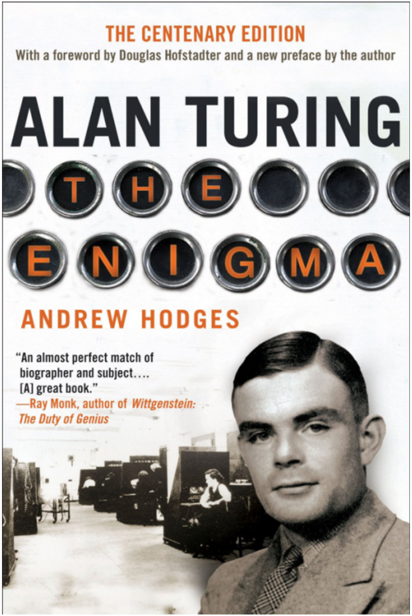


CSL 505

CRYPTOGRAPHY

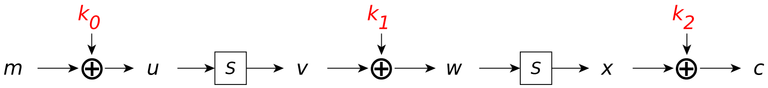
Lecture 7

More on Differential Cryptanalysis

Instructor
Dr. Dhiman Saha

Image Source: Google

Recall — DC of Sypher002



- Initialize counters $T_i = 0$, one for each possible key k_2 .
- For each message/ciphertext pair do
  - For each guess i for k_2 do
    - Compute $v_0' \oplus v_1'$
    - If $v_0' \oplus v_1' = d$ increase counter T_i
- Assume that the right key k_2 corresponds to the highest counter.

- What about the complexity of recovering each k_i

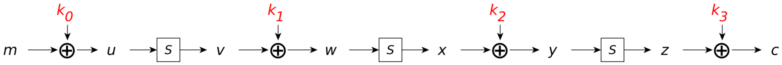
u_0	$u_1 = u_0 \oplus f$	$v_0 = S[u_0]$	$v_1 = S[u_1]$	$v_0 \oplus v_1$
0	f	6	b	d
1	e	4	9	d
2	d	c	a	6
3	c	5	8	d
4	b	0	d	d
5	a	7	3	4
6	9	2	f	d
7	8	e	1	f
8	7	1	e	f
9	6	f	2	d
a	5	3	7	4
b	4	d	0	d
c	3	8	5	d
d	2	a	c	6
e	1	9	4	d
f	0	b	6	d

in \out	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

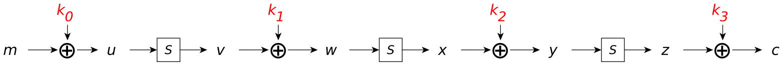
Recall the interpretation

Point to Ponder

What about Sypher003?



Point to Ponder
What about Sypher003?

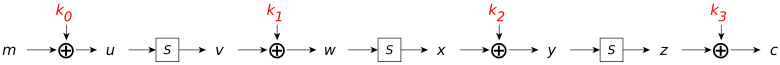


Hint

Two Round Characteristic

$$f \xrightarrow{S} d \xrightarrow{S} c$$

Point to Ponder — What about Sypher003?



Hint

Two Round Characteristic

$$f \xrightarrow{S} d \xrightarrow{S} c$$

- $\Pr\left[f \xrightarrow{S} d\right] = \frac{10}{16}$ and $\Pr\left[d \xrightarrow{S} c\right] = \frac{6}{16}$

Point to Ponder — What about Sypher003?

$$m \xrightarrow{\oplus\, k_0} u \xrightarrow{S} v \xrightarrow{\oplus\, k_1} w \xrightarrow{S} x \xrightarrow{\oplus\, k_2} y \xrightarrow{S} z \xrightarrow{\oplus\, k_3} c$$

Hint

Two Round Characteristic

$$f \xrightarrow{S} d \xrightarrow{S} c$$

- $\Pr\left[f \xrightarrow{S} d\right] = \frac{10}{16}$ and $\Pr\left[d \xrightarrow{S} c\right] = \frac{6}{16}$

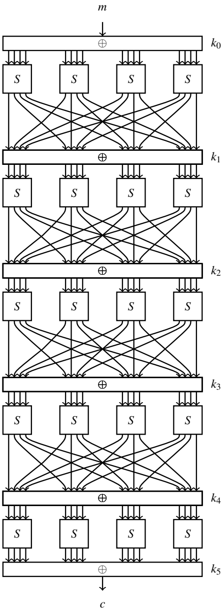
Assumption — Characteristics are independent

$$\Pr\left[f \xrightarrow{S} d \xrightarrow{S} c\right] = \frac{10}{16} \times \frac{6}{16} = \frac{15}{64}$$

Any Guess about Sypher004

What does it look like?

Point to Ponder — What about Sypher004?

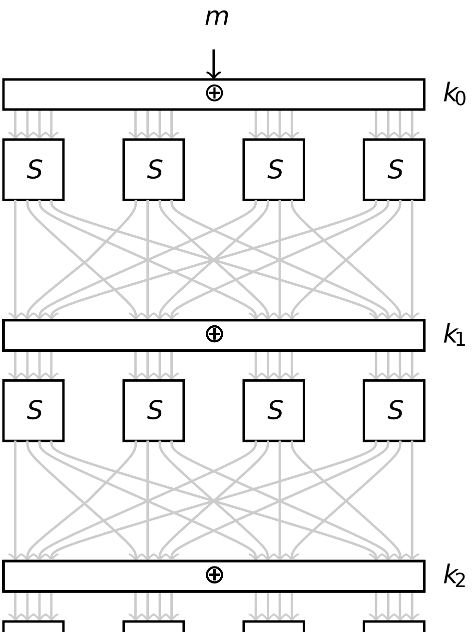


- Till now there was no **permutation** layer
- So we did not have to consider its effect

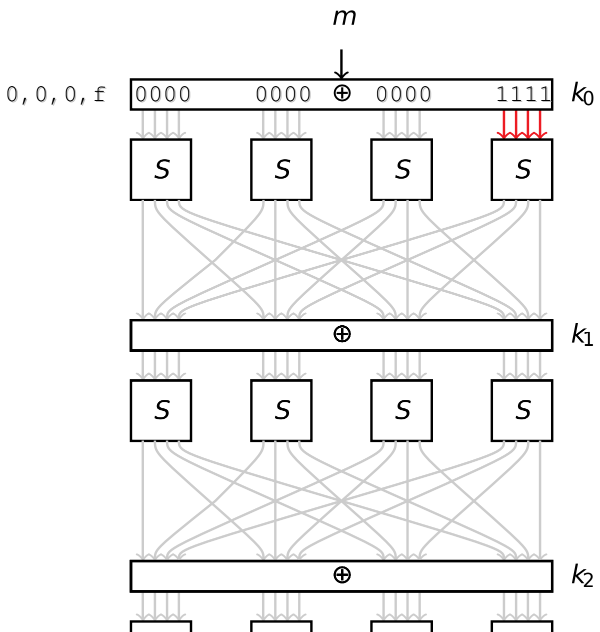
Notion of **Active** Sboxes

Note

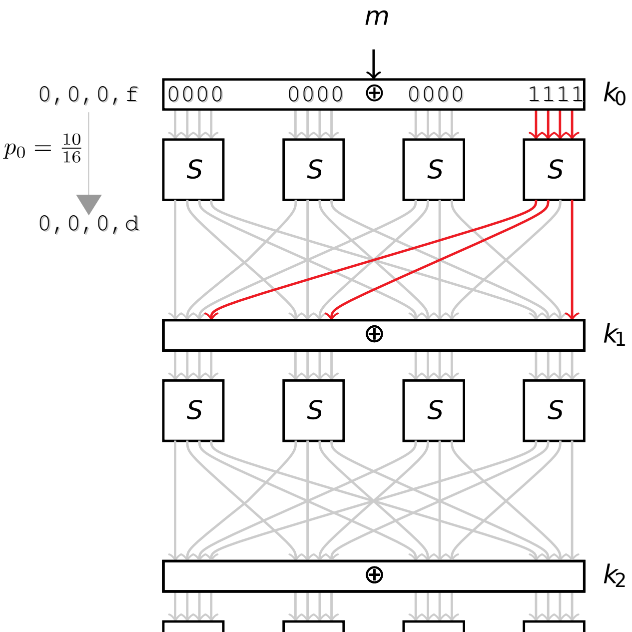
No permutation in last round. Why?


m
k0
S
S
S
S
k1
S
S
S
S
k2

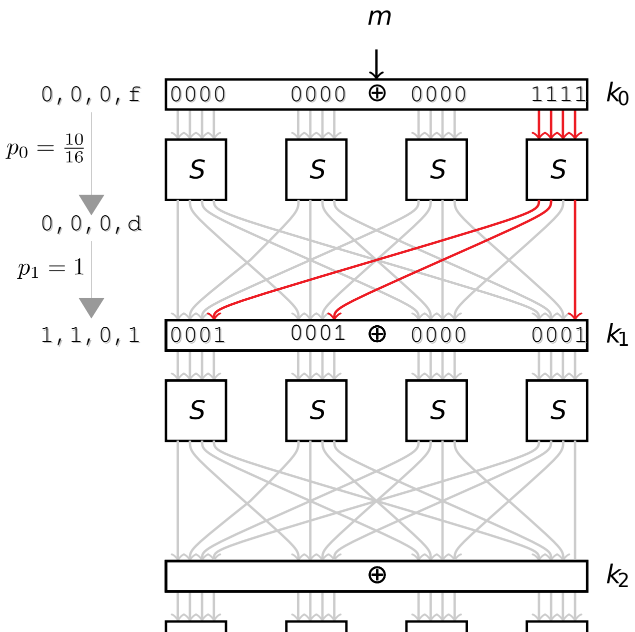
Input Difference (0,0,0,f)



Building Multi-Round Characteristics $p = \frac{10}{16}$

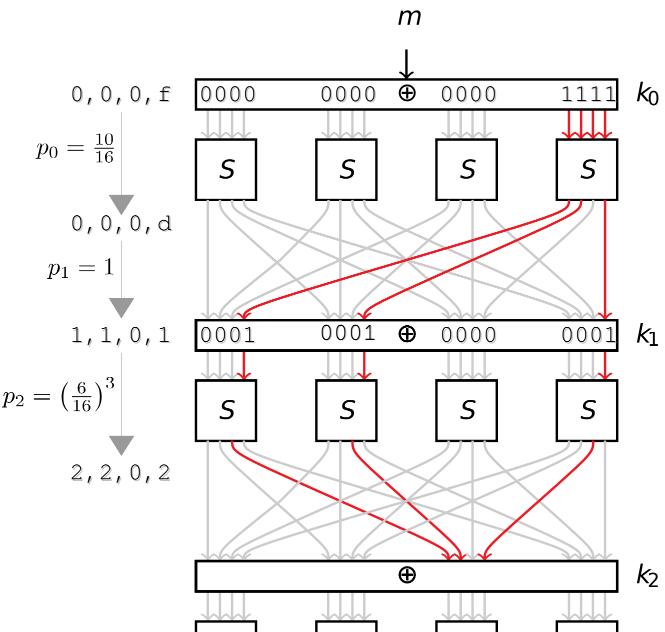


Building Multi-Round Characteristics $p = \frac{10}{16}$

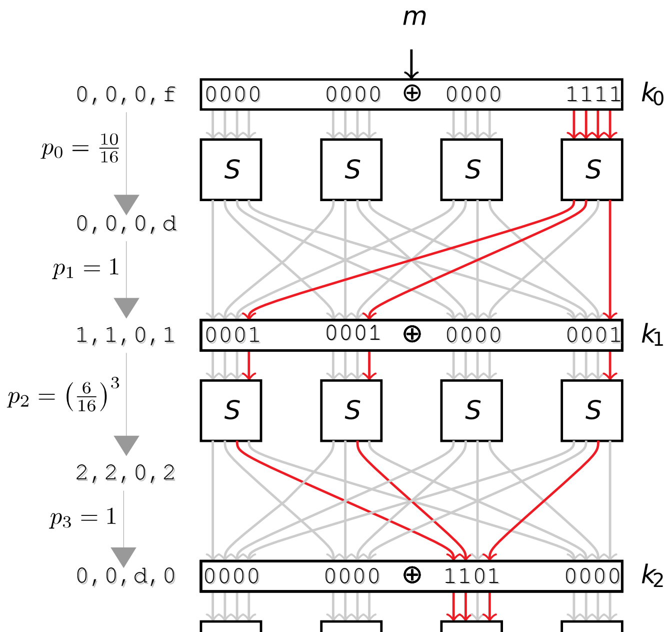


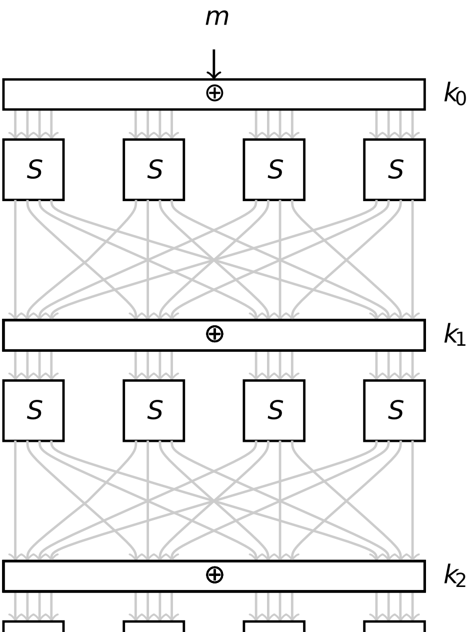
Building Multi-Round Characteristics

$$p = \frac{10}{16} \times \left(\frac{6}{16}\right)^3$$



Building Multi-Round Characteristics $p = \frac{10}{16} \times \left(\frac{6}{16}\right)^3$




m
k_0
S
S
S
S
k_1
S
S
S
S
k_2

For Reference

in \out	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Is there a strategy to construct these?

- What did we follow just now?

Local Optimum | **Greedy approach**

May not be the best thing to do

- The effects of P-layer come into consideration
- Minimization of number of **active** Sbox-es
- Note how each active Sbox contributes to the probability of the multi-round characteristics

Is there a strategy to construct these?

- What did we follow just now?

Local Optimum — **Greedy approach**

May not be the best thing to do

- The effects of P-layer come into consideration
- Minimization of number of **active** Sbox-es
- Note how each active Sbox contributes to the probability of the multi-round characteristics

Is there a strategy to construct these?

- What did we follow just now?

Local Optimum	Greedy approach
May not be the best thing to do	

- The effects of P-layer come into consideration
- Minimization of number of **active** Sbox-es
- Note how each active Sbox contributes to the probability of the multi-round characteristics

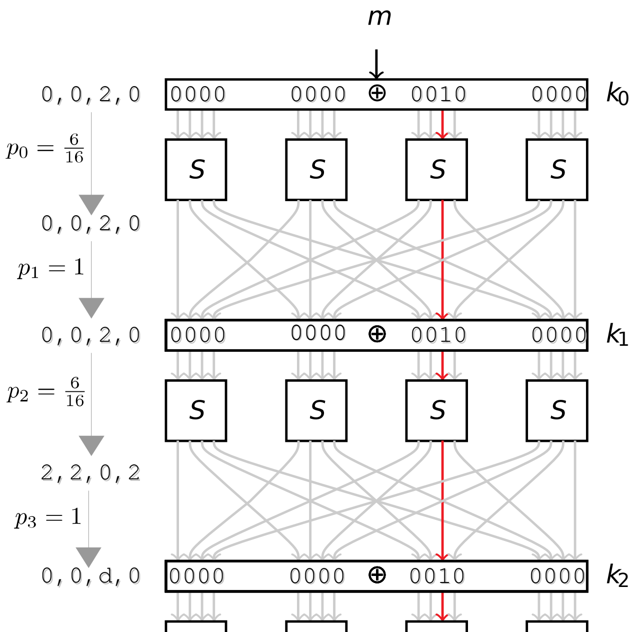
Let Us take A Non-Greedy Approach

DDT

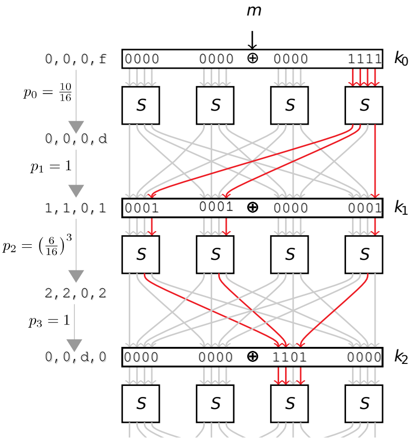
in \out	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

Look at $2 \rightarrow 2$ transition

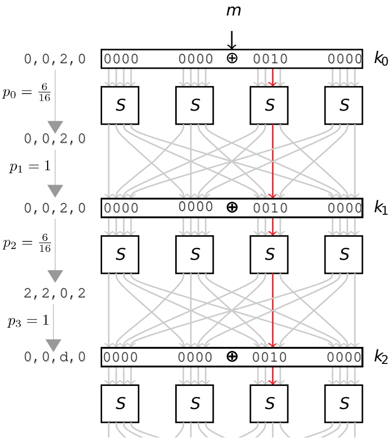
Example $\to p = \left(\frac{6}{16}\right)^2$ Input Diff. $\to (0, 0, 2, 0)$



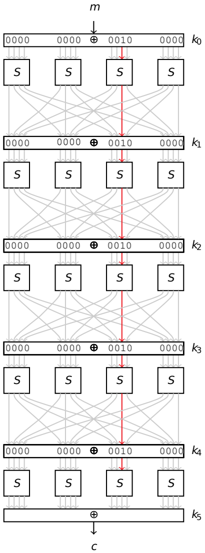
Greedy fails!!! Putting things in perspective



$$p = \frac{10}{16} \times \left(\frac{6}{16}\right)^3$$



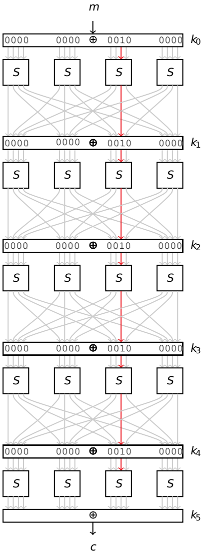
$$p = \left(\frac{6}{16}\right)^2$$



- Get 4-round characteristic
- Find conforming message pairs 

Why 4-rounds ?

- Recall previous attacks
- Partial decryption (go backwards)
- Last round will be inverted by guessing (part of) k_5
- To verify expected difference as per 4-round characteristic



- For the current characteristic, $p = \left(\frac{6}{16}\right)^4 \approx 0.02$

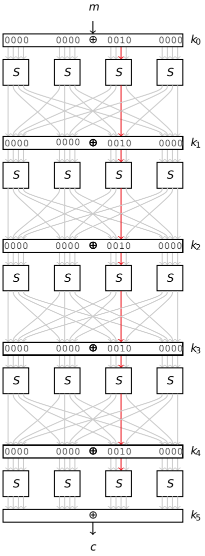
Whats the catch?

Probability of any given difference occurring at random is $\frac{1}{16} \approx 0.06 > 0.02$

- Implications?
- Ineffective distinguisher!

How to find a better one?

- No good answer, specially for large block sizes.
- Recent results on using Mixed Integer Linear Programming (MILP)



- For the current characteristic, $p = \left(\frac{6}{16}\right)^4 \approx 0.02$

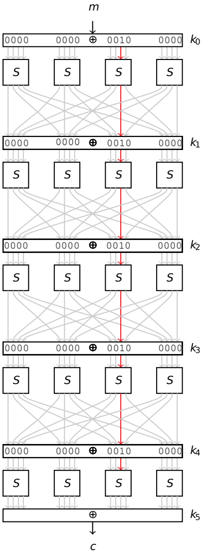
Whats the catch?

Probability of any given difference occurring at random is $\frac{1}{16} \approx 0.06 > 0.02$

- Implications?
- Ineffective distinguisher!

How to find a better one?

- No good answer, specially for large block sizes.
- Recent results on using Mixed Integer Linear Programming (MILP)



- For the current characteristic, $p = \left(\frac{6}{16}\right)^4 \approx 0.02$

Whats the catch?

Probability of any given difference occurring at random is $\frac{1}{16} \approx 0.06 > 0.02$

- Implications?
- Ineffective distinguisher!

How to find a better one?

- No good answer, specially for large block sizes.
- Recent results on using Mixed Integer Linear Programming (MILP)

Experimental Confirmation — 4-round Characteristic

- $k_0 = 5b92$
- $k_1 = 064b$
- $k_2 = 1e03$
- $k_3 = a55f$
- $k_4 = ecbd$
- $k_5 = 7ca5$

- $|\text{Message pairs}| = 2^{16} : \Delta = (0, 0, 2, 0)$
- Conforming message pairs found $= 1300$
- Conforming means?
- After **every round** difference is $(0, 0, 2, 0)$
- Computed probability $\frac{1300}{2^{16}} \approx 0.02$
- Matches expected probability

Home Work Problem

Can also be verified across other randomly chosen key sets.

Experimental Confirmation — 4-round Characteristic

- $k_0 = 5b92$
- $k_1 = 064b$
- $k_2 = 1e03$
- $k_3 = a55f$
- $k_4 = ecbd$
- $k_5 = 7ca5$

- $|\text{Message pairs}| = 2^{16} : \Delta = (0, 0, 2, 0)$
- Conforming message pairs found $= 1300$
- Conforming means?
- After **every round** difference is $(0, 0, 2, 0)$
- Computed probability $\frac{1300}{2^{16}} \approx 0.02$
- Matches expected probability

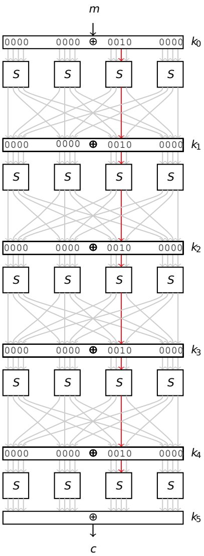
Home Work Problem

Can also be verified across other randomly chosen key sets.

Two optimization techniques

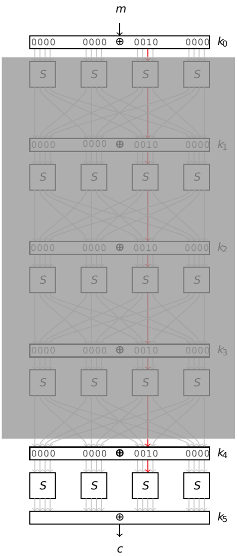
Differentials
Filtering

Characteristic



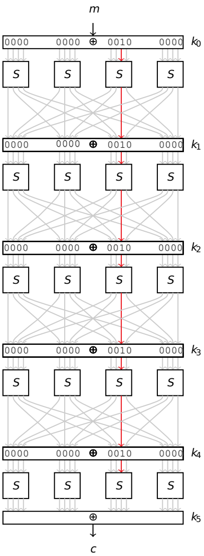
$$(0,0,2,0) \xrightarrow{R} (0,0,2,0) \xrightarrow{R} \cdots (0,0,2,0)$$

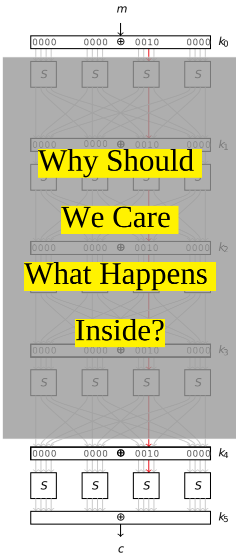
Differential



$$(0,0,2,0) \xrightarrow{R} ? \xrightarrow{R} ? \cdots ? \xrightarrow{R} (0,0,2,0)$$

Characteristic   Differential





$$(0,0,2,0) \xrightarrow{R} (0,0,2,0) \xrightarrow{R} \cdots (0,0,2,0)$$

$$(0,0,2,0) \xrightarrow{R} ? \xrightarrow{R} ? \cdots ? \xrightarrow{R} (0,0,2,0)$$

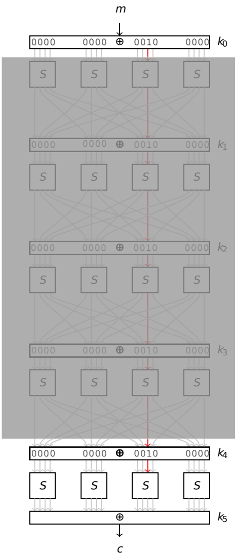
Example

$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0).$$

But it also contains at least three other possible characteristics. They are

$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,0,2) \xrightarrow{\mathscr{R}} (0,0,0,1) \xrightarrow{\mathscr{R}} (0,0,1,0) \xrightarrow{\mathscr{R}} (0,0,2,0),$$
$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,0,2) \xrightarrow{\mathscr{R}} (0,0,1,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0), \text{ and}$$
$$(0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,2,0) \xrightarrow{\mathscr{R}} (0,0,0,2) \xrightarrow{\mathscr{R}} (0,0,1,0) \xrightarrow{\mathscr{R}} (0,0,2,0).$$

Idea of filtering



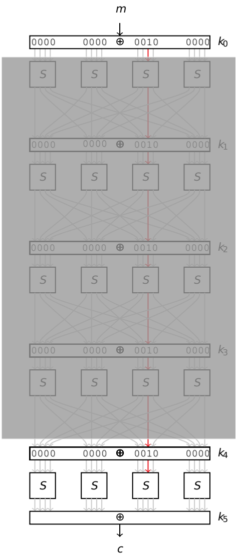
$$(0,0,2,0) \xrightarrow{R} ? \xrightarrow{R} ? \cdots ? \xrightarrow{R} (0,0,2,0)$$

- Lets look at the possibilities of the last round

Are all ciphertexts usable for us?

- Filtering?
- Note: For $(0,0,2,0) \rightarrow (0,0,2,0)$, 12-bits in the difference of cipher-texts must be zero
- What about remaining 4-bits?
- We again look at the Sbox

Idea of filtering



$$(0,0,2,0) \xrightarrow{R} ? \xrightarrow{R} ? \cdots ? \xrightarrow{R} (0,0,2,0)$$

- Lets look at the possibilities of the last round

Are all ciphertexts usable for us?

- Filtering?
- Note: For $(0,0,2,0) \to (0,0,2,0)$, 12-bits in the difference of cipher-texts must be zero
- What about remaining 4-bits?
- We again look at the Sbox

Note transitions from 2 $\to \{1, 2, 9, a\}$ DDT

in \ out	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	6	-	-	-	-	2	-	2	-	-	2	-	4	-
2	-	6	6	-	-	-	-	-	-	2	2	-	-	-	-	-
3	-	-	-	6	-	2	-	-	2	-	-	-	4	-	2	-
4	-	-	-	2	-	2	4	-	-	2	2	2	-	-	2	-
5	-	2	2	-	4	-	-	4	2	-	-	2	-	-	-	-
6	-	-	2	-	4	-	-	2	2	-	2	2	2	-	-	-
7	-	-	-	-	-	4	4	-	2	2	2	2	-	-	-	-
8	-	-	-	-	-	2	-	2	4	-	-	4	-	2	-	2
9	-	2	-	-	-	2	2	2	-	4	2	-	-	-	-	2
a	-	-	-	-	2	2	-	-	-	4	4	-	2	2	-	-
b	-	-	-	2	2	-	2	2	2	-	-	4	-	-	2	-
c	-	4	-	2	-	2	-	-	2	-	-	-	-	-	6	-
d	-	-	-	-	-	-	2	2	-	-	-	-	6	2	-	4
e	-	2	-	4	2	-	-	-	-	-	2	-	-	-	-	6
f	-	-	-	-	2	-	2	-	-	-	-	-	-	10	-	2

- Any other transition from 2 is impossible 
- Message pairs leading to ciphertext pairs giving differences other than $\{1, 2, 9, a\}$ in the third nibble can be discarded