Cryptology: Data Encryption Standard

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES

Table of Contents

Encipherment

Encipherment

- Split the input into left and right halves: L and R

Encipherment

Encipherment

- Split the input into left and right halves: L and R
- Shift the right half, R, to the left

Encipherment

Encipherment

- Split the input into left and right halves: L and R
- Shift the right half, R, to the left
- "Add" the left half, L, to $f(R, K_i)$, where K_i is the round key and shift right

Encipherment

Encipherment

- Split the input into left and right halves: L and R
- Shift the right half, R, to the left
- "Add" the left half, L, to $f(R, K_i)$, where K_i is the round key and shift right
- Repeat the previous steps except for the last round

Encipherment

Encipherment

- Split the input into left and right halves: L and R
- Shift the right half, R, to the left
- "Add" the left half, L, to $f(R, K_i)$, where K_i is the round key and shift right
- Repeat the previous steps except for the last round
- In the last round swap the left and right halves then rejoin them

Encipherment

"hi"$\equiv$ (11010001101001)

Encipherment

"hi" $\equiv$ (11010001101001)

$L_0 = (1101000)$ $\quad$ $R_0 = (1101001)$

Encipherment

$$\text{“hi”} \equiv (11010001101001)$$

$$L_0 = (1101000) \qquad R_0 = (1101001)$$

$$R_1 = L_0 \oplus R_0 \oplus K_0 = (1101000) \oplus (1101001) \oplus (1110011)$$

Encipherment

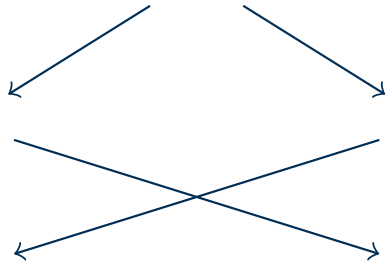
$$\text{“hi”} \equiv (11010001101001)$$

$$L_0 = (1101000) \qquad R_0 = (1101001)$$

$$R_1 = L_0 \oplus R_0 \oplus K_0 = (1110010)$$

Encipherment

"hi" $\equiv (11010001101001)$

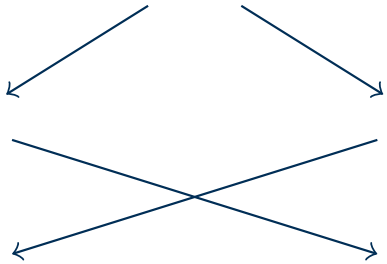


$L_0 = (1101000)$ $\quad R_0 = (1101001)$

$L_1 = (1101001)$ $\quad R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

Encipherment

"hi"$\equiv (11010001101001)$



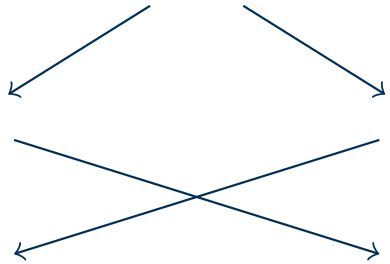
$L_0 = (1101000)$ $\quad R_0 = (1101001)$

$L_1 = (1101001)$ $\quad R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

$$R_2 = L_1 \oplus R_1 \oplus K_1 = (1101001) \oplus (1110010) \oplus (1100111)$$

Encipherment

"hi"$\equiv (11010001101001)$



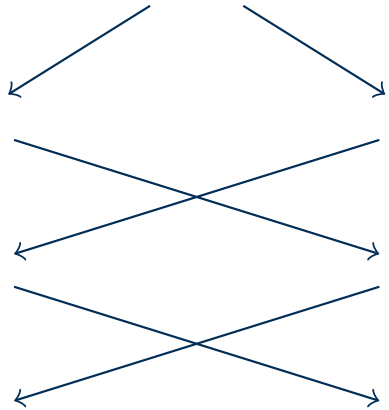
$L_0 = (1101000)$ $\quad R_0 = (1101001)$

$L_1 = (1101001)$ $\quad R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

$$R_2 = L_1 \oplus R_1 \oplus K_1 = (1111100)$$

Encipherment

"hi"$\equiv (11010001101001)$



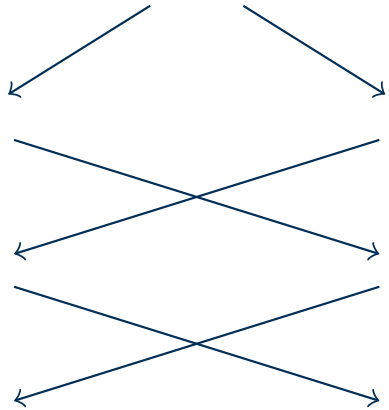
$L_0 = (1101000)$ $\quad R_0 = (1101001)$

$L_1 = (1101001)$ $\quad R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

$L_2 = (1110010)$ $\quad R_2 = L_1 \oplus f(R_1, K_1) = (1111100)$

Encipherment

"hi"$\equiv (11010001101001)$



$L_0 = (1101000)$ $\quad R_0 = (1101001)$

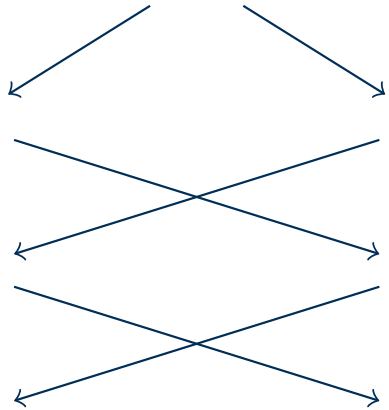
$L_1 = (1101001)$ $\quad R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

$L_2 = (1110010)$ $\quad R_2 = L_1 \oplus f(R_1, K_1) = (1111100)$

$$R_3 = L_2 \oplus R_2 \oplus K_2 = (1110010) \oplus (1111100) \oplus (1001111)$$

Encipherment

"hi"$\equiv (11010001101001)$



$L_0 = (1101000)$ $\quad R_0 = (1101001)$

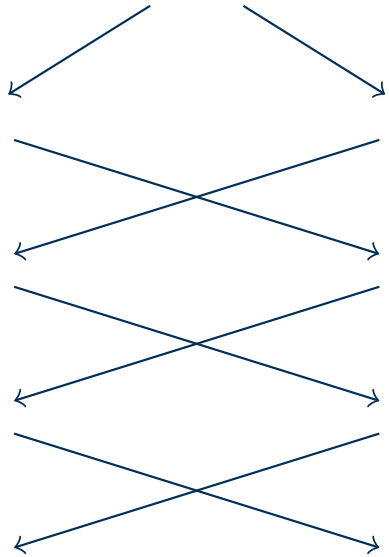
$L_1 = (1101001)$ $\quad R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

$L_2 = (1110010)$ $\quad R_2 = L_1 \oplus f(R_1, K_1) = (1111100)$

$$R_3 = L_2 \oplus R_2 \oplus K_2 = (1000001)$$

Encipherment

"hi"$\equiv (11010001101001)$



$L_0 = (1101000)$ $\quad R_0 = (1101001)$

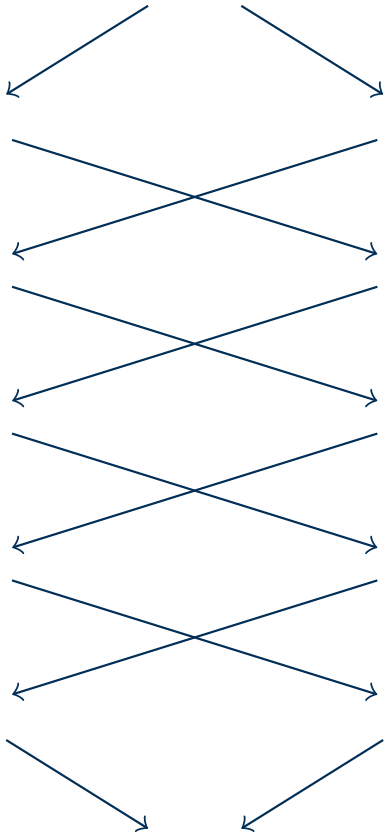
$L_1 = (1101001)$ $\quad R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

$L_2 = (1110010)$ $\quad R_2 = L_1 \oplus f(R_1, K_1) = (1111100)$

$L_3 = (1111100)$ $\quad R_3 = L_2 \oplus f(R_2, K_2) = (1000001)$

Encipherment

"hi"$\equiv (11010001101001)$



$L_0 = (1101000)$ $R_0 = (1101001)$

$L_1 = (1101001)$ $R_1 = L_0 \oplus f(R_0, K_0) = (1110010)$

$L_2 = (1110010)$ $R_2 = L_1 \oplus f(R_1, K_1) = (1111100)$

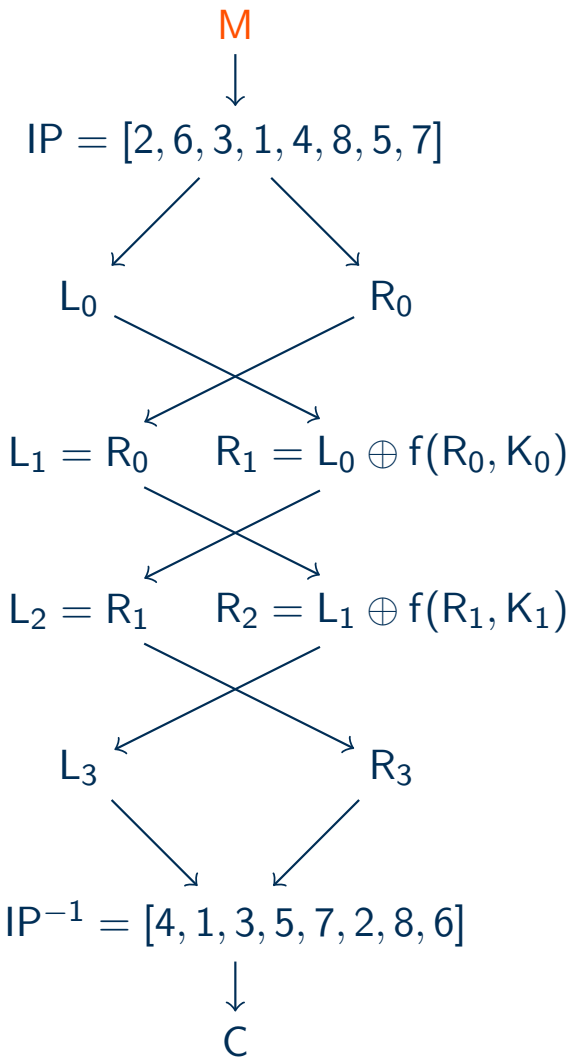
$L_3 = (1111100)$ $R_3 = L_2 \oplus f(R_2, K_2) = (1000001)$

$L_4 = (1000001)$ $R_4 = (1111100)$

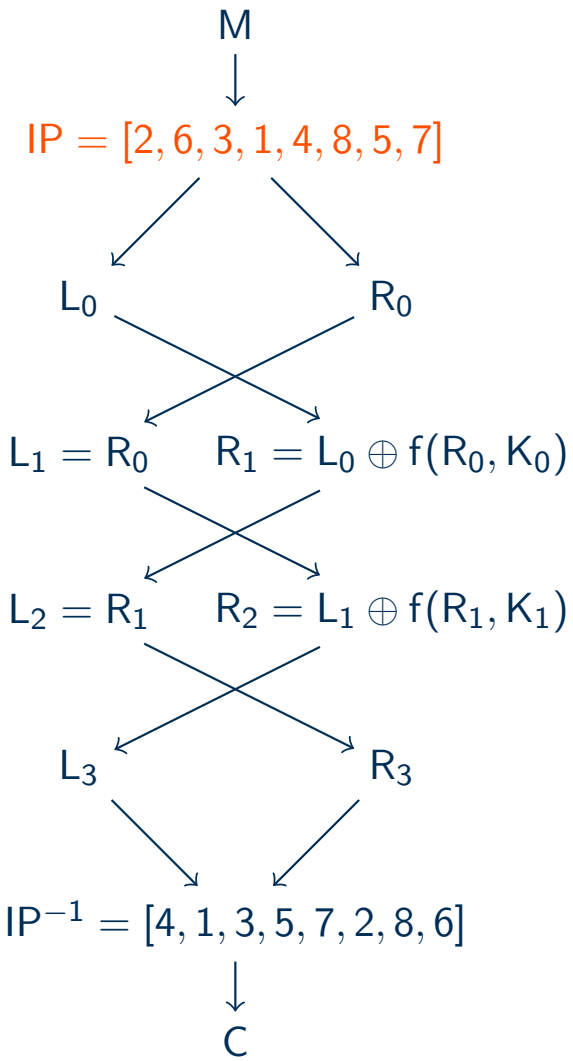
$(1111100\ 1110010)$

Table of Contents

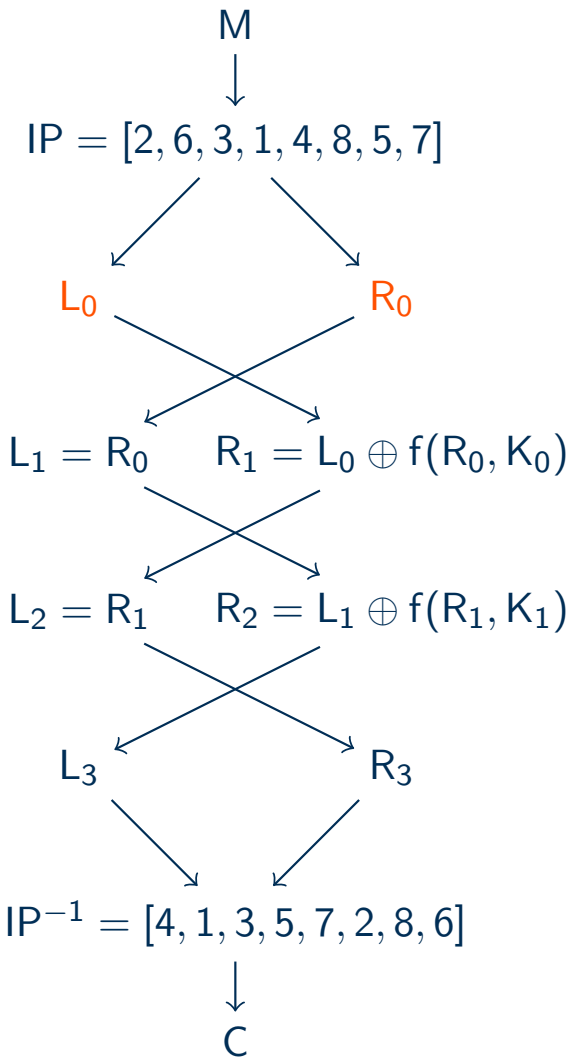
Really Simple DES Overview



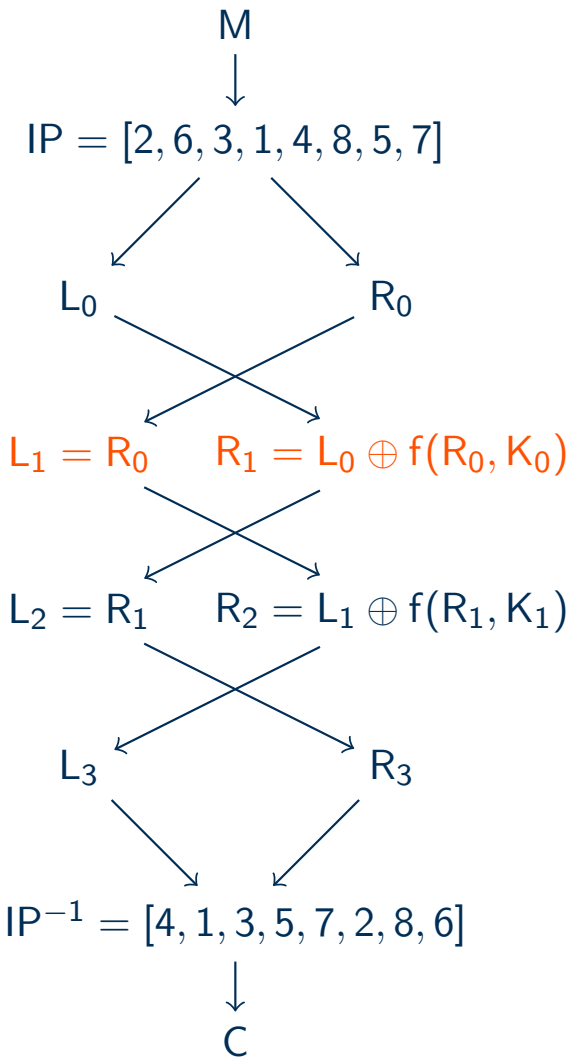
Really Simple DES Overview



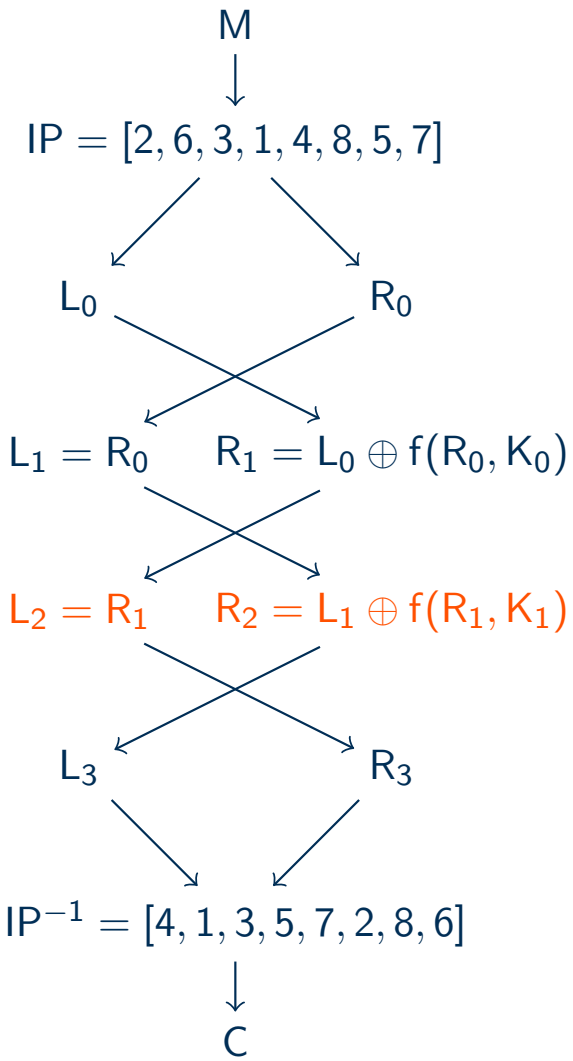
Really Simple DES Overview



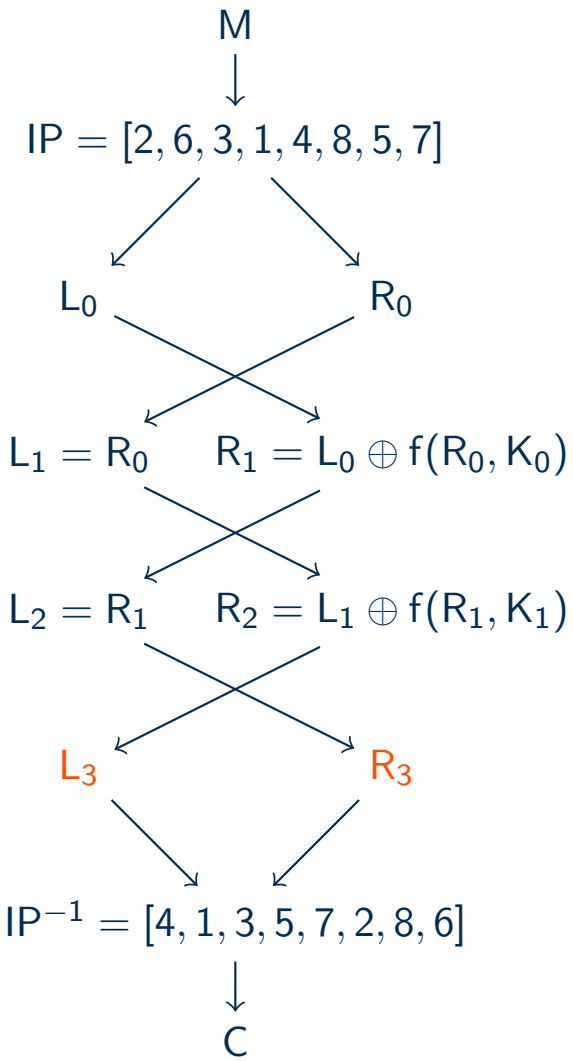
Really Simple DES Overview



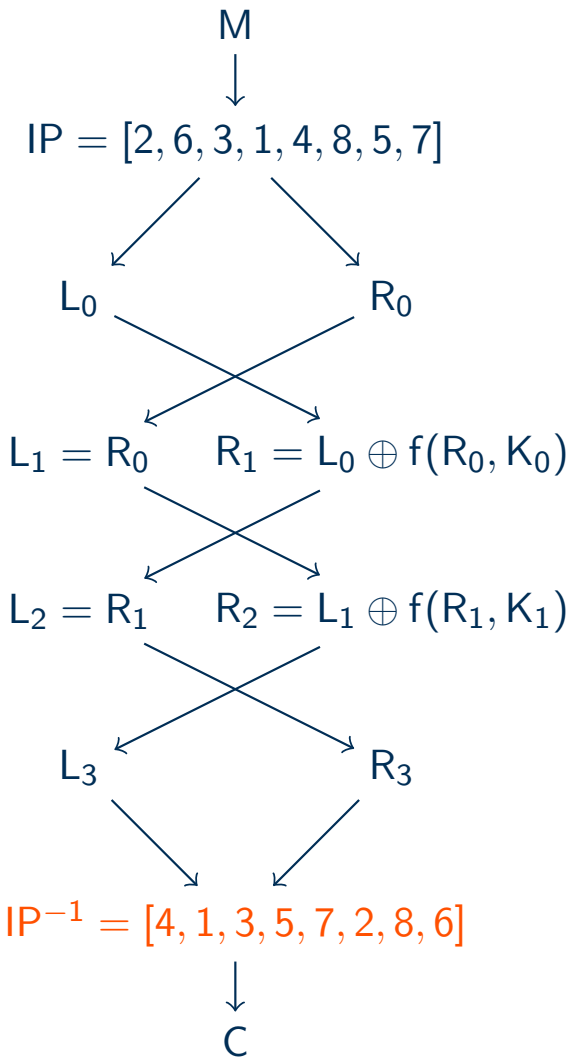
Really Simple DES Overview



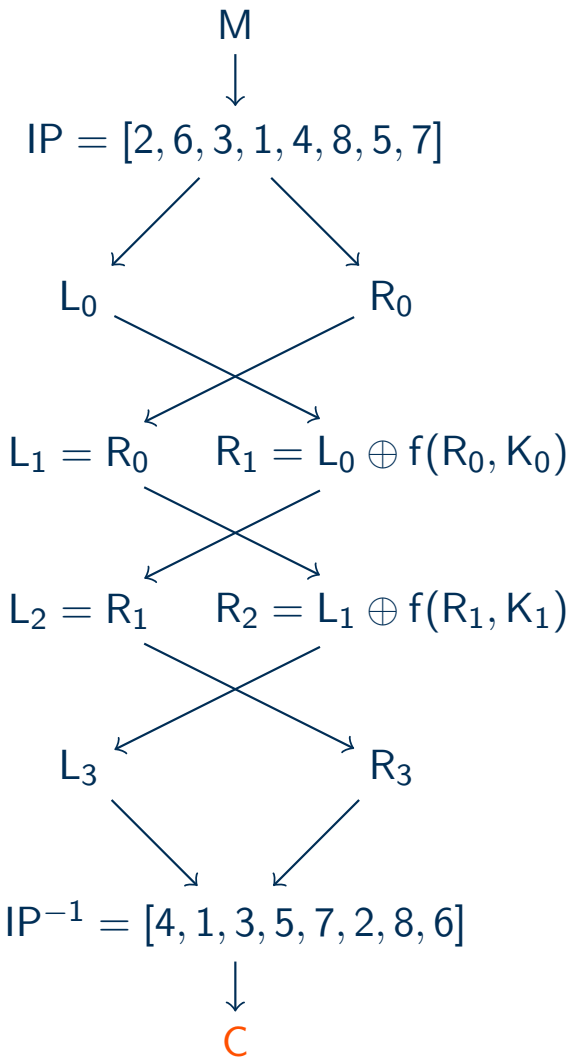
Really Simple DES Overview



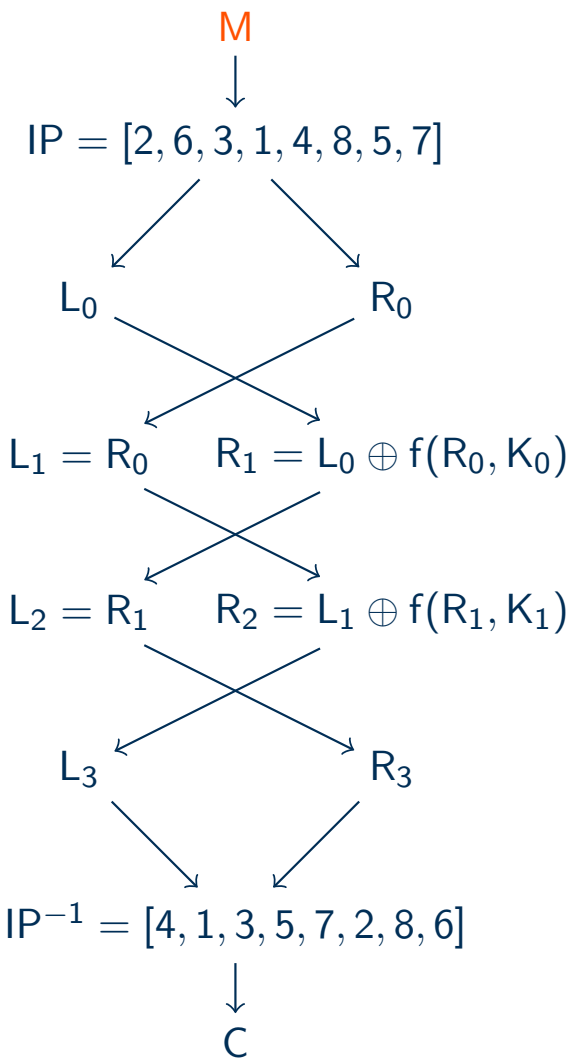
Really Simple DES Overview

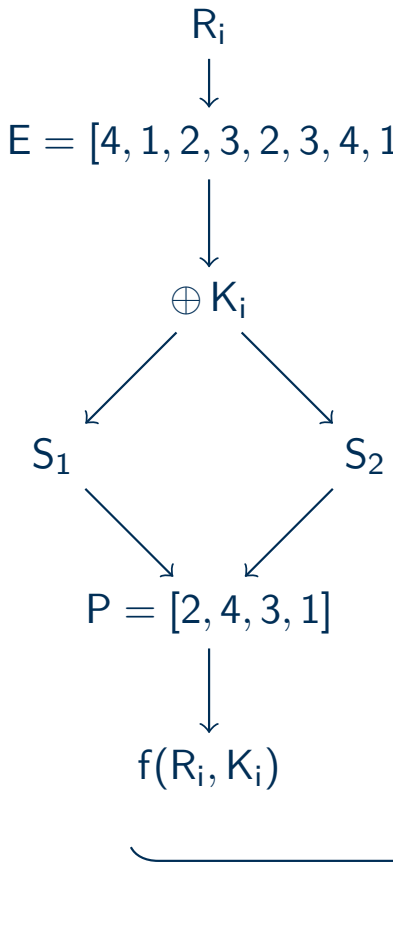


Really Simple DES Overview



Really Simple DES





$f(R_i, K_i)$

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

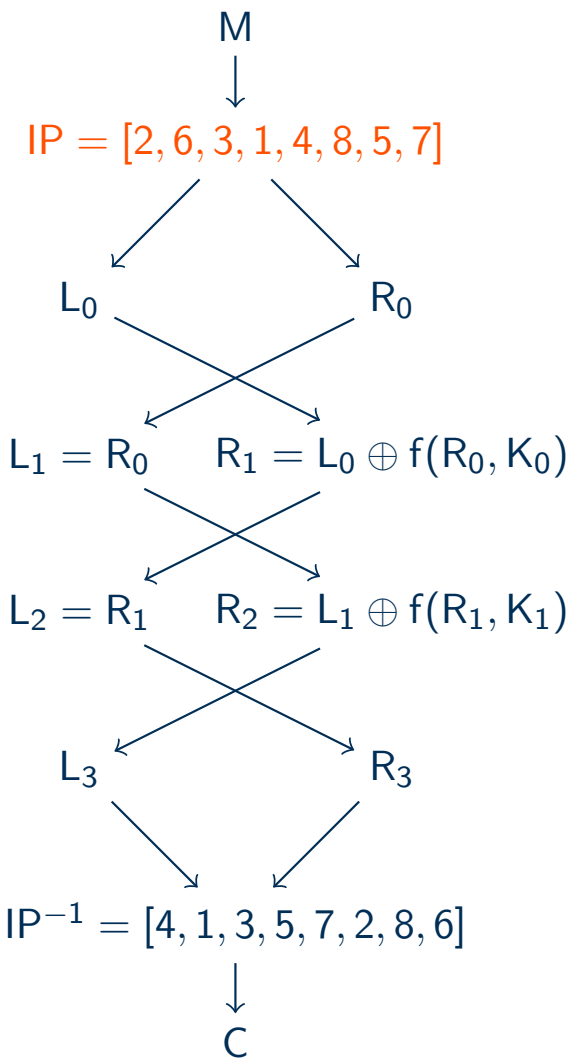
S-Box 1

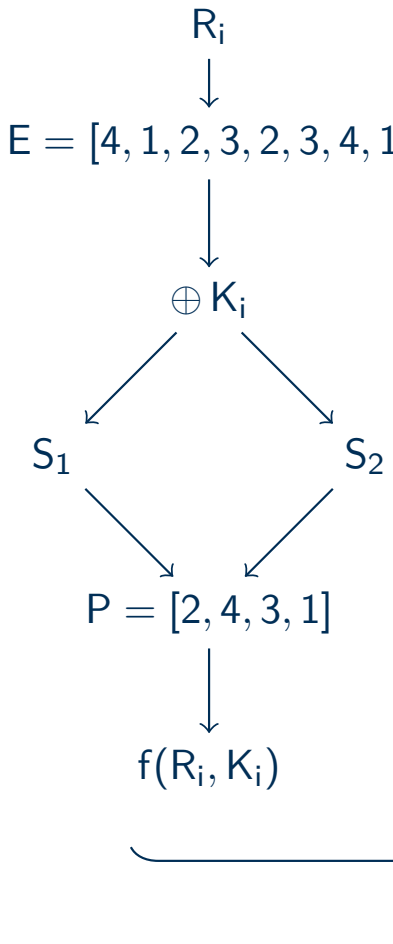
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Really Simple DES





$f(R_i, K_i)$

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

S-Box 1

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

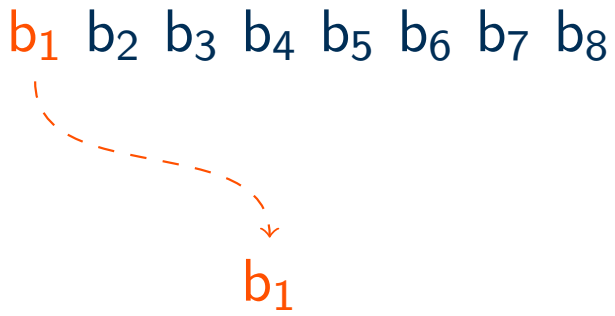
	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Permutations

$$b_1 \; b_2 \; b_3 \; b_4 \; b_5 \; b_6 \; b_7 \; b_8$$

Permutations

$$\text{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$



Permutations

$$\begin{array}{c} \\ \mathrm{IP} = [2,6,3,1,4,8,5,7] \end{array} \left\{ \begin{array}{cccccccc} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 \\ \downarrow & & & & & & & \\ b_2 & & & & & & & b_1 \end{array} \right.$$

Permutations

$$\text{IP} = [2, 6, 3, 1, 4, 8, 5, 7] \left\{ \begin{array}{cccccccc} b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 \\ & & \downarrow & & & & & \\ b_2 & & b_3 & b_1 & & & & \end{array} \right.$$

Permutations

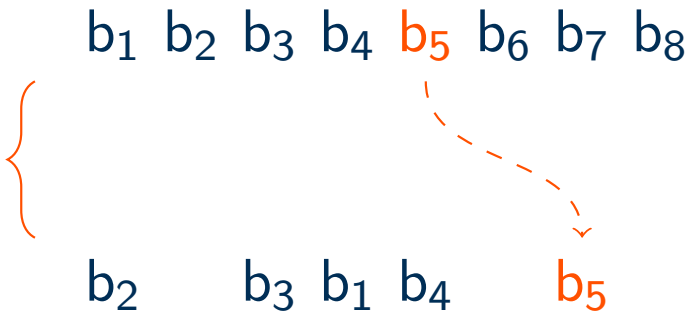
$$IP = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2 \quad b_3\ b_1\ b_4$$

Permutations

$$IP = [2, 6, 3, 1, 4, 8, 5, 7]$$



Permutations

$$\text{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2\ b_6\ b_3\ b_1\ b_4\ \ \ b_5$$

Permutations

$$IP = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2\ b_6\ b_3\ b_1\ b_4\ \quad b_5\ b_7$$

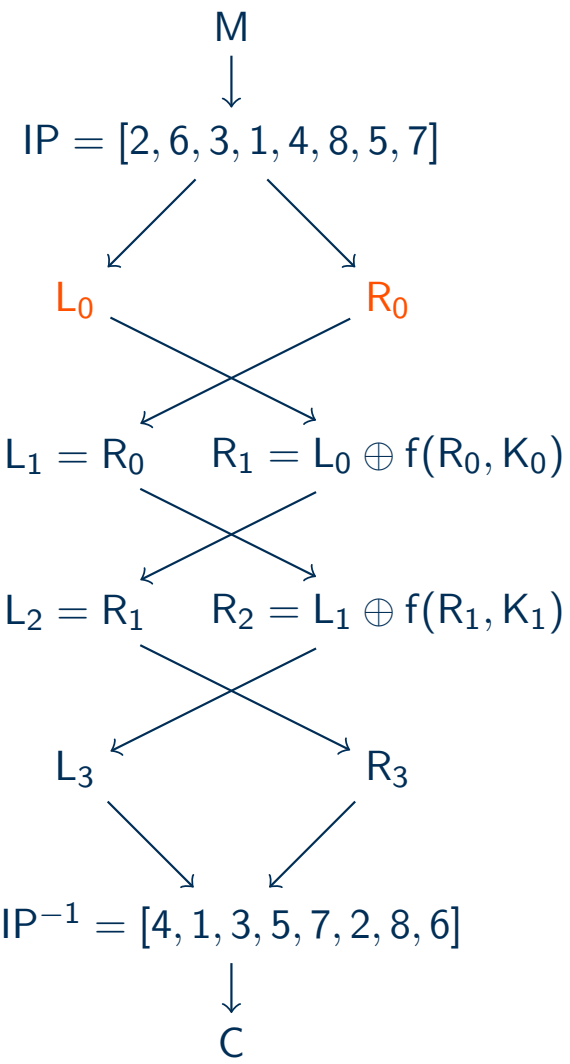
Permutations

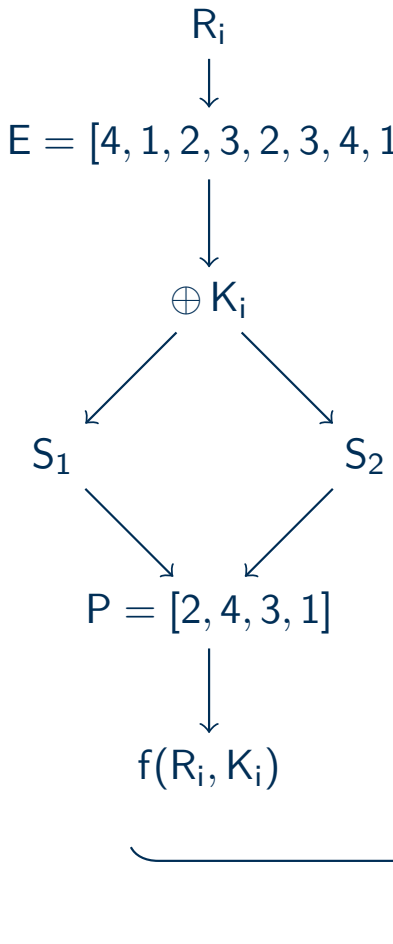
$$\text{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7$$

Really Simple DES





$f(R_i, K_i)$

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

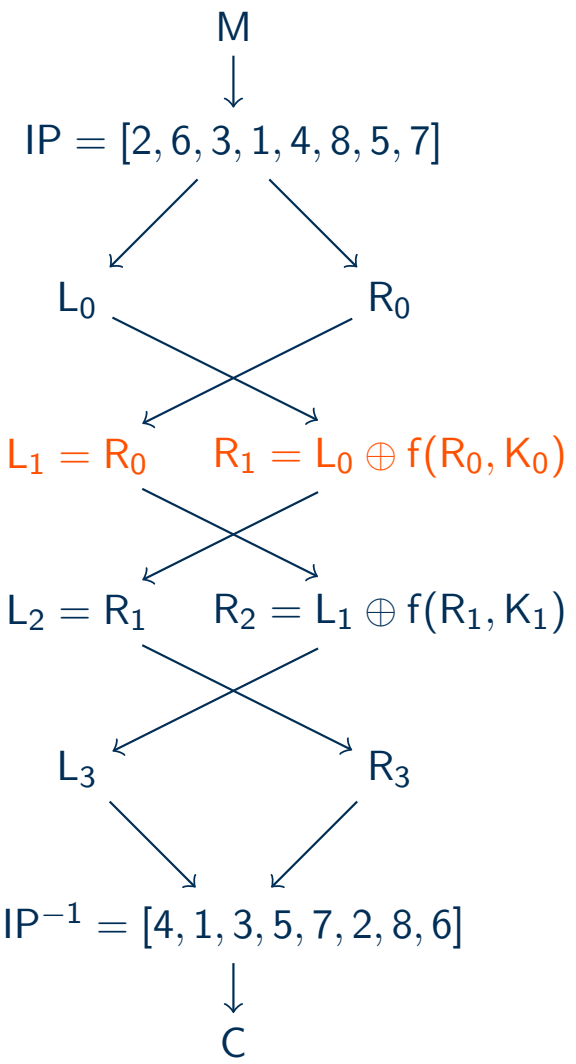
S-Box 1

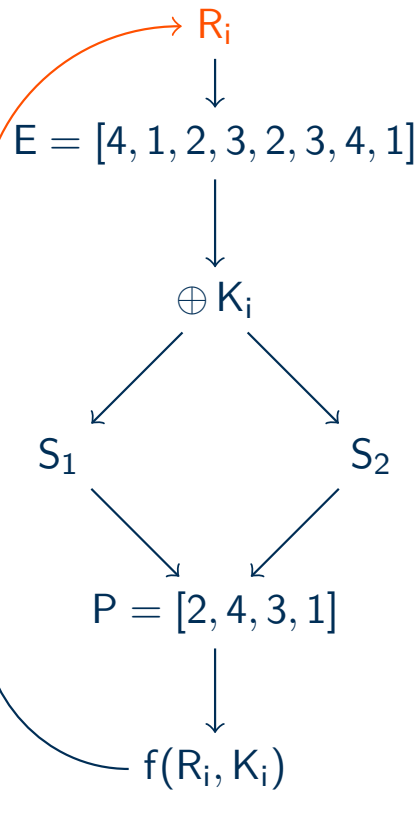
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Really Simple DES





f(Ri, Ki)

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

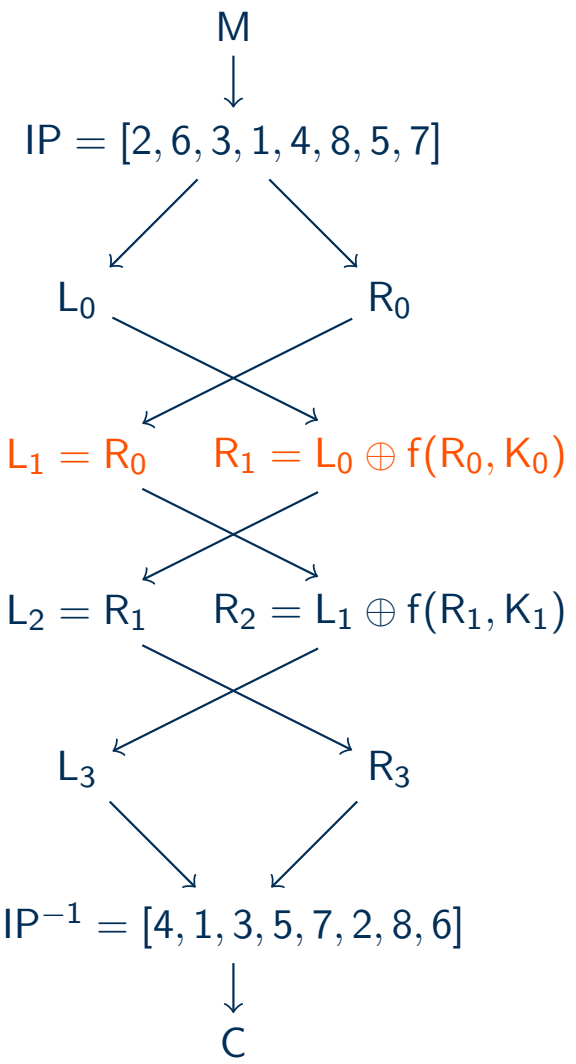
S-Box 1

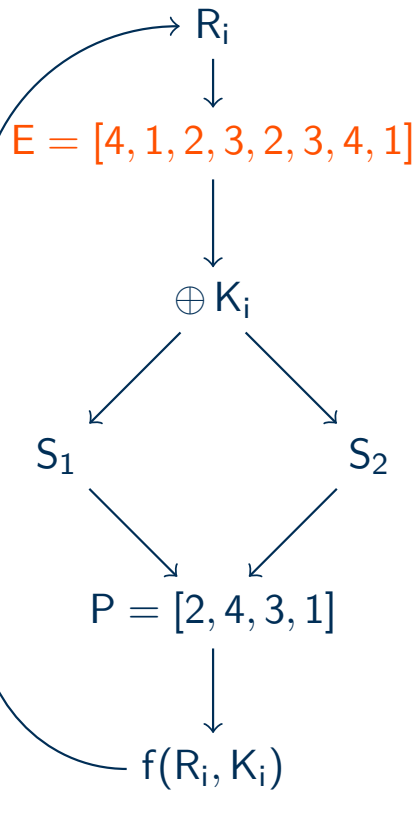
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Really Simple DES





f(Ri, Ki)

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

S-Box 1

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

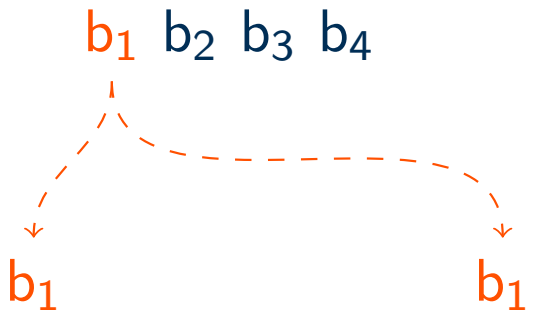
	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Expansion from 4 to 8 bits

$b_1\ b_2\ b_3\ b_4$

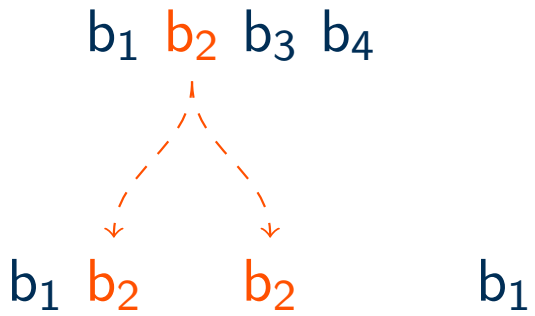
Expansion from 4 to 8 bits

$$E = [4, 1, 2, 3, 2, 3, 4, 1]$$



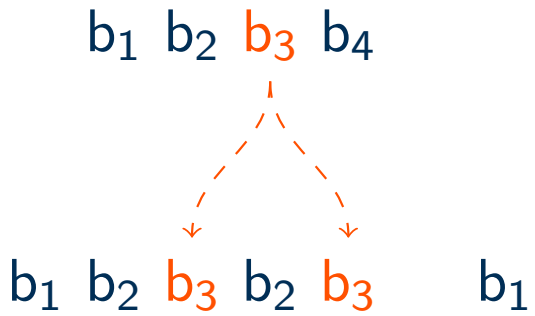
Expansion from 4 to 8 bits

$$E = [4, 1, 2, 3, 2, 3, 4, 1]$$



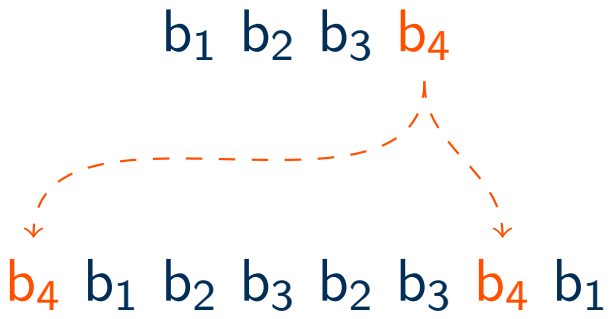
Expansion from 4 to 8 bits

$$E = [4, 1, 2, 3, 2, 3, 4, 1]$$

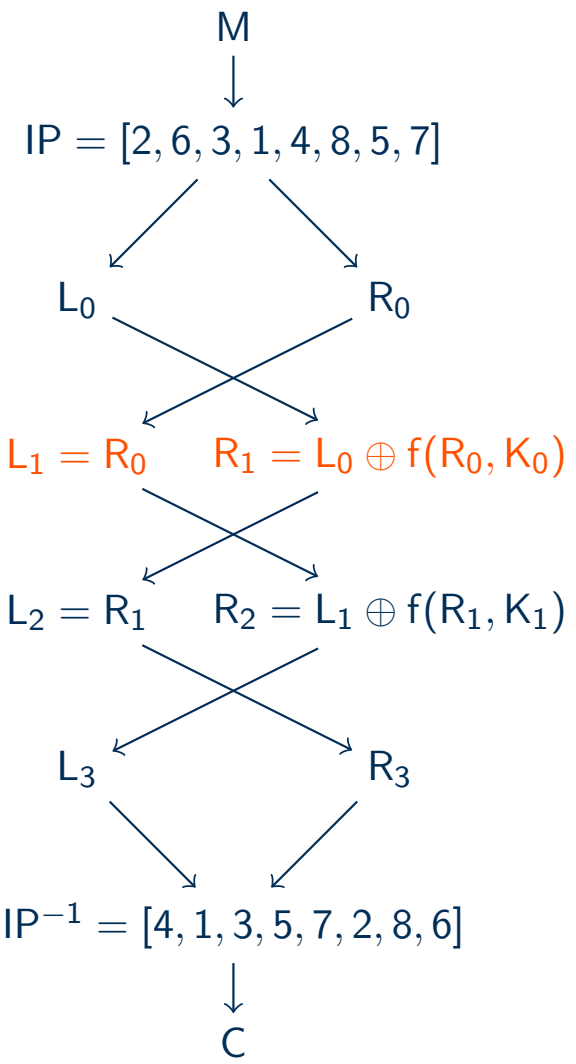


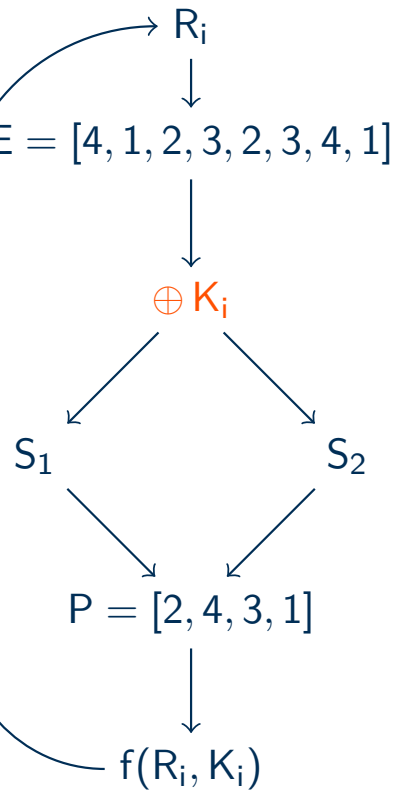
Expansion from 4 to 8 bits

$$E = [4, 1, 2, 3, 2, 3, 4, 1]$$



Really Simple DES





Key Schedule

Key 0: (11100111)

Key 1: (11001111)

S-Box 1

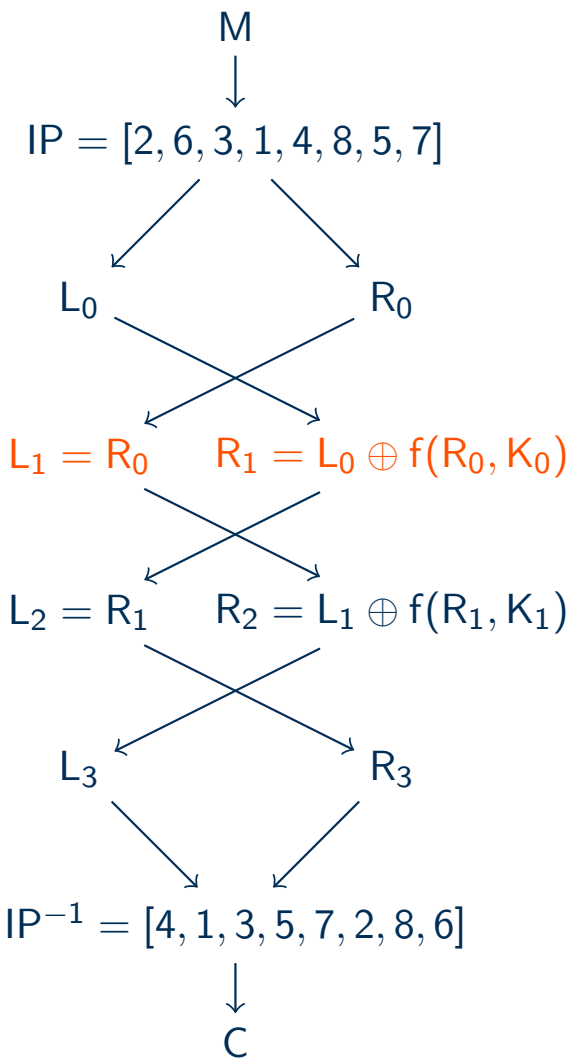
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

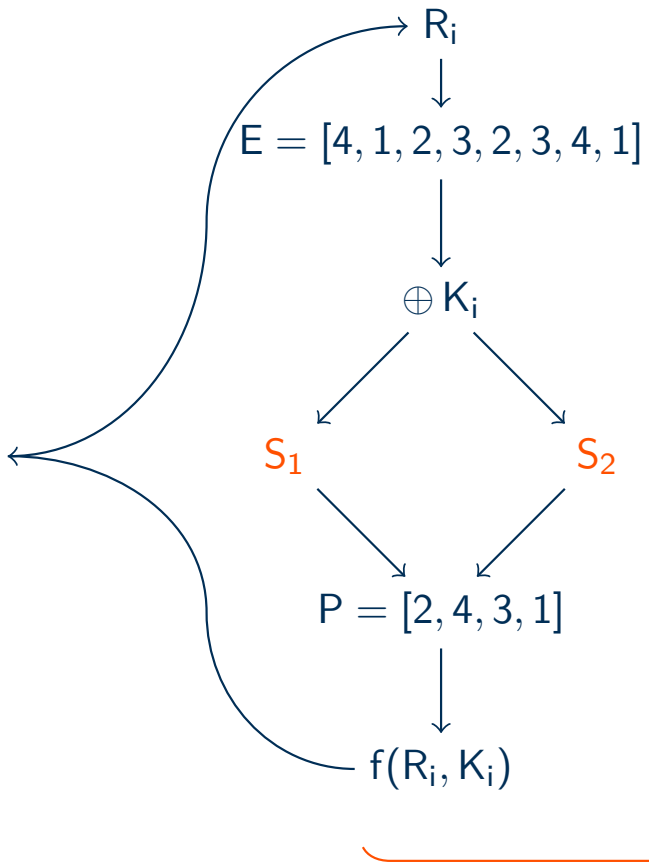
S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

$f(R_i, K_i)$

Really Simple DES





Key Schedule

Key 0: (11100111)

Key 1: (11001111)

S-Box 1

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

$f(R_i, K_i)$

Using S-Boxes

Look up (1101) in S-Box 1:

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

Using S-Boxes

Look up (1101) in S-Box 1:

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

Using S-Boxes

Look up (1101) in S-Box 1:

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

Using S-Boxes

Look up (1101) in S-Box 1:

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

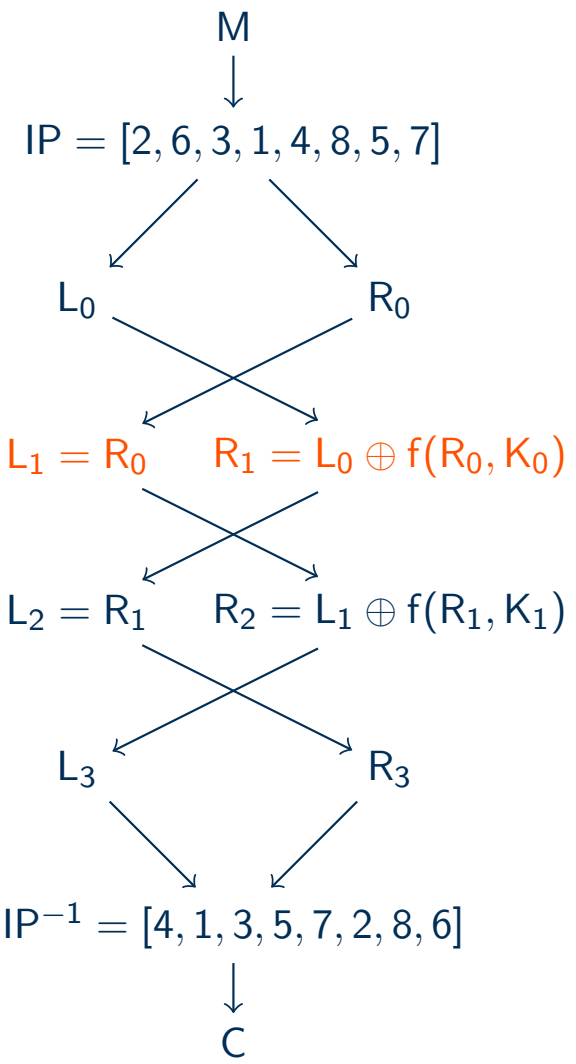
Using S-Boxes

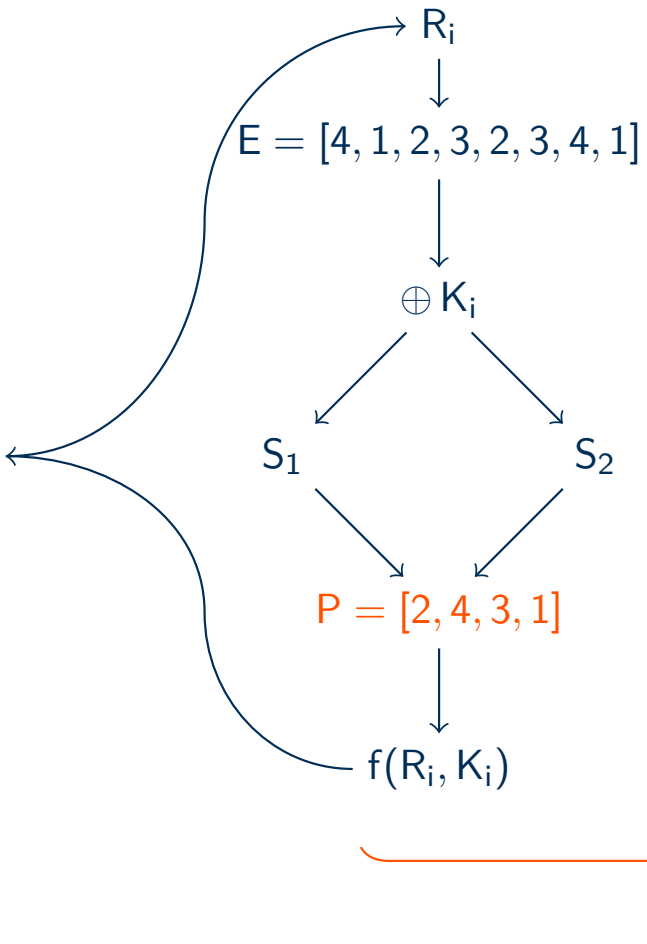
Look up (1101) in S-Box 1:

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

So the output is (01)

Really Simple DES





f(Ri, Ki)

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

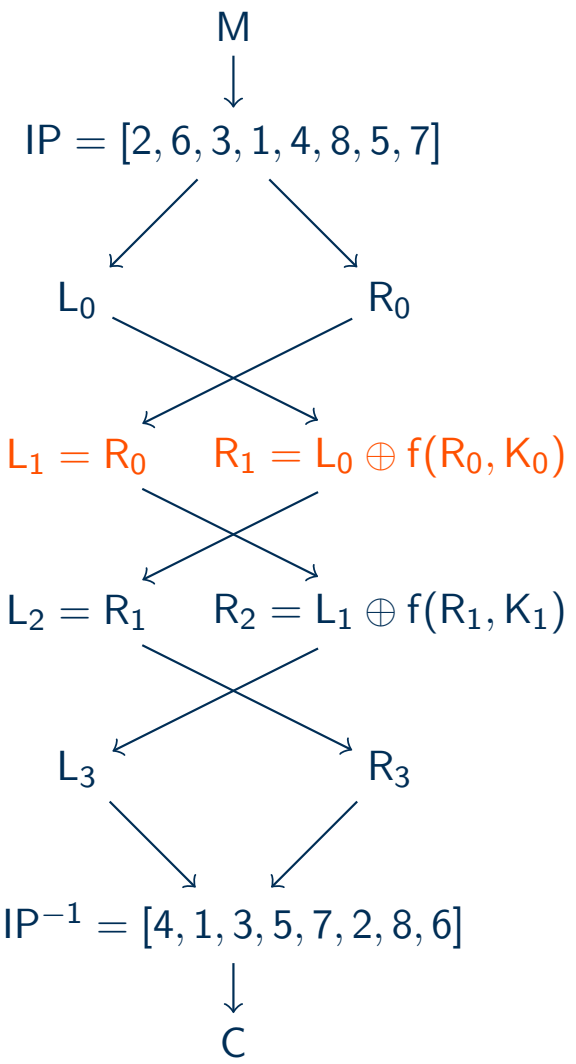
S-Box 1

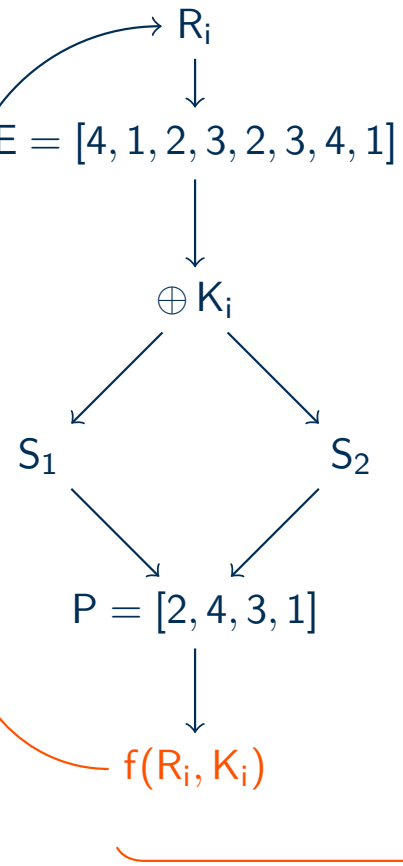
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Really Simple DES





f(Ri, Ki)

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

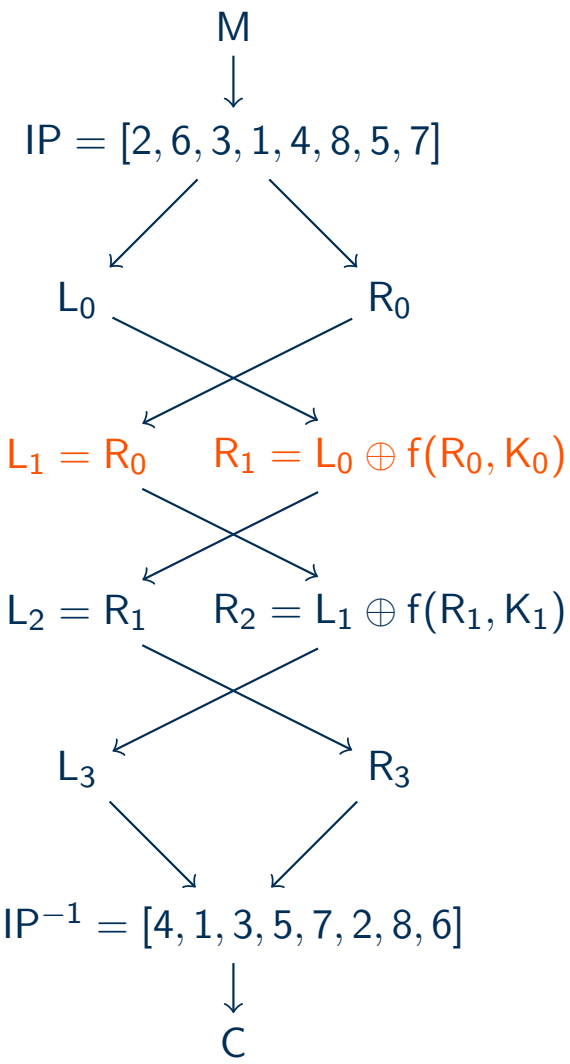
S-Box 1

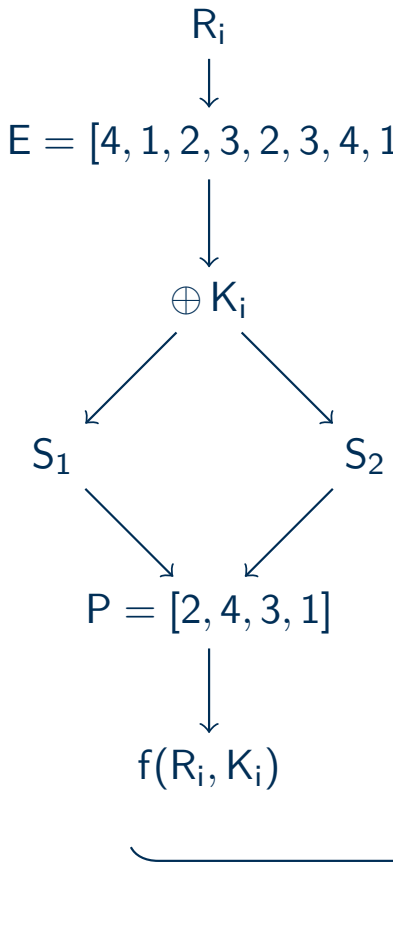
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Really Simple DES





$f(R_i, K_i)$

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

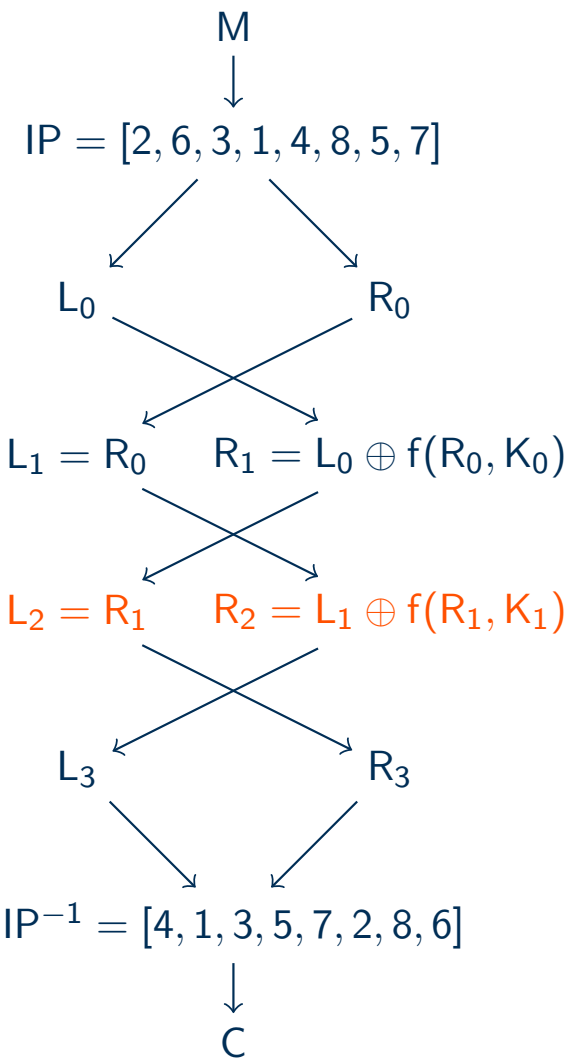
S-Box 1

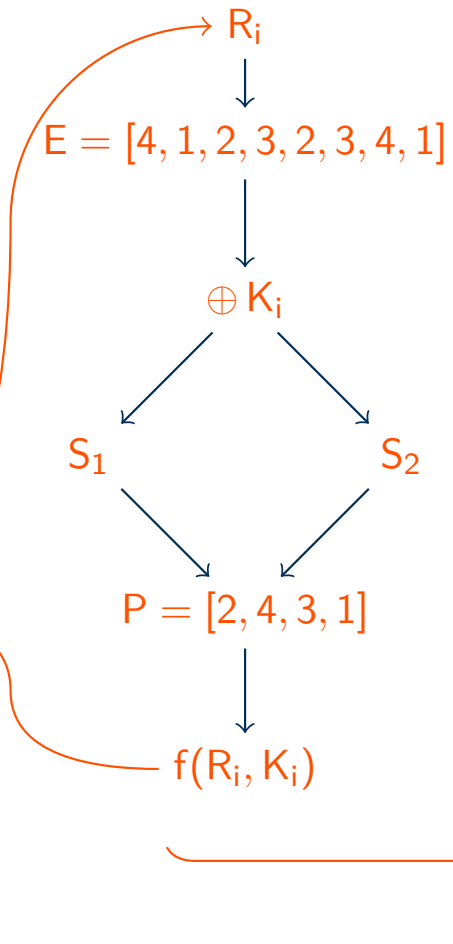
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Really Simple DES





Key Schedule

Key 0: (11100111)

Key 1: (11001111)

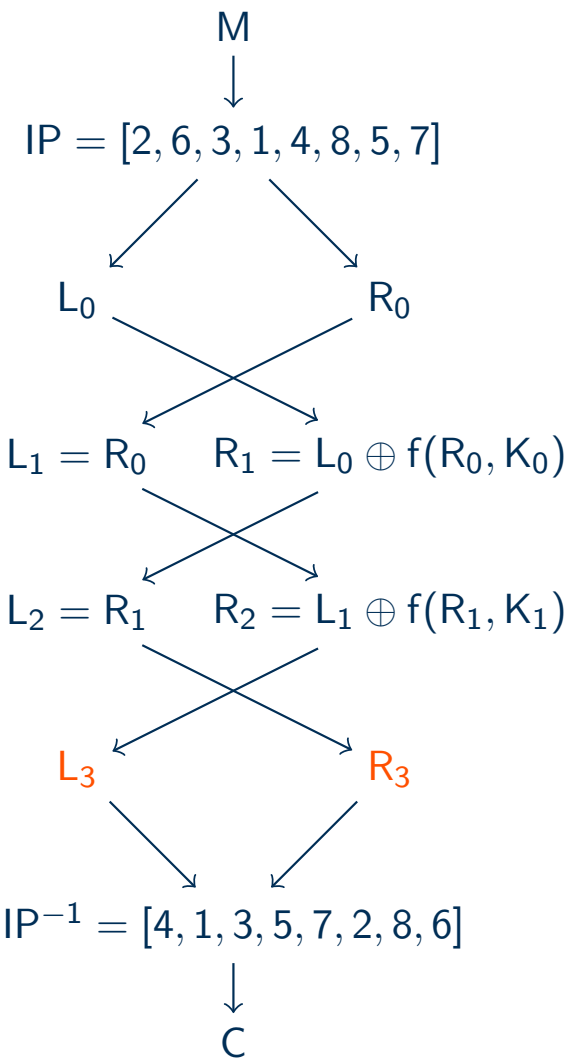
S-Box 1

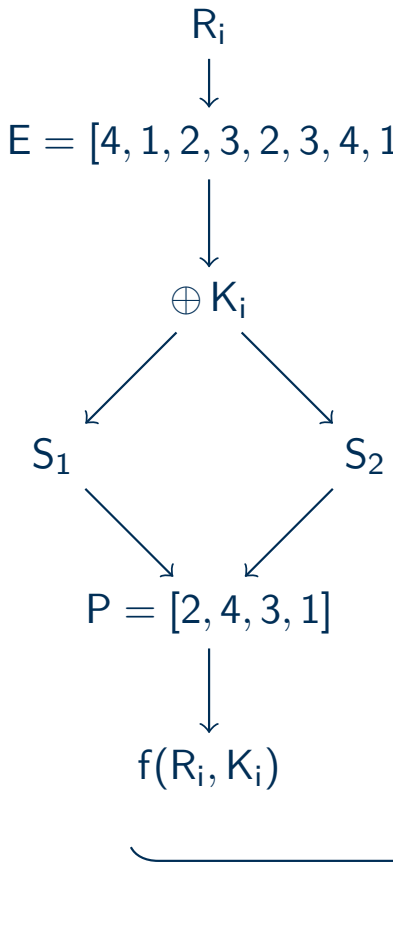
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Really Simple DES





Key Schedule

Key 0: (11100111)

Key 1: (11001111)

S-Box 1

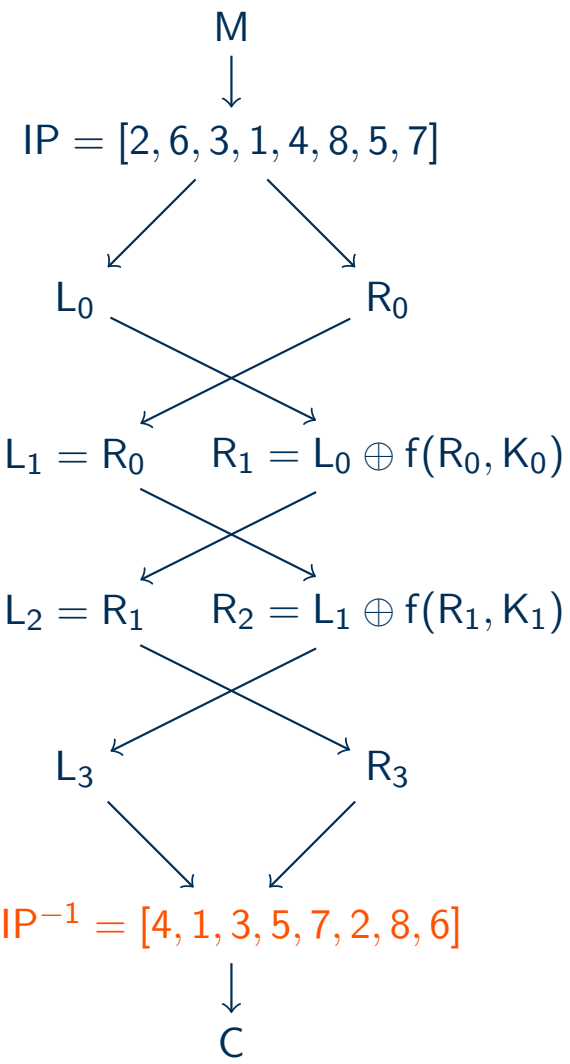
	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

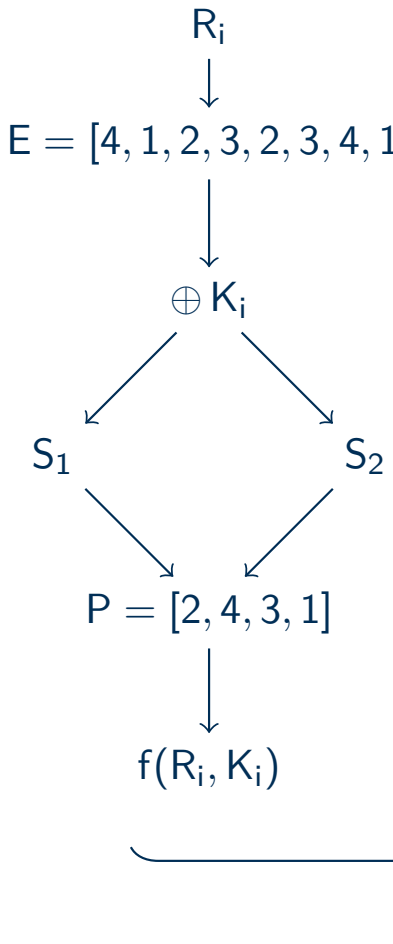
S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

$f(R_i, K_i)$

Really Simple DES





$f(R_i, K_i)$

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

S-Box 1

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Permutations

$$\text{IP} = [2, 6, 3, 1, 4, 8, 5, 7] \begin{cases} b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8 \\ \\ b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7 \end{cases}$$

Permutations

$$\mathrm{IP} = [2, 6, 3, 1, 4, 8, 5, 7] \begin{cases} b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8 \\ \\ \\ \\ \\ \\ \\ \\ b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7 \end{cases}$$

$$\mathrm{IP}^{-1} = [4, 1, 3, 5, 7, 2, 8, 6]$$

Permutations

$$\begin{array}{rl} & b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8 \\ \mathrm{IP} = [2,6,3,1,4,8,5,7] & \Big\{ \\ & b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7 \\ \mathrm{IP}^{-1} = [4,1,3,5,7,2,8,6] & \Big\{ \\ & b_1 \end{array}$$

Permutations

$$\mathrm{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7$$

$$\mathrm{IP}^{-1} = [4, 1, 3, 5, 7, 2, 8, 6]$$

$$b_1\ b_2$$

Permutations

$$\begin{array}{rl} & b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8 \\ \mathrm{IP} = [2,6,3,1,4,8,5,7] & \Big\{ \\ & b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7 \\ \mathrm{IP}^{-1} = [4,1,3,5,7,2,8,6] & \Big\{ \\ & b_1\ b_2\ b_3 \end{array}$$

Permutations

$$\mathrm{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$\mathrm{IP}^{-1} = [4, 1, 3, 5, 7, 2, 8, 6]$$

$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$

$b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7$

$b_1\ b_2\ b_3\ b_4$

Permutations

$$\mathrm{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7$$

$$\mathrm{IP}^{-1} = [4, 1, 3, 5, 7, 2, 8, 6]$$

$$b_1\ b_2\ b_3\ b_4\ b_5$$

Permutations

$$\mathrm{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7$$

$$\mathrm{IP}^{-1} = [4, 1, 3, 5, 7, 2, 8, 6]$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6$$

Permutations

$$\begin{array}{rl} & b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8 \\ \mathrm{IP} = [2,6,3,1,4,8,5,7] & \Big\{ \\ & b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7 \\ \mathrm{IP}^{-1} = [4,1,3,5,7,2,8,6] & \Big\{ \\ & b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7 \end{array}$$

Permutations

$$\mathrm{IP} = [2, 6, 3, 1, 4, 8, 5, 7]$$

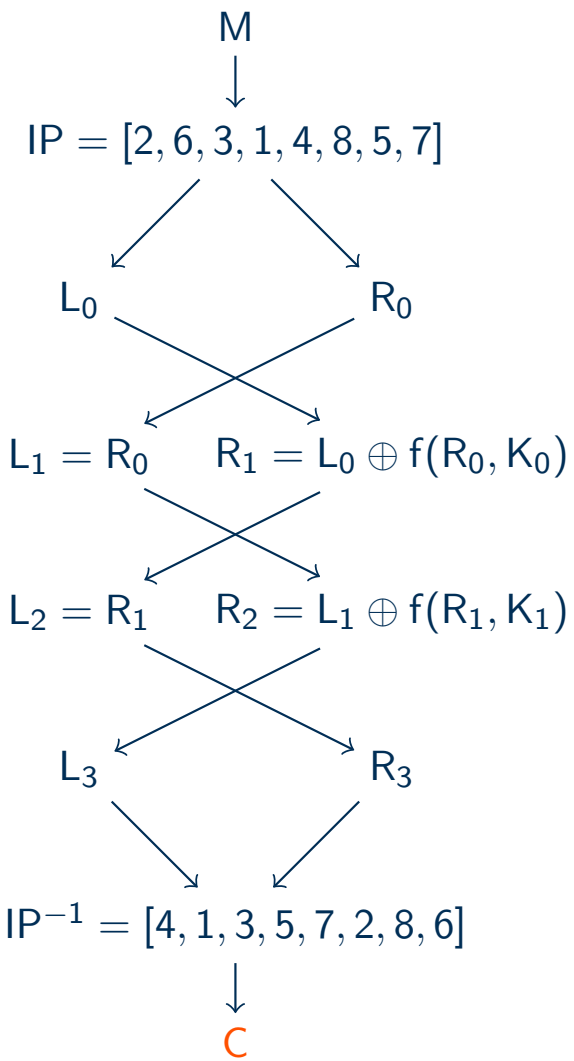
$$\mathrm{IP}^{-1} = [4, 1, 3, 5, 7, 2, 8, 6]$$

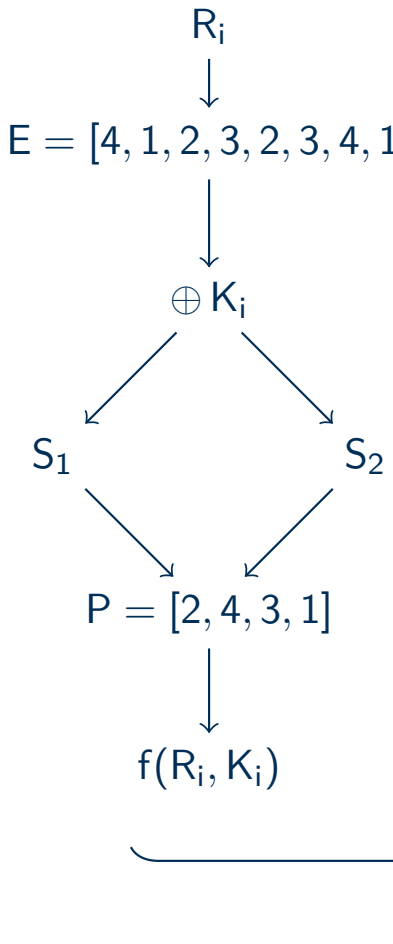
$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

$$b_2\ b_6\ b_3\ b_1\ b_4\ b_8\ b_5\ b_7$$

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8$$

Really Simple DES





$f(R_i, K_i)$

Key Schedule

Key 0: (11100111)

Key 1: (11001111)

S-Box 1

	00	01	10	11
00	01	11	10	11
01	11	10	01	00
10	00	10	01	11
11	11	01	11	10

S-Box 2

	00	01	10	11
00	00	01	10	11
01	10	00	01	11
10	11	00	01	00
11	10	01	10	11

Table of Contents

Summary

- Reviewed Feistel's Cipher

Summary

- Reviewed Feistel's Cipher
- Data Encryption Standard

Summary

- Reviewed Feistel's Cipher
- Data Encryption Standard
- Permutations

Summary

- Reviewed Feistel's Cipher
- Data Encryption Standard
- Permutations
- Expansions and S-Boxes

Cryptology: Data Encryption Standard

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES