Key processing

Initial key (10 bits) 10 1000 0010

Apply initial permutation (P10) 10 0000 1100

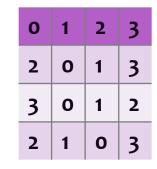
**Split** 

10000 01100

Left circular shift (each half) 00001 11000

Permutation with P8 (k1) 1010 0100

	1	0	3	2
S0=	3	2	1	0
	0	2	1	3
	3	1	0	2





**S1=** 

Key processing

Key after first shift

00001 11000

**S0=** 

**S1=** 

Left circular shift by 2 (each half) 00100 00011

0100 0011

Permutation with P8 (k2)

P10=

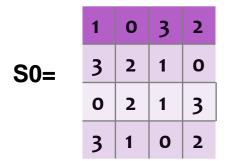
P8=

P4=

 $k1 = 1010 \ 0100$  $k2 = 0100\ 0011$ 

Plaintext 0110 1101

Initial permutation 1110 0110



0	1	2	3
2	0	1	3
3	0	1	2
2	1	0	3

**S1=** 

**Plaintext** 

0110 1101

Initial permutation

1110 0110

S0= 1 0 3 2 0 2

3

1

1

0

S1=

0	1	2	3
2	0	1	3
3	0	1	2
2	1	0	3

Expansion/permutation of right 4 bits

0011 1100

P4=

2 4 3 1

XOR with k1

0011 1100 xor 1010 0100

1001 1000

IP=

2 6 3 1 4 8 5 7

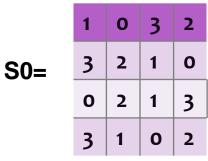
E/P=

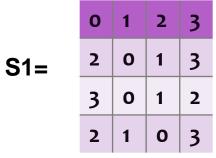


 $k1 = 1010 \ 0100$ 

k2 = 0100 0011

Get row/column from first half 1001 1000





Get row/column from first half

Row = 11 (3)Column = 00 (0)

Apply to S0

	1	0	3	2
S0=	3	2	1	0
	0	2	1	3
	3	1	0	2

0	1	2	3
2	0	1	3
3	0	1	2
2	1	0	3

S1=

Get row/column from first half

$$Row = 11 (3)$$
  
 $Column = 00 (0)$ 

Apply to S0, gets 3 (11)

	1	0	3	2	
S0=	3	2	1	0	S1=
	8	2	1	3	
(	3	1	0	2	



2

0

0 | 1

0 1

3

2

3

Get row/column from first half 1001 1000

$$Row = 11 (3)$$

Column = 00 (0)

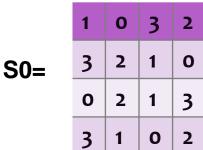
Apply to S0, gets 3 (11)

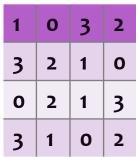
Get row/column from second half 1001 1000

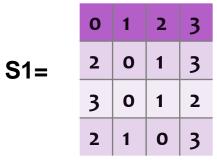
Row =

Column = 00 (0)

Apply to S1









Get row/column from first half 1001 1000

$$Row = 11 (3)$$

Column = 00 (0)

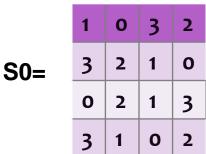
Apply to S0, gets 3 (11)

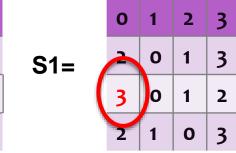
Get row/column from second half 1001 1000

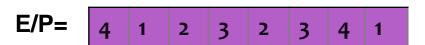
$$Row = 10 (2)$$

Column = 00 (0)

Apply to S1, gets 3 (11)







$$k1 = 1010 \ 0100$$
  
 $k2 = 0100 \ 0011$ 

Get row/column from first half 1001 1000

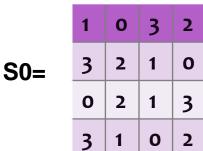
$$Row = 11 (3)$$
  
 $Column = 00 (0)$ 

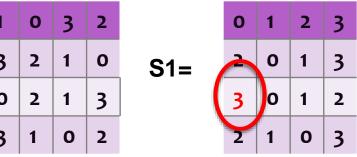
Get row/column from second half 1001 1000

$$Row = 10 (2)$$
  
 $Column = 00 (0)$ 

Column =

Apply to S1, gets 3 (11)



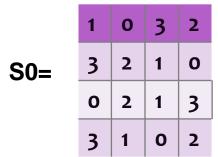


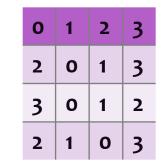


```
k1 = 1010 \ 0100
k2 = 0100\ 0011
```

Result of IP 1110 0110

Previous data
1111
Apply permutation P4
1111





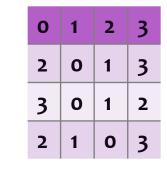
**S1=** 

Previous data
1111
Apply permutation P4
1111

XOR with left half from IP

1111 xor 1110 0001

	1	0	3	2
S0=	3	2	1	0
	0	2	1	3
	3	1	0	2



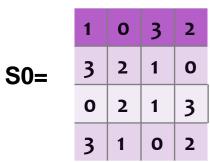


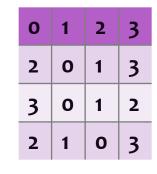
**S1=** 

 $k1 = 1010 \ 0100$  $k2 = 0100 \ 0011$ 

Result of IP 1110 0110

Previous data
1111
Apply permutation P4
1111





XOR with left half from IP

1111 xor 1110 0001



S1=

IP= 2 6 3 1 4 8 5 7

Those will replace left half, while previous right stays the same

0001 0110
Then swap the halves
0110 0001

Current value 0110 0001

**S0**=

Expansion/permutation of right 4 bits 1000 0010

1	0	3	2
3	2	1	0
0	2	1	3
3	1	0	2

S1= 0 1 2 3 2 0 1 3 3 0 1 2 2 1 0 3

XOR with k2

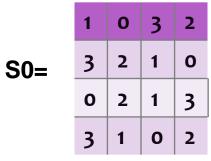
1000 0010 xor

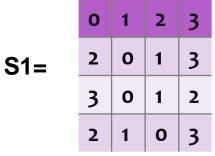
0100 0011 1100 0001



P4=

Get row/column from first half 1100 0001





$$k1 = 1010 \ 0100$$
  
 $k2 = 0100 \ 0011$ 

Get row/column from first half

Row = 10 (2)

Column = 10 (2)

Apply to S0

	1	0	3	2
S0=	3	2	1	0
	0	2	1	3
	3	1	0	2

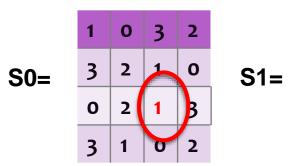
0	1	2	3
2	0	1	3
3	0	1	2
2	1	0	3

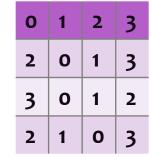
S1=

Get row/column from first half

$$Row = 10 (2)$$
  
 $Column = 10 (2)$ 

Apply to S0, gets 1 (01)





Get row/column from first half 1100 0001

$$Row = 10 (2)$$

Column = 10 (2)

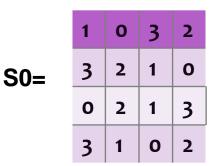
Apply to S0, gets 1 (01)

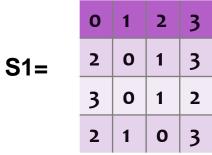
Get row/column from second half 1100 0001

$$Row = 01 (1)$$

Column = 00 (0)

Apply to S1







$$k1 = 1010 \ 0100$$
  
 $k2 = 0100 \ 0011$ 

Get row/column from first half 1100 0001

$$Row = 10 (2)$$
  
 $Column = 10 (2)$ 

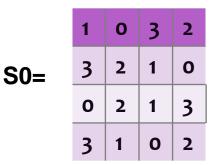
Apply to S0, gets 1 (01)

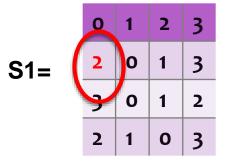
Get row/column from second half 1100 0001

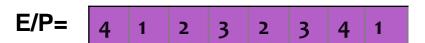
$$Row = 01 (1)$$

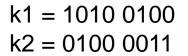
Column = 00 (0)

Apply to S1 gets 2 (10)









Get row/column from first half

$$Row = 10 (2)$$
  
 $Column = 10 (2)$ 

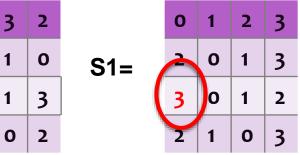
Apply to S0, gets 1 (01)

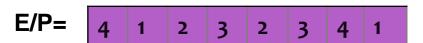
Get row/column from second half

$$Row = 01 (1)$$
  
 $Column = 00 (0)$ 

Apply to S1 gets 2 (10)

	1	0	3	2
<b>S</b> 0=	3	2	1	0
	0	2	1	3
	3	1	0	2

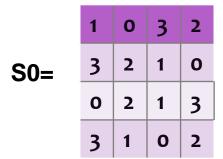


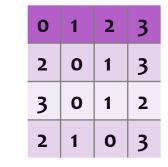


$$k1 = 1010 \ 0100$$
  
 $k2 = 0100 \ 0011$ 

Current Result 0110 0001

Previous data
0110
Apply permutation P4
1010



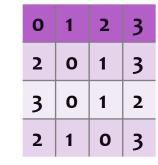


**S1=** 

Previous data
0110
Apply permutation P4
1010



1	0	3	2
3	2	1	0
0	2	1	3
3	1	0	2



XOR with left half from current result

1010 xor 0110 1100

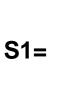


**S1=** 

Previous data
0110
Apply permutation P4
1010



1	0	3	2
3	2	1	0
0	2	1	3
3	1	0	2



P4=

0	1	2	3
2	0	1	3
3	0	1	2
2	1	0	3

XOR with left half from current result



Those will replace left half, while previous right stays the same



1100 0001 Apply reverse of IP (IP-1)

0100

0110