

## Simplified DES

12-bit block

9-bit key

Two 4 x 3 S-boxes

4 rounds

Feistel cipher

Trappe, W. and Washington, L. *Introduction to Cryptography and Coding Theory*.

### XOR

| $\oplus$ | 0 | 1 |   | F | T |
|----------|---|---|---|---|---|
| 0        | 0 | 1 | F | F | T |
| 1        | 1 | 0 | T | T | F |

### S-boxes

| $S_1$ | 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   |
|-------|-----|-----|-----|-----|-----|-----|-----|-----|
| 0     | 101 | 010 | 001 | 110 | 011 | 100 | 111 | 000 |
| 1     | 001 | 100 | 110 | 010 | 000 | 111 | 101 | 011 |

| $S_2$ | 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   |
|-------|-----|-----|-----|-----|-----|-----|-----|-----|
| 0     | 100 | 000 | 110 | 101 | 111 | 001 | 011 | 010 |
| 1     | 101 | 011 | 000 | 111 | 110 | 010 | 001 | 100 |

| Decimal | Binary |
|---------|--------|
| 0       | 000    |
| 1       | 001    |
| 2       | 010    |
| 3       | 011    |
| 4       | 100    |
| 5       | 101    |
| 6       | 110    |
| 7       | 111    |

## Key Schedule

9 bits of key 111 010 110

Use the 8 bits on the left for k1 1110 1011

Rotate to the left one bit 110 101 101

Use the 8 bits on the left for k2 1101 0110

Rotate to the left 1 bit 101 011 011

Use the 8 bits on the left for k3 1010 1101

Rotate to the left 1 bit 010 110 111

Use the 8 bits on the left for k4 0101 1011

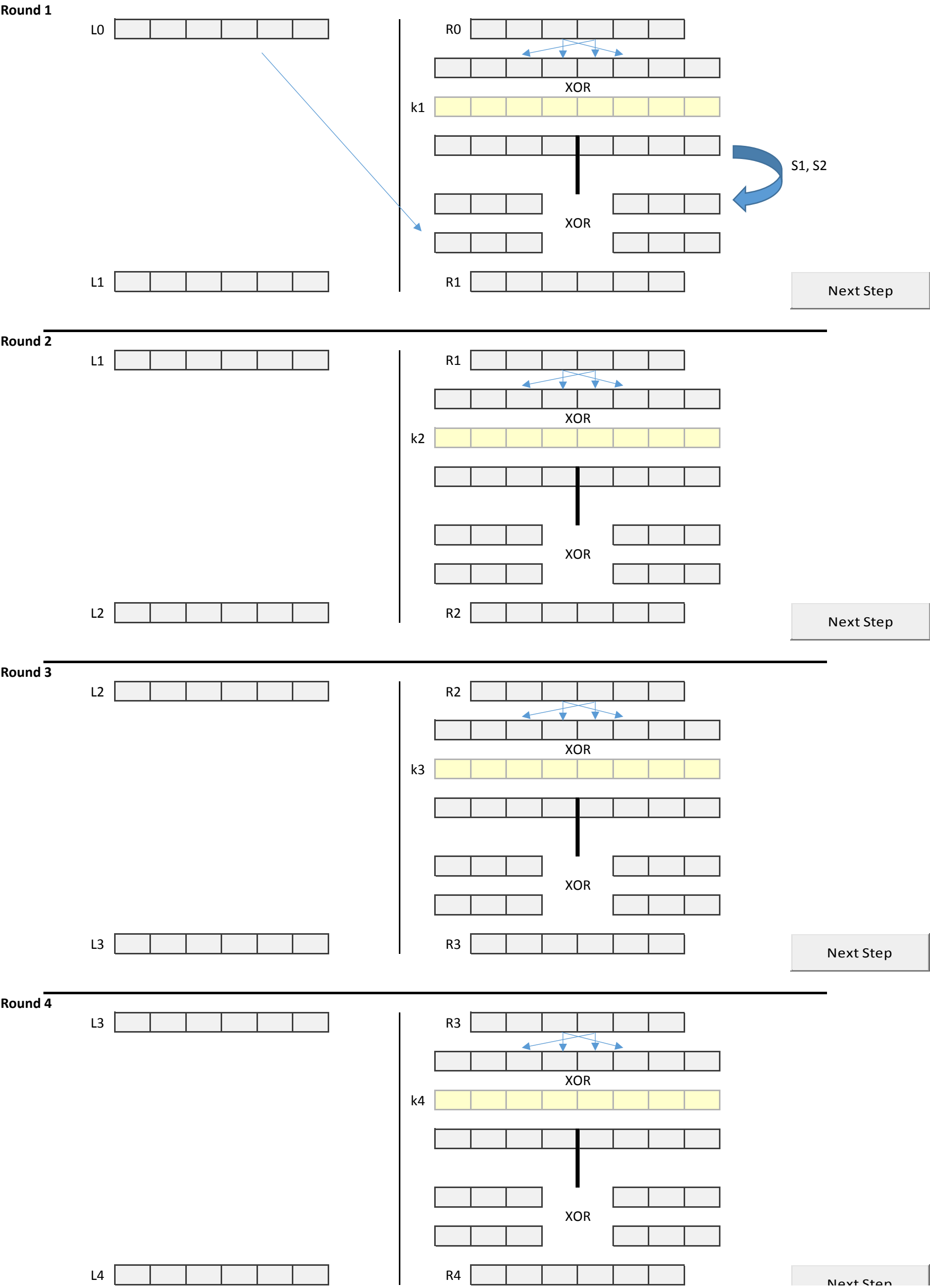
Simplified DES algorithm from Trappe and Washington

Key:

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|

Message:

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|



Key:

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|

Message:

|   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|

Round  
1

L0

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 1 |
|---|---|---|---|---|---|

R0

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|

XOR

k1

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
|---|---|---|---|---|---|---|---|

|   |   |   |
|---|---|---|
| 1 | 0 | 1 |
|---|---|---|

XOR

|   |   |   |
|---|---|---|
| 1 | 0 | 1 |
|---|---|---|

|   |   |   |
|---|---|---|
| 1 | 1 | 0 |
|---|---|---|

|   |   |   |
|---|---|---|
| 1 | 0 | 1 |
|---|---|---|

R1

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|

S1,  
S2

Next Step

Round  
2

L1

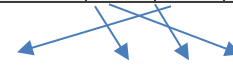
|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|

L2

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|

R1

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|



|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|

XOR

k2

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
|---|---|---|---|---|---|---|---|

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|



|   |   |   |
|---|---|---|
| 1 | 1 | 1 |
|---|---|---|

XOR

|   |   |   |
|---|---|---|
| 0 | 0 | 1 |
|---|---|---|

|   |   |   |
|---|---|---|
| 1 | 1 | 0 |
|---|---|---|

|   |   |   |
|---|---|---|
| 1 | 0 | 1 |
|---|---|---|

R2

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 0 |
|---|---|---|---|---|---|

Next Step

Round  
3

L2

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|

L3

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 0 |
|---|---|---|---|---|---|

R2

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 0 |
|---|---|---|---|---|---|



|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
|---|---|---|---|---|---|---|---|

XOR

k3

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|



|   |   |   |
|---|---|---|
| 1 | 0 | 0 |
|---|---|---|

XOR

|   |   |   |
|---|---|---|
| 0 | 0 | 0 |
|---|---|---|

|   |   |   |
|---|---|---|
| 0 | 0 | 0 |
|---|---|---|

|   |   |   |
|---|---|---|
| 0 | 1 | 1 |
|---|---|---|

R3

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|

Next Step

Round  
4

L3

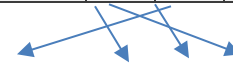
|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 0 |
|---|---|---|---|---|---|

L4

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|

R3

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|



|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|

XOR

k4

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|---|

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|---|



|   |   |   |
|---|---|---|
| 1 | 1 | 1 |
|---|---|---|

XOR

|   |   |   |
|---|---|---|
| 1 | 0 | 1 |
|---|---|---|

|   |   |   |
|---|---|---|
| 0 | 0 | 1 |
|---|---|---|

|   |   |   |
|---|---|---|
| 1 | 0 | 0 |
|---|---|---|

R4

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | 1 |
|---|---|---|---|---|---|

Next Step