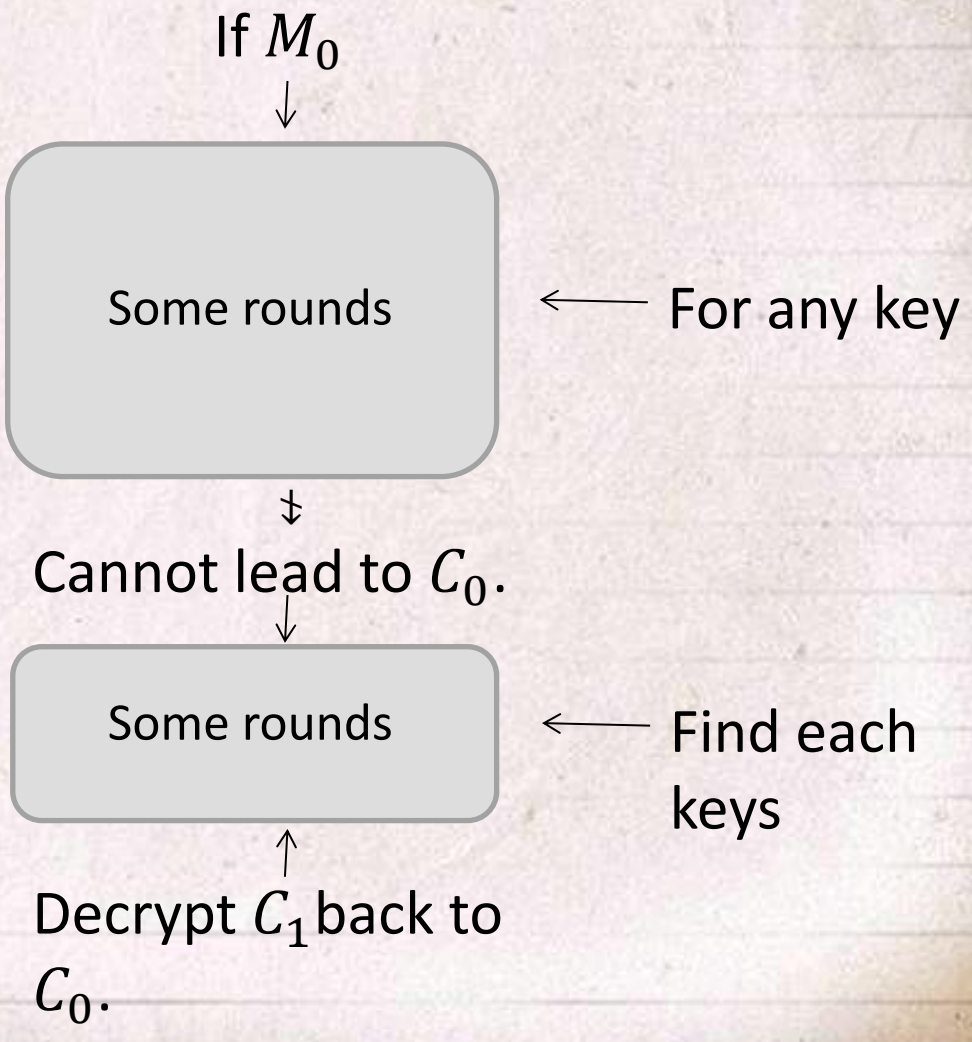
Enigma – for example

- Some of the attacks on Enigma were based on the observation that letters can not be encrypted to themselves.

$$Enigma(M_0) \neq M_0$$

In General

- (M_0, C_1) is a pair. $M_0 \to C_1$.
- $M_0 \nrightarrow C_0$.
- $\{\forall\ key |\ C_1 \to C_0\}$ is an impossible key.



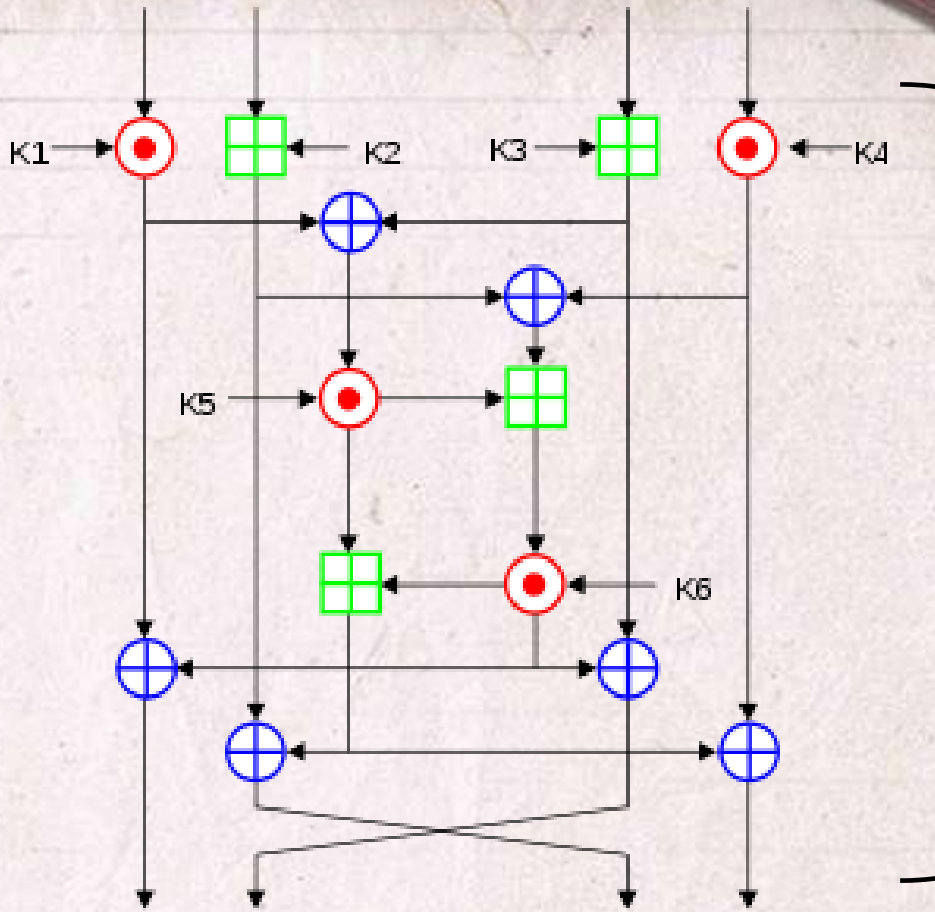
IDEA

- International Data Encryption Algorithm.
- First described in 1991.
- Block cipher.
- Symmetric.
- Key sizes: 128 bits.
- Block sizes: 64 bits.

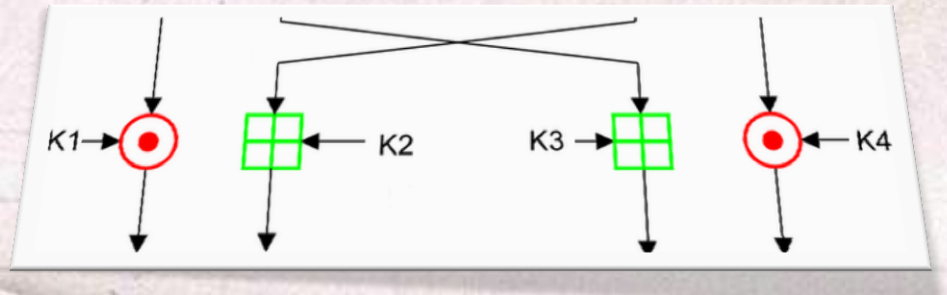
⊕ - XOR.

⊞ - Addition modulo 2^{16}

⊙ - Multiplication modulo $2^{16}+1$



X 8 rounds



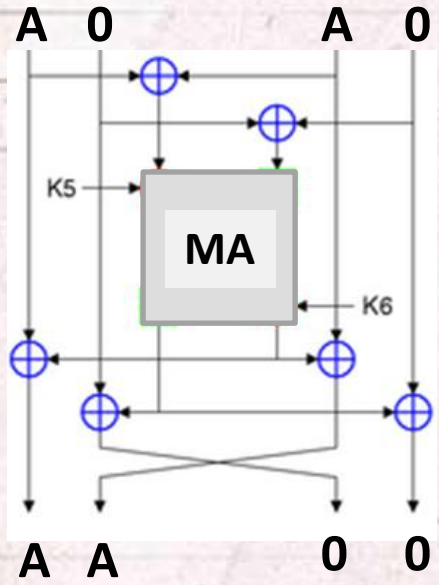
+ Final round.
Half round.

Encryption security

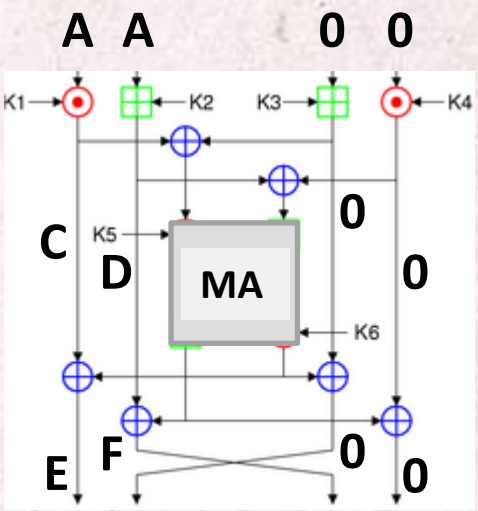
- Combination of different mathematical groups.
- Creation of "incompatibility“:
  - $Z^*_{2^{16}+1} \rightarrow Z_{2^{16}}$
  - $Z_{2^{16}} \rightarrow Z^*_{2^{16}+1}$

Remark: $Z^*_{2^{16}+1}$ doesn’t contain 0 like $Z_{2^{16}}$, so in $Z^*_{2^{16}+1}$ 0 will be converted to 2^{16} since $0 \equiv 2^{16}(mod\ 2^{16})$.

A 2.5-round Impossible Differential

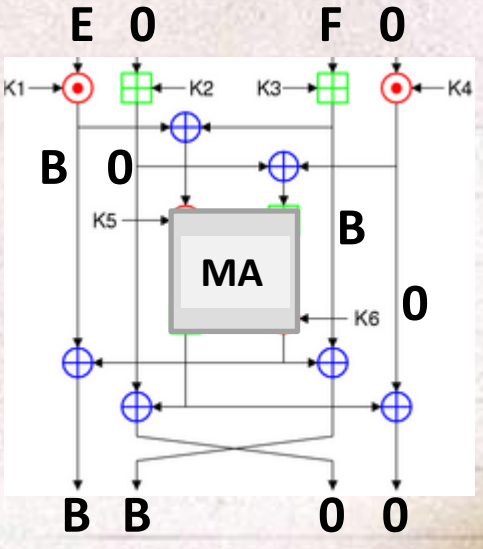


A⊕0=A
A⊕0=A
⟶ MA ⟶ 0



B⊕B=0
0⊕0=0
⟶ MA ⟶ 0

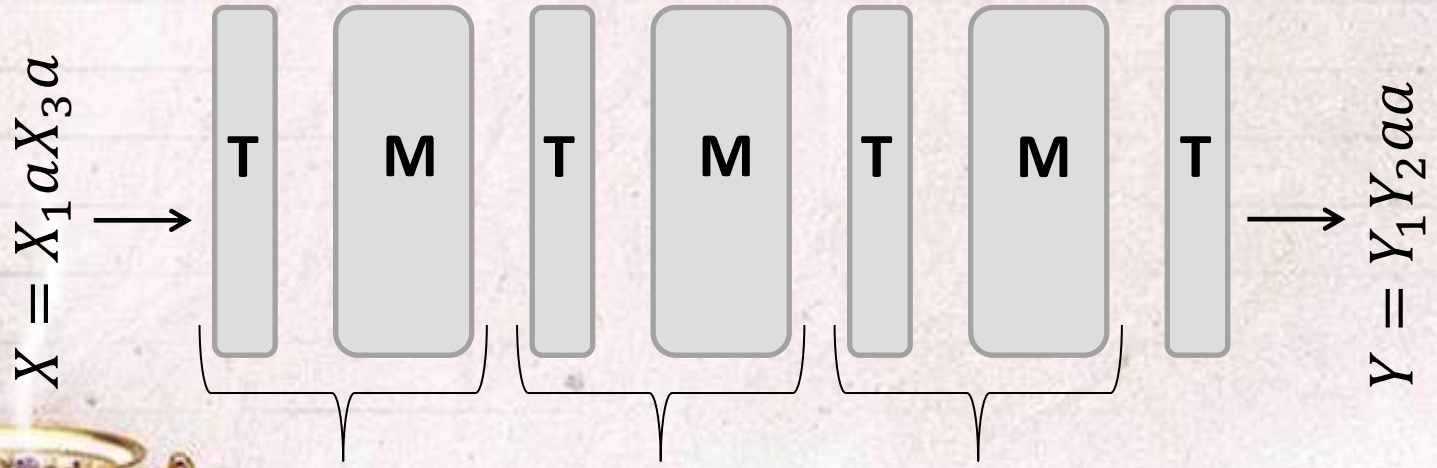
A⊕A=0
0⊕0=0
⟶ MA ⟶ 0



0 ⊕0=0 => C=E
0 ⊕0=0 => D=F

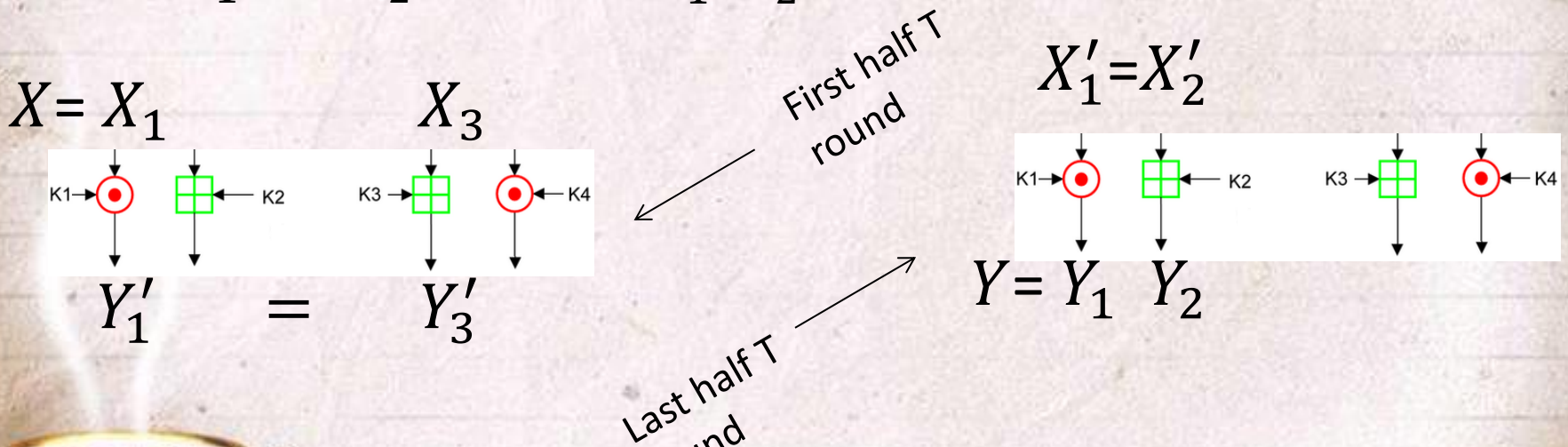
An Attack on 3.5 Round IDEA

1. Get all 2^{32} plaintexts of the form $X = X_1 a X_3 a$.
2. Collect about 2^{31} ciphertexts pairs satisfying $Y_3' = Y_4' = 0$.



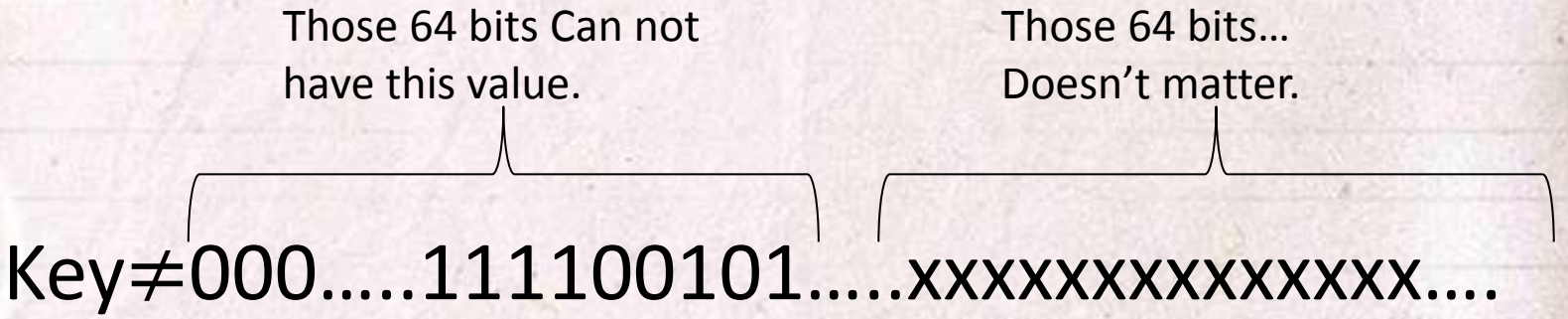
An Attack on 3.5 Round IDEA

3. Choose a pair:
    1. Try all 2^{32} subkeys of first T round encrypting X_1 and X_3 into Y_1 and Y_3 such that $Y_1'=Y_3'$.
    2. Try all 2^{32} subkeys of last T round decrypting Y_1 and Y_2 into X_1 and X_2 such that $X_1'=X_2'$.



An Attack on 3.5 Round IDEA

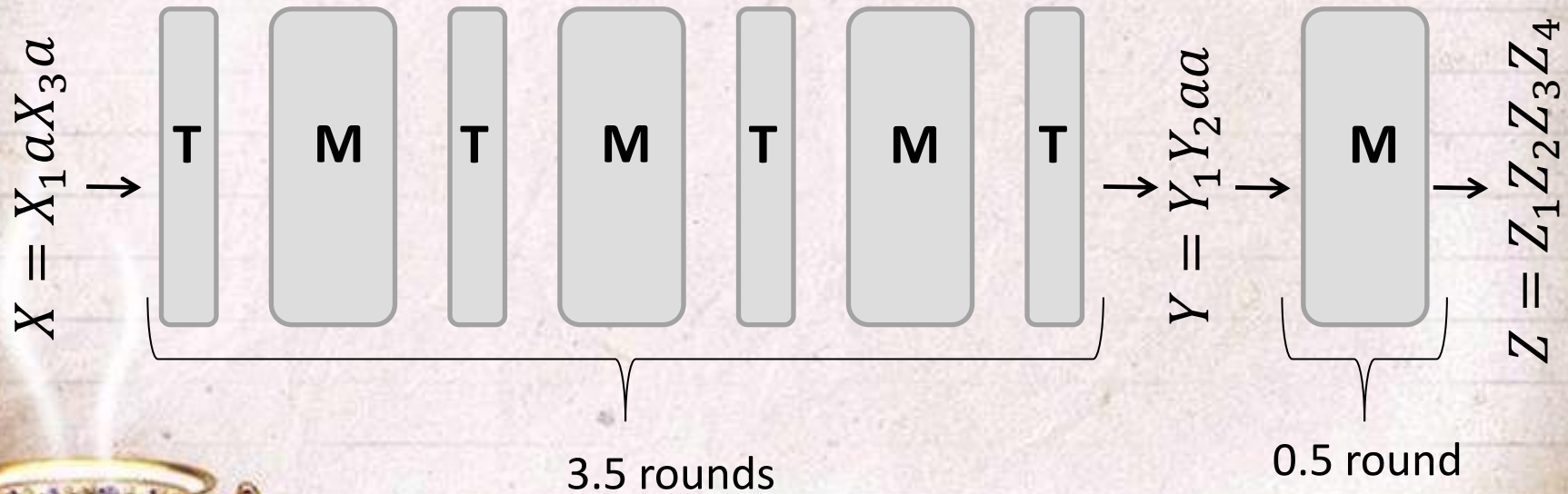
4. For each pair, collect all subkeys bits answering previous step. Those cannot be the real value of the key.



- Each pair defines a list of about 2^{32} incorrect keys.
- Repeat this for each of the 2^{31} pairs. And continue to do so for $90 \cdot 2^{31}$ such pairs - Number of wrong key value is 2^{64}.
- Symmetric-key algorithm – Do the same with (0,a,0,a) instead of (a,0,a,0). In the end we will get 18 bits left to find for getting 128 bit of secret key.
- This attack requires 2^{53} steps of analysis.

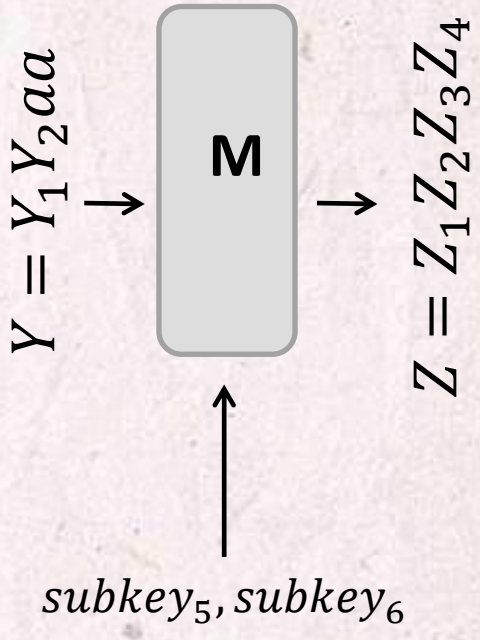
An Attack on 4 Round IDEA

- Reducing 4 rounds problem to 3.5 rounds problem…



An Attack on 4 Round IDEA

- Find $subkey_5, subkey_6$ decrypting from Z to Y.



- Finding $subkey_5, subkey_6$ for last T half, increases our efforts but reveals $subkey_3$ at T round 2.

$$subkey_3^2 \in subkey_5^5 \cup subkey_6^5$$

- By revealing $subkey_3^2$ we can calculate $subkey_1^2$ - both of them lead to the same differential.

$$(subkey_3^2 \boxplus X_3^2) \oplus (subkey_3^2 \boxplus X_3^{2\prime}) = (subkey_1^2 \odot X_1^2) \oplus (subkey_1^2 \odot X_1^{2\prime})$$

- Similarly we can find $subkey_1^5, subkey_2^5$.

$$(subkey_2^5 \boxplus X_2^5) \oplus (subkey_2^5 \boxplus X_2^{5\prime}) = (subkey_1^5 \odot X_1^5) \oplus (subkey_1^5 \odot X_1^{5\prime})$$

An Attack on 4 Round IDEA

- Eventually, this attack requires about 2^{38} chosen plaintexts, and about 2^{70} encryptions.

Attacks on Khufu and Khafre

- Khufu and Khafre are both:
  - 64-bit block.
  - 512-bit key.
  - Block ciphers.
  - Feistel cipher, means the input is split into two 32-bit halves (L and R).
  - Contain the same round steps.

Khufu VS Khafre

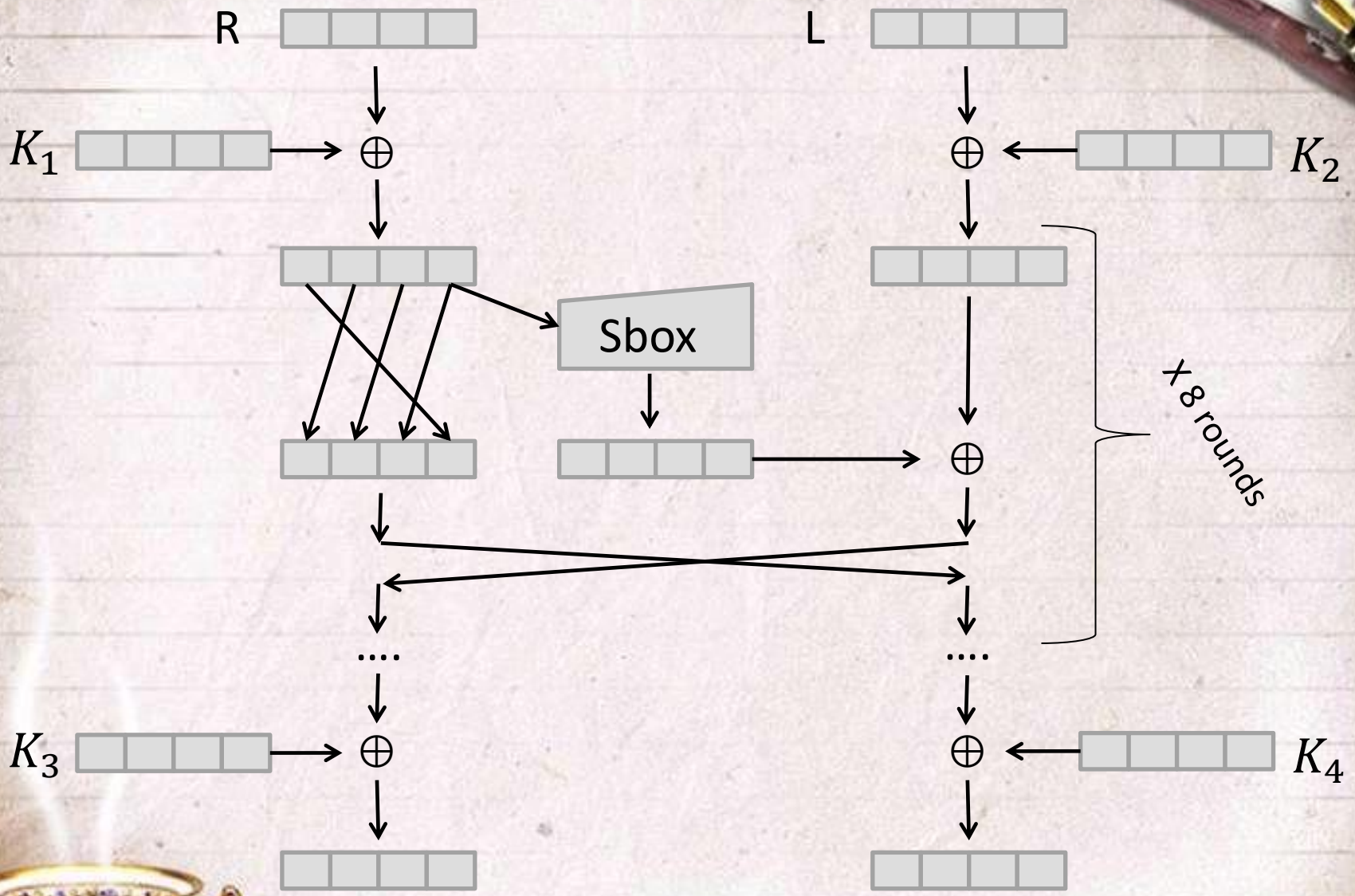
- Khufu is faster due to a smaller number of rounds.
- Khufu is based on key dependent S-boxes. These are unknown to an attacker and thus defy analysis based on specific properties of the S-box.
- In Khufu, the only additional way in which the key is used is at the beginning and the end of the cipher.

Khufu VS Khafre

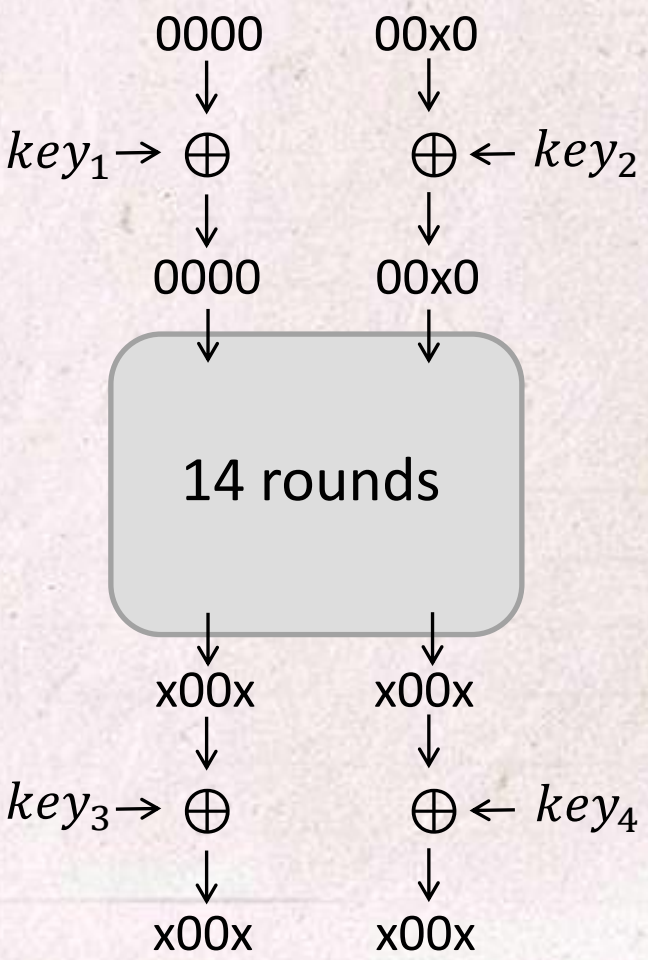
- Khafre S-boxes are known.
- Khufu xors the key to the data, every eight rounds. Not only at the beginning and the end like Khufu.

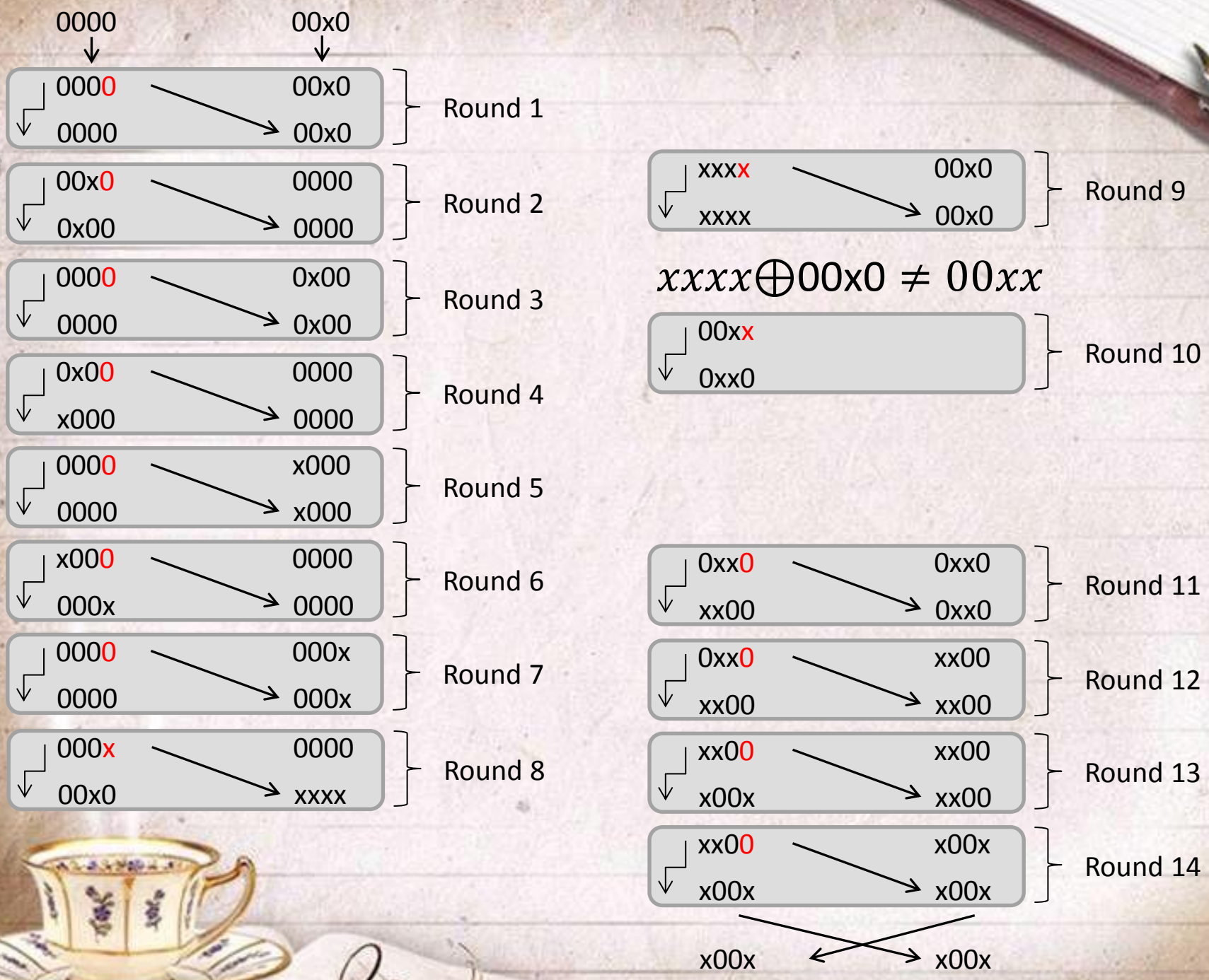
Introduction to attack on a simplified Khufu

- Following attack is not very sensitive to the differences between these two ciphers, since it is independent of the choice of the S-boxes.
- Any how, it is believed that Khufu is stronger, because of its key-dependent S-boxes.


R
L
K_1
K_2
Sbox
x 8 rounds
K_3
K_4

A 14-round Impossible Differential




0000
00x0
0000
00x0
0000
00x0
Round 1
00x0
0000
0x00
0000
Round 2
0000
0x00
0000
0x00
Round 3
0x00
0000
x000
0000
Round 4
0000
x000
0000
x000
Round 5
x000
0000
000x
0000
Round 6
0000
000x
0000
000x
Round 7
000x
0000
00x0
xxxx
Round 8
xxxx
00x0
xxxx
00x0
Round 9
$xxxx \oplus 00x0 \neq 00xx$
00xx
0xx0
Round 10
0xx0
0xx0
xx00
0xx0
Round 11
0xx0
xx00
xx00
xx00
Round 12
xx00
xx00
x00x
xx00
Round 13
xx00
x00x
x00x
x00x
Round 14
x00x
x00x

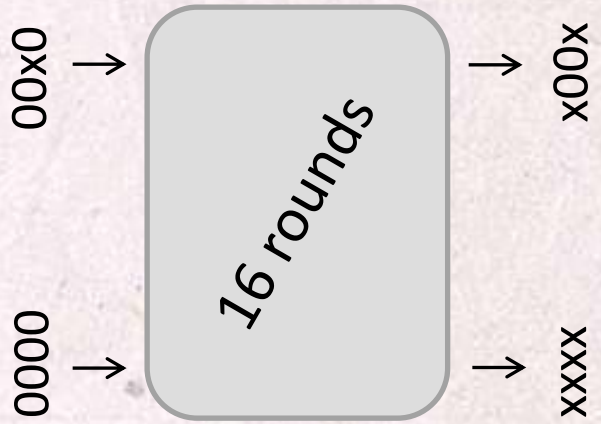
Impossible Differentials

Rounds	Input		Output
14	000000x0	$\not\to$	x00xx00x
14	00x000x0	$\not\to$	x00x000x
15	000000x0	$\not\to$	x00xx00x
15	000000x0	$\not\to$	x00x000x
15	000000x0	$\not\to$	x00xx000
16	000000x0	$\not\to$	x000000x
16	000000x0	$\not\to$	000xx000
18	000000x0	$\not\to$	x0000000
18	000000x0	$\not\to$	0000000x
20	000000x0	$\not\to$	000x0000

An Attack on 16 Rounds Khufu…

…Using 15-round impossible differential

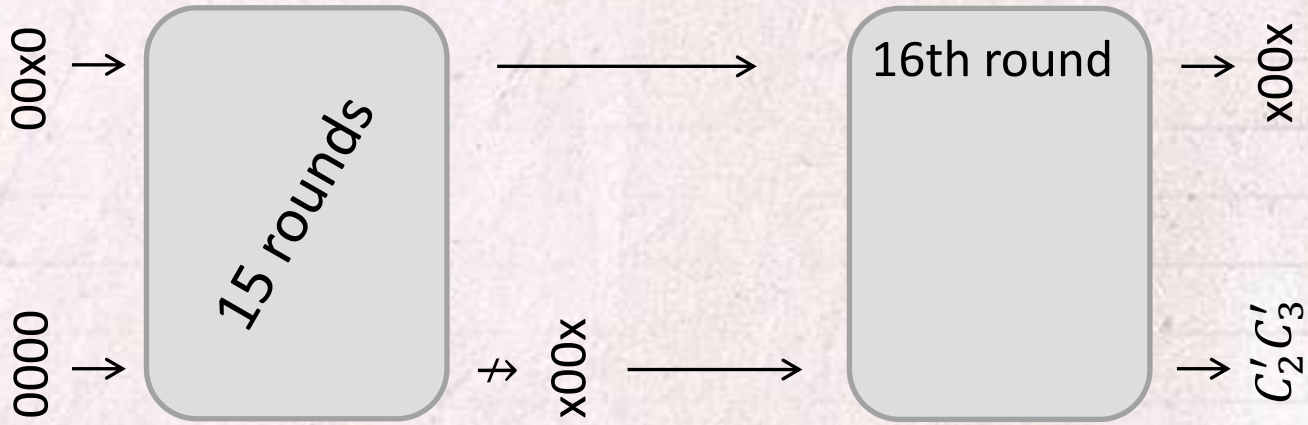
1. Encrypt structures of $2^8 = 256$ plaintexts differing only in the 7th byte.
2. Keep only those with zero difference in cipher-text bytes 5 and 6.



An Attack on 16 Rounds Khufu…

…Using 15-round impossible differential

3. For each remaining pair (P_1, P_2) get the impossible condition on the two middle bytes at the S-box of the last round.



$$S[P_1]_2 \oplus S[P_2]_2 \neq C_2' \; and \; S[P_1]_3 \oplus S[P_2]_3 \neq C_3'$$

What does it mean

$S[P_1]_2 \oplus S[P_2]_2 \neq C_2 \; and \; S[P_1]_3 \oplus S[P_2]_3 \neq C_3$:

- $S[P_1]_2 \oplus S[P_2]_2$ and $S[P_1]_3 \oplus S[P_2]_3$ can not be equal to 0 together.

- Find which S-box values give the impossible condition, and exclude them.

An Attack on 16 Rounds Khufu

- Eventually, this attack requires about 2^{41} chosen plain-texts to get an S-box.
- When the S-box is revealed, subkeys 5 to 8 doesn't matter any more, and all that left are subkeys 1 to 4.

Conclusions

- Since the introduction of differential cryptanalysis, came several approaches to the design of ciphers suggesting more security against this attack.
- One way of proving a cipher is increasing number of possible ciphertexts for each plaintext.

$$E(M_0) \rightarrow 2^{|M_0|} - |impossibles|$$

Example: One Time Pad

- One Time Pad is a perfect cipher satisfying:

$$E(M_0) \rightarrow 2^{M_0} - 0$$

- There are no impossible outcomes.

Expanded S-box

- A general belief is that large expanding S-boxes ($|input\ bits| < |output\ bits|$) offer increased security against differential attacks.
- However, such S-boxes contain very few possible entries $|input\ bits|$, and all the other $|output\ bits| - |input\ bits|$ pairs of input/output differences are impossible.

Thank you for listening

And watching

References

- Miss in the Middle Attacks on IDEA, Khufu and Khafre – Eli Biham, Alex Biryukov, Adi Shamir.
- Wikipedia - International Data Encryption Algorithm
- YouTube - Miss in the Middle Attacks on IDEA, - Alex Biryukov