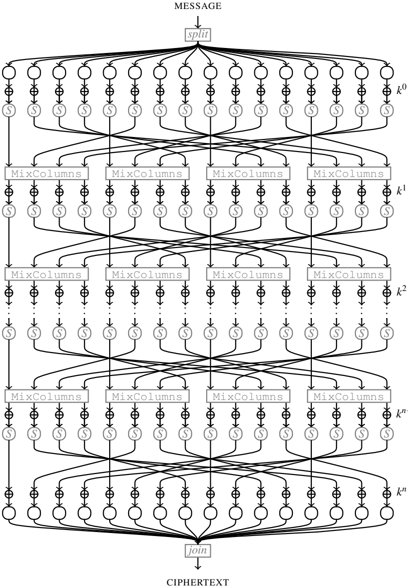


Image Source: Google

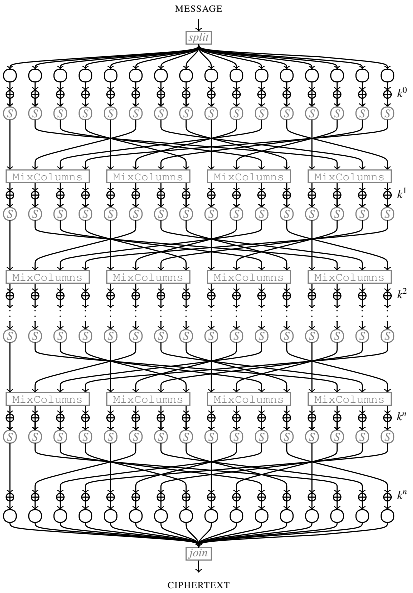
CS 553
CRYPTOGRAPHY

Lecture 13
Analyzing AES

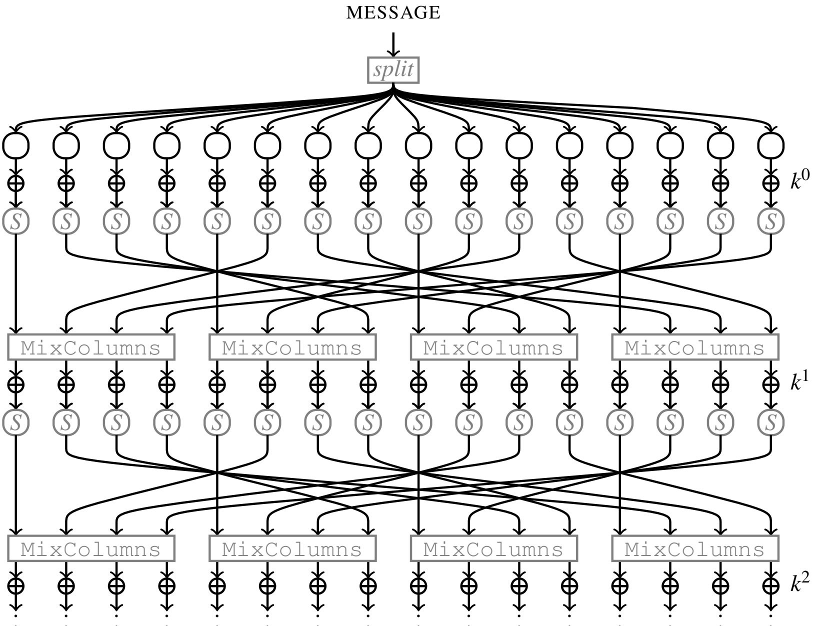
Instructor
Dr. Dhiman Saha

AES

2D



AES



Recall AES Internals

The Sbox

	$S[\cdot]$															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

The value of $S[ab]$ is given by the entry in row a and column b

Recall AES Internals

The Sbox Inverse

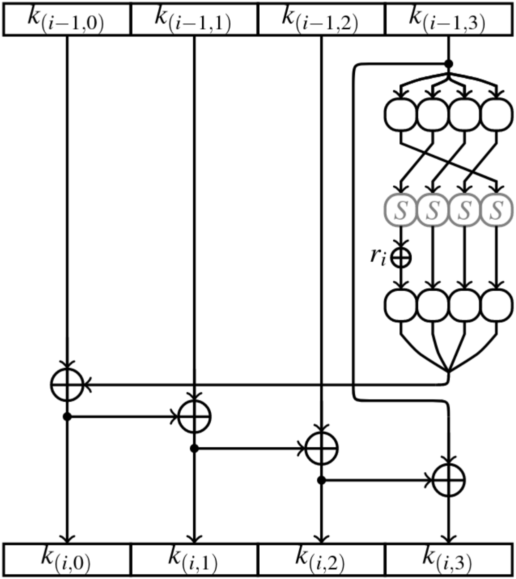
$S^{-1}[\cdot]$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

$$M = \begin{pmatrix} \mathtt{02} & \mathtt{03} & \mathtt{01} & \mathtt{01} \\ \mathtt{01} & \mathtt{02} & \mathtt{03} & \mathtt{01} \\ \mathtt{01} & \mathtt{01} & \mathtt{02} & \mathtt{03} \\ \mathtt{03} & \mathtt{01} & \mathtt{01} & \mathtt{02} \end{pmatrix} \quad \text{and} \quad M^{-1} = \begin{pmatrix} \mathtt{0e} & \mathtt{0b} & \mathtt{0d} & \mathtt{09} \\ \mathtt{09} & \mathtt{0e} & \mathtt{0b} & \mathtt{0d} \\ \mathtt{0d} & \mathtt{09} & \mathtt{0e} & \mathtt{0b} \\ \mathtt{0b} & \mathtt{0d} & \mathtt{09} & \mathtt{0e} \end{pmatrix}.$$

Recall AES Internals

The Key Schedule



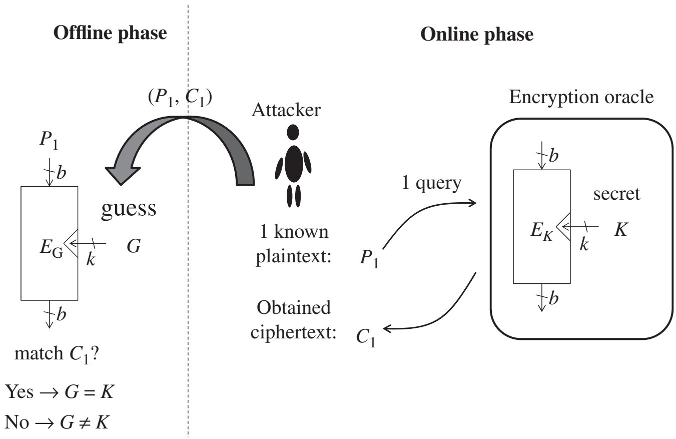
Attack Complexity — Data, Time, Memory

$$(D, T, M)$$

- the attacker can ask D queries to the oracle under the assumed attack model,
- the attacker can spend the cost of executing the encryption or decryption algorithm T times,
- the attacker has enough memory to store M data of the size b bits,

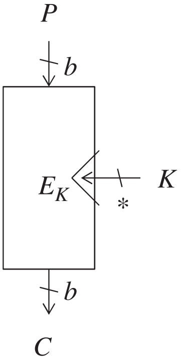
- Generic Attacks
  - Brute-force Attack
  - Code-Book Attack

Brute force attack for $k < b$



$$(\texttt{Data, Time, Memory}) = (\mathit{negl.}, 2^k, \mathit{negl.})$$

Codebook Attack



Look-up table

P	C
P_0	C_0
P_1	C_1
$\vdots$	$\vdots$
P_{2^b-1}	C_{2^b-1}

2^b entries

$2b$ bits

$$\texttt{(Data, Time, Memory)} = (2^b, \textit{negl.}, 2^b)$$

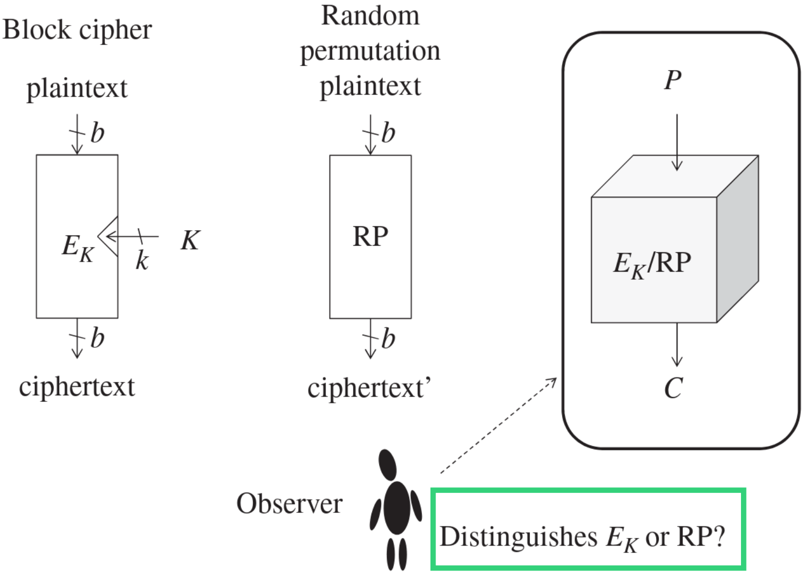
Security of Block Ciphers

- Block ciphers are required to provide some robustness against cryptanalysis.
- To measure the security of block ciphers, security notions must be defined.
- There are several classes of security notions.
- Three major notions are:
  - Key recovery **resistance**
  - Plaintext recovery **resistance**
  - Indistinguishability from a random permutation

Security Notions

- **Key recovery resistance:**
  - For any choice of the key K, the block cipher must resist the attack that **efficiently** recovers the value of K.
- **Plaintext recovery resistance:**
  - For any choice of the key K, and for any choice of the ciphertext C, the block cipher must resist the attack that **efficiently** recovers the corresponding plaintext value P such that $E_K(P) = C$.
- **Indistinguishability: Refer next slide**

Indistinguishability Framework



Distinguishes E_K or RP?

Strong VS Weak

- If the key recovery resistance is broken on a block cipher, the other two notions are broken **automatically**.
  - $\Longrightarrow$ Key recovery resistance is the weakest security notion among the three

Designers point of view

Key recovery resistance is the easiest security notion to satisfy

Attackers point of view

Key recovery resistance is the hardest security notion to break.

- In general, block ciphers are expected to have **ideal** security.
- Thus, **efficiently** breaking **indistinguishability** is considered to be a significant vulnerability for block ciphers

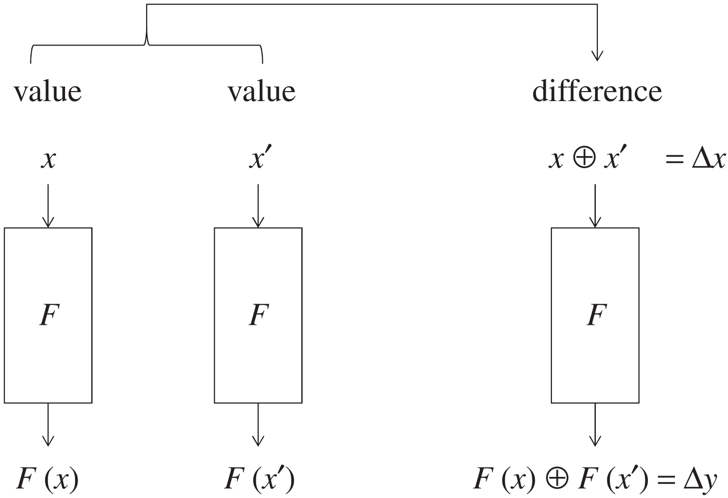
The Shortcut Attacks

The complexity of a shortcut attack must satisfy all of the following three conditions.

$$Data < 2^b,\ Time < 2^k,\ Memory < 2^k$$

Our First Shortcut Attack:
Differential Cryptanalysis

The Notion of Difference



value

value

difference

x

x'

$x \oplus x' \quad = \Delta x$

F

F

F

$F(x)$

$F(x')$

$F(x) \oplus F(x') = \Delta y$

AES Linear Layer

$$\begin{bmatrix} \texttt{2} & \texttt{3} & \texttt{1} & \texttt{1} \\ \texttt{1} & \texttt{2} & \texttt{3} & \texttt{1} \\ \texttt{1} & \texttt{1} & \texttt{2} & \texttt{3} \\ \texttt{3} & \texttt{1} & \texttt{1} & \texttt{2} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Figure: Zero Input Diff

AES Linear Layer

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Figure: Zero Input Diff

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \Delta \\ 0 \end{bmatrix} = \begin{bmatrix} \Delta \\ 3\Delta \\ 2\Delta \\ \Delta \end{bmatrix}$$

Figure: Non-Zero Input Diff

AES Linear Layer

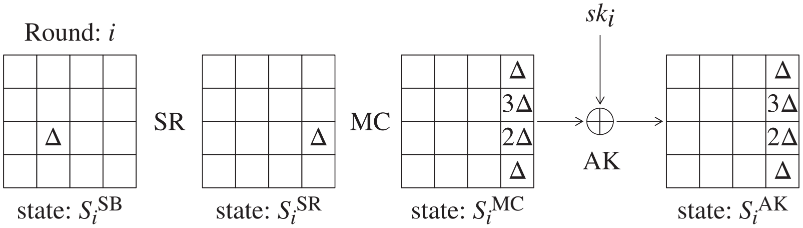
$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Figure: Zero Input Diff

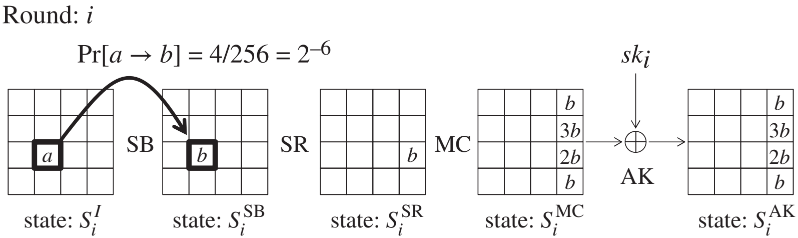
$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ \Delta \\ 0 \end{bmatrix} = \begin{bmatrix} \Delta \\ 3\Delta \\ 2\Delta \\ \Delta \end{bmatrix}$$

Figure: Non-Zero Input Diff

Diff. Through Linear Operations


Round: i
Δ
SR
Δ
MC
Δ
3Δ
2Δ
Δ
sk_i
AK
Δ
3Δ
2Δ
Δ
state: S_i^{SB}
state: S_i^{SR}
state: S_i^{MC}
state: S_i^{AK}

AES One Round Diff. Propagation

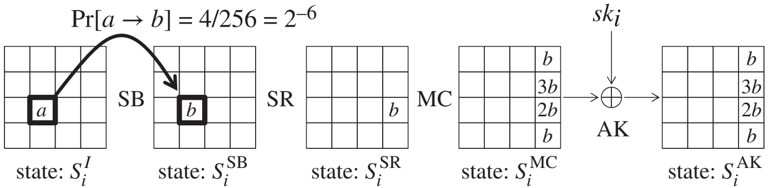


- From DDT,

$$\texttt{max differential prob} = \frac{1}{2^6}$$

AES Two Rounds Diff. Prob. $= 2^{-30}$

Round: i



$\Pr[a \to b] = 4/256 = 2^{-6}$

state: S_i^I

	a		

state: S_i^{SB}

	b		

state: S_i^{SR}

			b

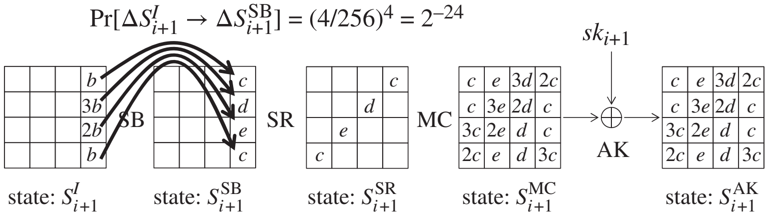
state: S_i^{MC}

			b
			$3b$
			$2b$
			b

state: S_i^{AK}

			b
			$3b$
			$2b$
			b

Round: $i + 1$



$\Pr[\Delta S_{i+1}^I \to \Delta S_{i+1}^{SB}] = (4/256)^4 = 2^{-24}$

state: S_{i+1}^I

			b
			$3b$
			$2b$
			b

state: S_{i+1}^{SB}

			c
			d
			e
			c

state: S_{i+1}^{SR}

			c
		d	
	e		
c			

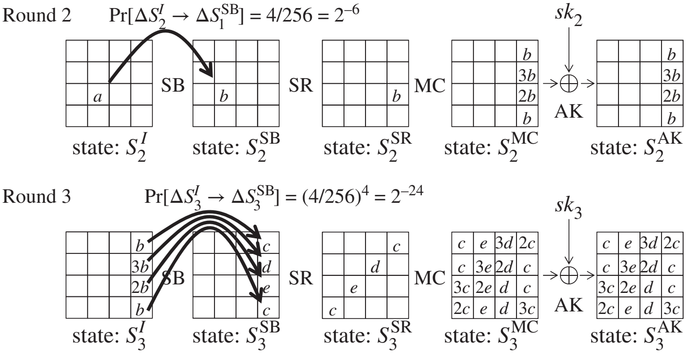
state: S_{i+1}^{MC}

c	e	$3d$	$2c$
c	$3e$	$2d$	c
$3c$	$2e$	d	c
$2c$	e	d	$3c$

state: S_{i+1}^{AK}

c	e	$3d$	$2c$
c	$3e$	$2d$	c
$3c$	$2e$	d	c
$2c$	e	d	$3c$

AES TWO → Three Rounds

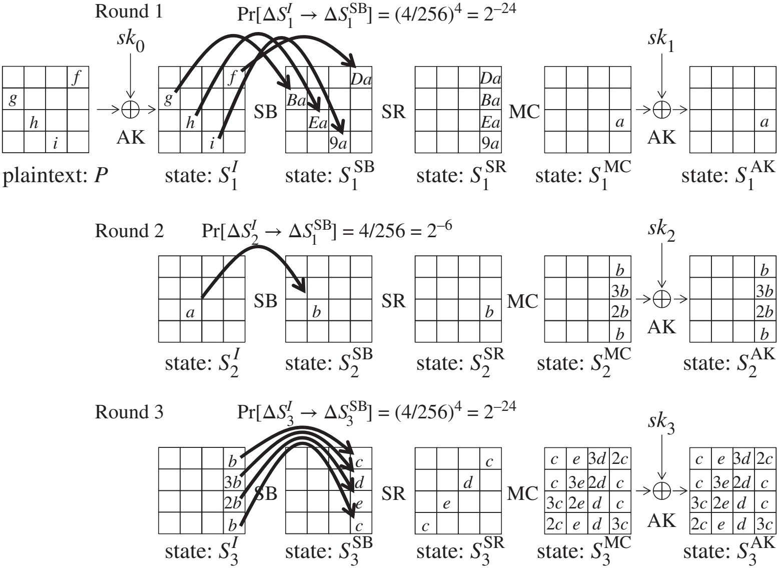


Round 2 $\Pr[\Delta S_2^I \rightarrow \Delta S_1^{\mathrm{SB}}] = 4/256 = 2^{-6}$

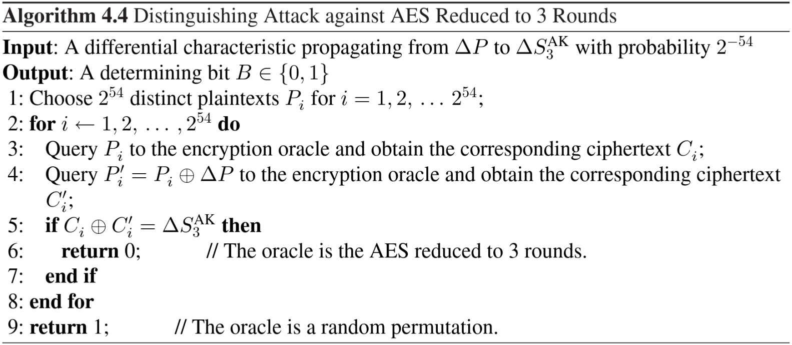
Round 3 $\Pr[\Delta S_3^I \rightarrow \Delta S_3^{\mathrm{SB}}] = (4/256)^4 = 2^{-24}$

a
SB
b
SR
b
MC
b
3b
2b
b
sk_2
AK
b
3b
2b
b
state: S_2^I
state: S_2^{SB}
state: S_2^{SR}
state: S_2^{MC}
state: S_2^{AK}
b
3b
2b
b
SB
c
d
e
c
SR
c
d
e
c
MC
c e 3d 2c
c 3e 2d c
3c 2e d c
2c e d 3c
sk_3
AK
c e 3d 2c
c 3e 2d c
3c 2e d c
2c e d 3c
state: S_3^I
state: S_3^{SB}
state: S_3^{SR}
state: S_3^{MC}
state: S_3^{AK}

AES Three Rounds Diff. Prob. $= 2^{-54}$



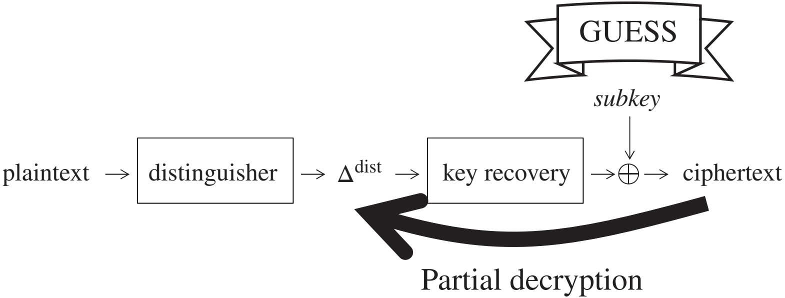
Distinguishing Attack against AES Reduced to 3 Rounds



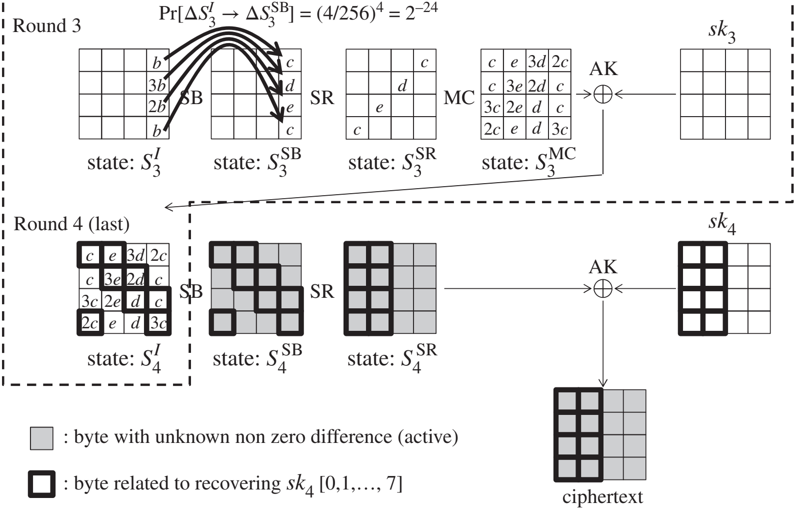
Algorithm 4.4 Distinguishing Attack against AES Reduced to 3 Rounds

```
Input: A differential characteristic propagating from $\Delta P$ to $\Delta S_3^{\mathrm{AK}}$ with probability $2^{-54}$
Output: A determining bit $B \in \{0, 1\}$
Choose $2^{54}$ distinct plaintexts $P_i$ for $i = 1, 2, \ldots 2^{54}$;
for $i \leftarrow 1, 2, \ldots, 2^{54}$ do
    Query $P_i$ to the encryption oracle and obtain the corresponding ciphertext $C_i$;
    Query $P'_i = P_i \oplus \Delta P$ to the encryption oracle and obtain the corresponding ciphertext $C'_i$;
    if $C_i \oplus C'_i = \Delta S_3^{\mathrm{AK}}$ then
        return 0;          // The oracle is the AES reduced to 3 rounds.
    end if
end for
return 1;          // The oracle is a random permutation.
```

Recall — Key Recovery Framework



Recovering left half of last Sub-key

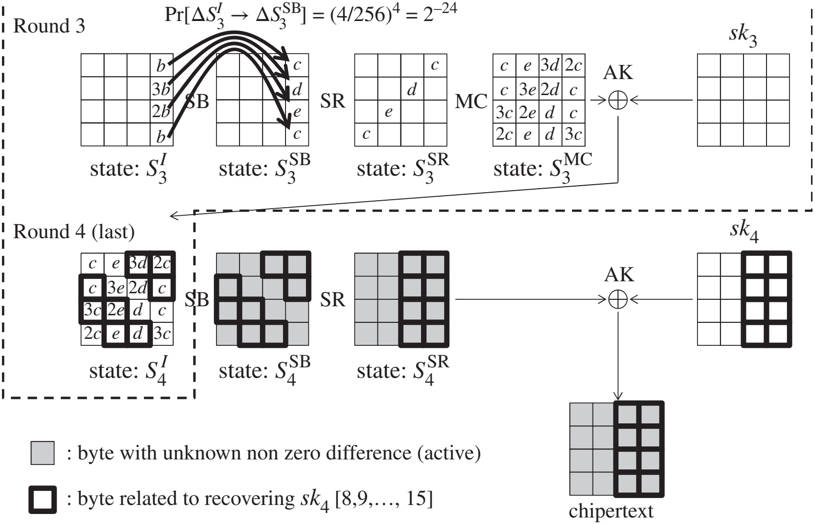


$\Pr[\Delta S_3^I \rightarrow \Delta S_3^{SB}] = (4/256)^4 = 2^{-24}$

▨ : byte with unknown non zero difference (active)

□ : byte related to recovering sk_4 [0,1,…, 7]

Recovering right half of last Sub-key



▨ : byte with unknown non zero difference (active)

□ : byte related to recovering sk_4 [8,9,…, 15]

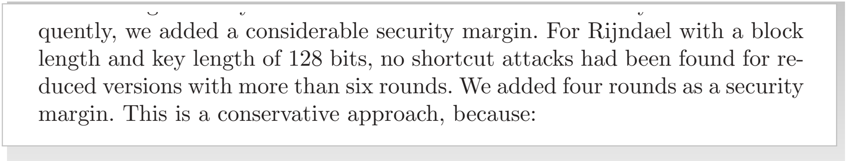
The Number of Rounds?

AES-128	10
AES-192	12
AES-256	14

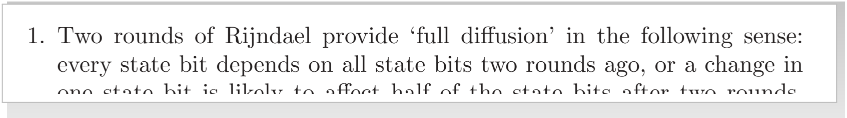
The Design Rationale

Reference: The Design of Rijndael (Section 3.5)

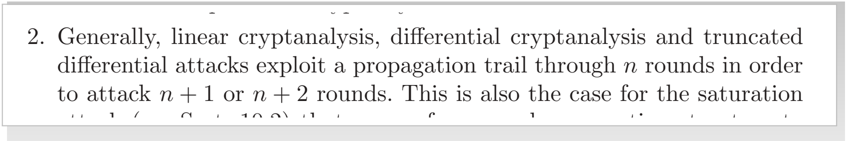
10 Rounds



quently, we added a considerable security margin. For Rijndael with a block length and key length of 128 bits, no shortcut attacks had been found for reduced versions with more than six rounds. We added four rounds as a security margin. This is a conservative approach, because:



1. Two rounds of Rijndael provide 'full diffusion' in the following sense: every state bit depends on all state bits two rounds ago, or a change in one state bit is likely to affect half of the state bits after two rounds.



2. Generally, linear cryptanalysis, differential cryptanalysis and truncated differential attacks exploit a propagation trail through n rounds in order to attack $n + 1$ or $n + 2$ rounds. This is also the case for the saturation

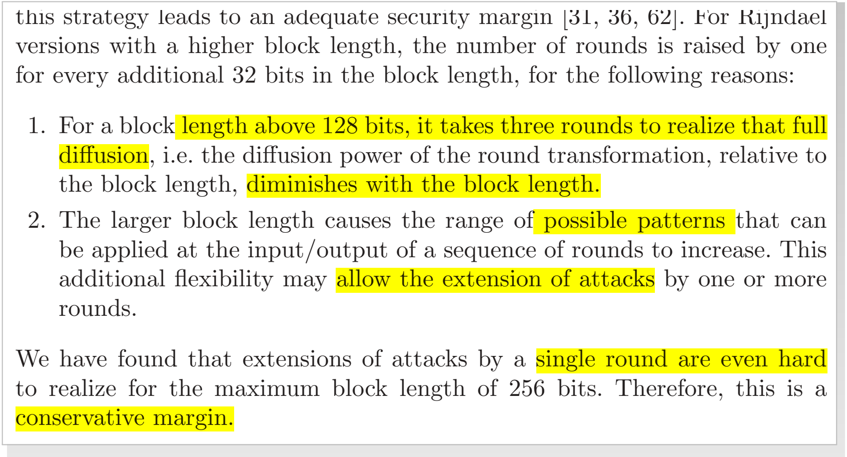
12/14 Rounds AES-192/256

#Rounds++ for |Key|+=32

> For Rijndael versions with a longer key, the number of rounds was raised by one for every additional 32 bits in the cipher key. This was done for the following reasons:
>
> 1. One of the main objectives is the absence of shortcut attacks, i.e. attacks that are more efficient than an exhaustive key search. Since the workload of an exhaustive key search grows with the key length, shortcut attacks can afford to be less efficient for longer keys.
> 2. (Partially) known-key and related-key attacks exploit the knowledge of cipher key bits or the ability to apply different cipher keys. If the cipher key grows, the range of possibilities available to the cryptanalyst increases.

Non-standard AES Larger Block Size

#Rounds++ for |Key|+=32



this strategy leads to an adequate security margin [31, 36, 62]. For Rijndael versions with a higher block length, the number of rounds is raised by one for every additional 32 bits in the block length, for the following reasons:

1. For a block length above 128 bits, it takes three rounds to realize that full diffusion, i.e. the diffusion power of the round transformation, relative to the block length, diminishes with the block length.
2. The larger block length causes the range of possible patterns that can be applied at the input/output of a sequence of rounds to increase. This additional flexibility may allow the extension of attacks by one or more rounds.

We have found that extensions of attacks by a single round are even hard to realize for the maximum block length of 256 bits. Therefore, this is a conservative margin.

The Verdict

Number of rounds (N_r) as a function of N_b and N_k

	N_b				
N_k	4	5	6	7	8
4	10	11	12	13	14
5	11	11	12	13	14
6	12	12	12	13	14
7	13	13	13	13	14
8	14	14	14	14	14

$$N_b = \frac{\textit{block length}}{32} \qquad N_k = \frac{\textit{key length}}{32}$$

Next Class: Complexity Analysis