School of InfoComm Technology — Taking IT Higher

NGEE ANN POLYTECHNIC

CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

WEEK 14.1

DATA ENCRYPTION STANDARD (DES) AND 3DES

Last Updated: 1/11/2020

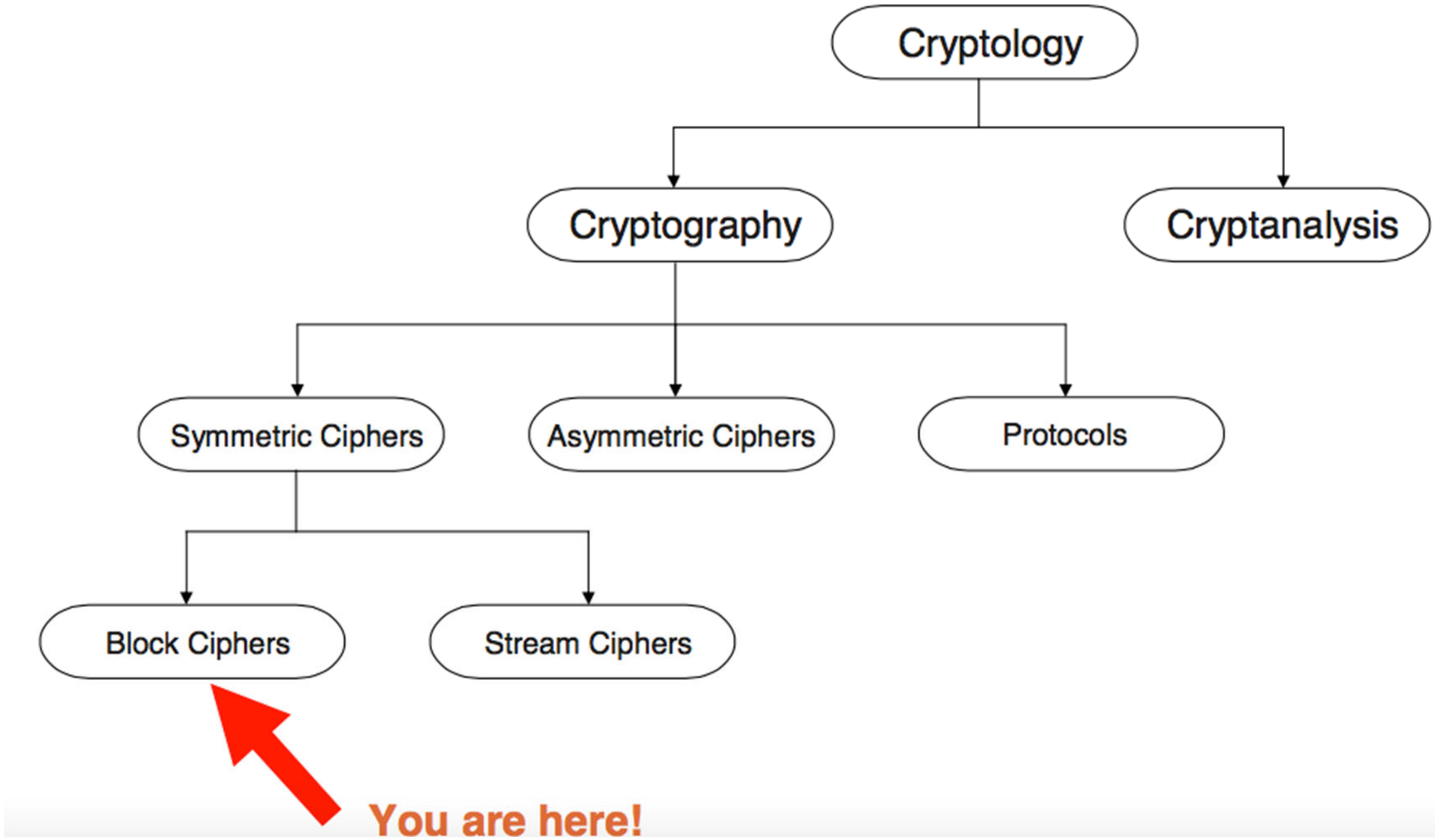
Contents

- Introduction to DES
- Overview of the DES Algorithm
- Internal Structure of DES
- Decryption
- Security of DES

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Introduction to DES

Classification of DES in the Field of Cryptology



Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Knowledge Component

DES Facts

- Data Encryption Standard (DES) encrypts blocks of size 64 bit.
- Developed by IBM based on the cipher Lucifer under influence of the National Security Agency (NSA), the design criteria for DES have not been published.
- Standardized 1977 by the National Bureau of Standards (NBS) today called National Institute of Standards and Technology (NIST)
- Most popular block cipher for most of the last 30 years.
- By far best studied symmetric algorithm.
- Nowadays considered insecure due to the small key length of 56 bit.
- But: 3DES yields very secure cipher, still widely used today.
- Replaced by the Advanced Encryption Standard (AES) in 2000

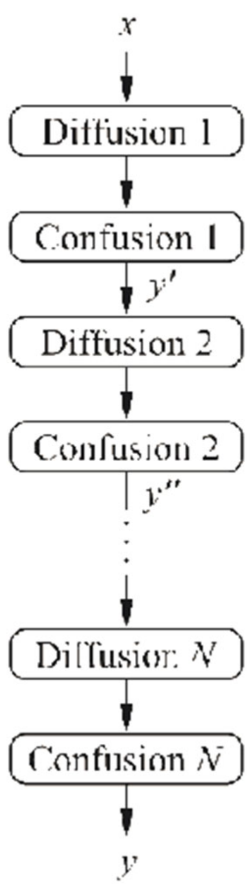
Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Block Cipher Primitives: Confusion and Diffusion

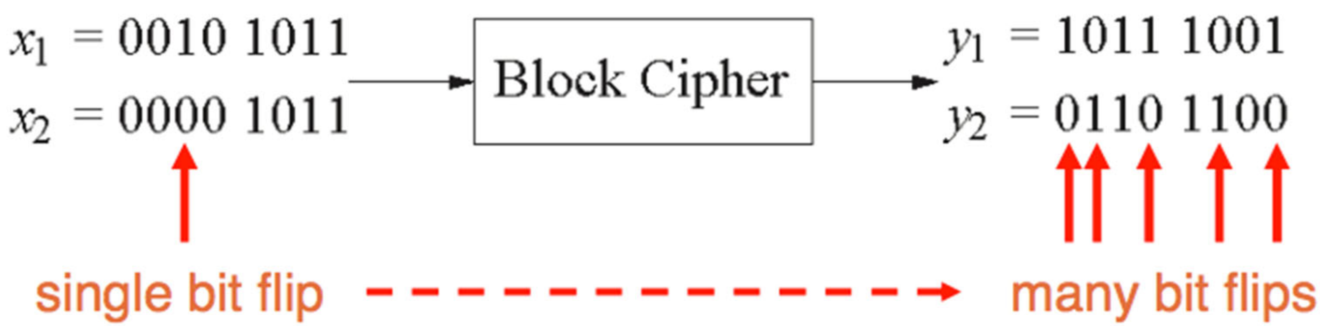
- Claude Shannon: There are two primitive operations with which strong encryption algorithms can be built:
  - **Confusion:** An encryption operation where the relationship between key and ciphertext is obscured.
    - Today, a common element for achieving confusion is substitution, which is found in both AES and DES.
  - **Diffusion:** An encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext.
    - A simple diffusion element is the bit permutation, which is frequently used within DES.
- Both operations by themselves cannot provide security. The idea is to concatenate confusion and diffusion elements to build so called product ciphers.

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Product Ciphers



- Most of today‘s block ciphers are product ciphers as they consist of rounds which are applied repeatedly to the data.
- Can reach excellent diffusion: changing of one bit of plaintext results on average in the change of half the output bits.

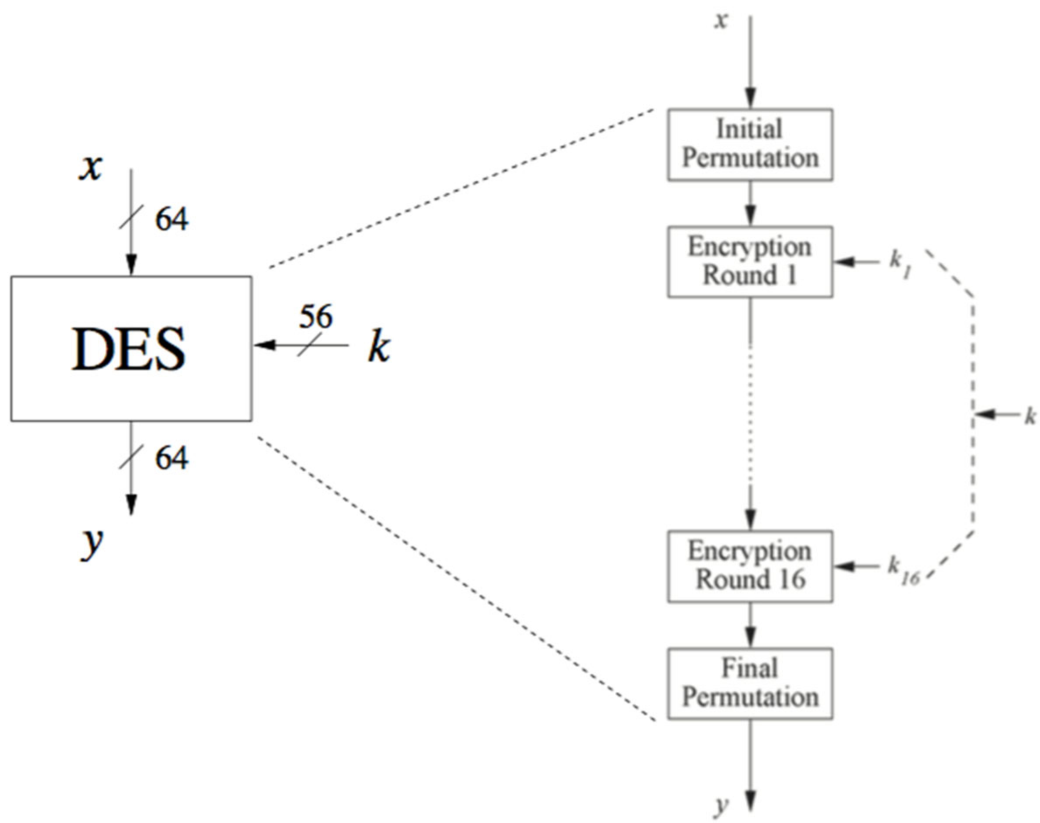


Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Overview of the DES Algorithm

Overview of the DES Algorithm

- Encrypts blocks of size 64 bits.
- Uses a key of size 56 bits.
- Symmetric cipher: uses same key for encryption and decryption
- Uses 16 rounds which all perform the identical operation
- Different subkey in each round derived from main key



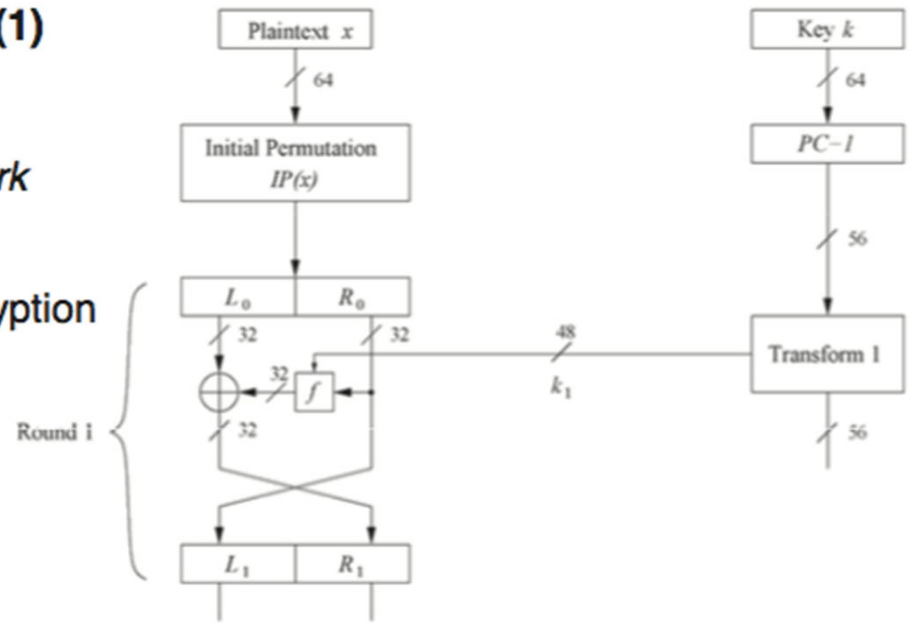
Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Knowledge Component

Feistel Network (1)

The DES Feistel Network (1)

- DES structure is a *Feistel network*
- Advantage: encryption and decryption differ only in keyschedule



- Bitwise initial permutation, then 16 rounds
  1. Plaintext is split into 32-bit halves L_i and R_i
  2. R_i is fed into the function *f*, the output of which is then XORed with L_i
  3. Left and right half are swapped
- Rounds can be expressed as:

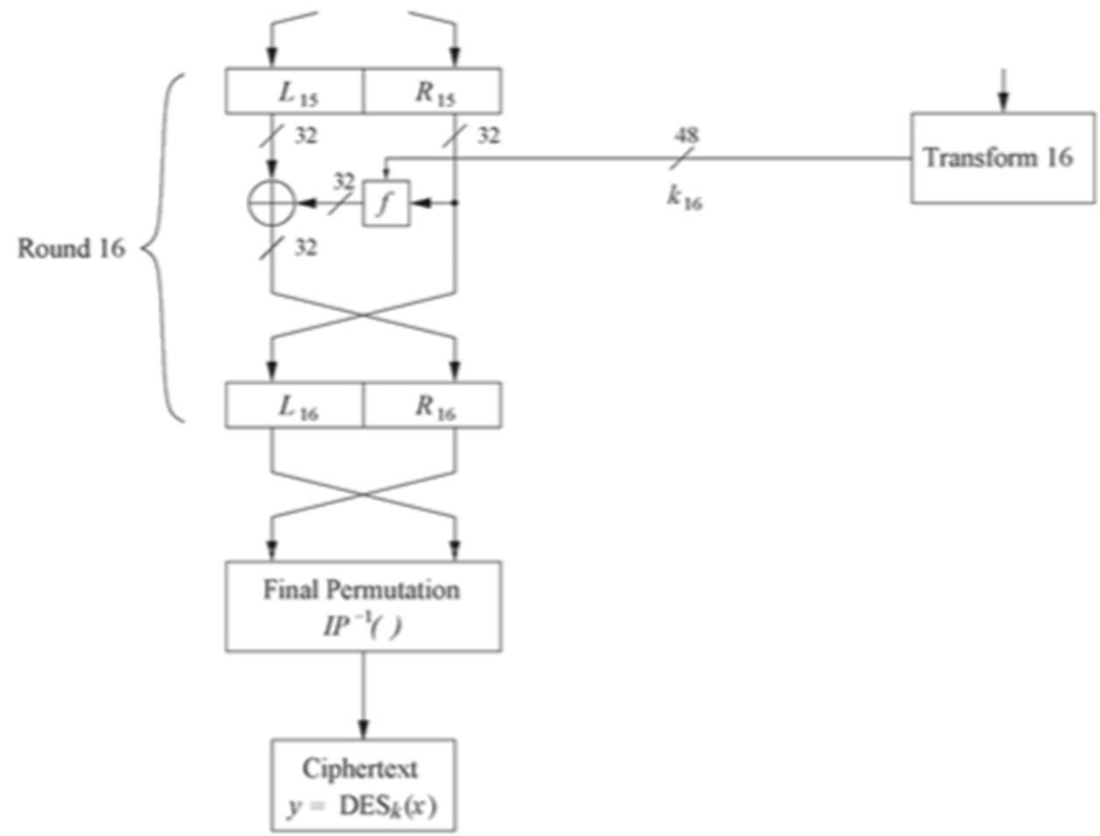
$$L_i = R_{i-1},$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Knowledge Component

Feistel Network (2)

- L and R swapped again at the end of the cipher, i.e., after round 16 followed by a final permutation



Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Internal Structure of DES

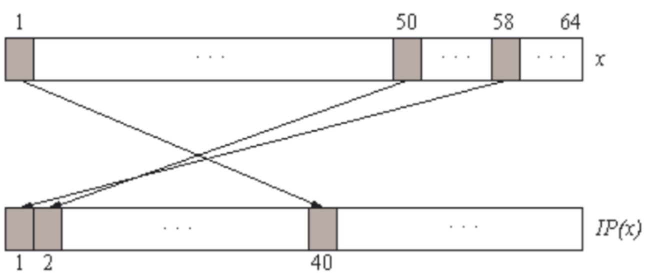
Knowledge Component

Initial and Final Permutation

- Bitwise Permutations.
- Inverse operations.
- Described by tables *IP* and *IP*$^{-1}$.

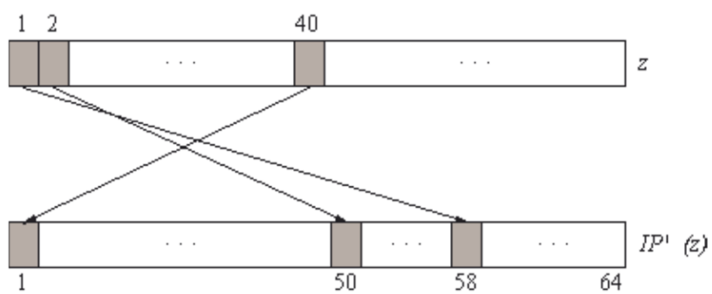
Initial Permutation

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7



Final Permutation

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25



Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Exercise

- Given that the input is given as hexadecimal as:

  0x0000 0080 0000 0002

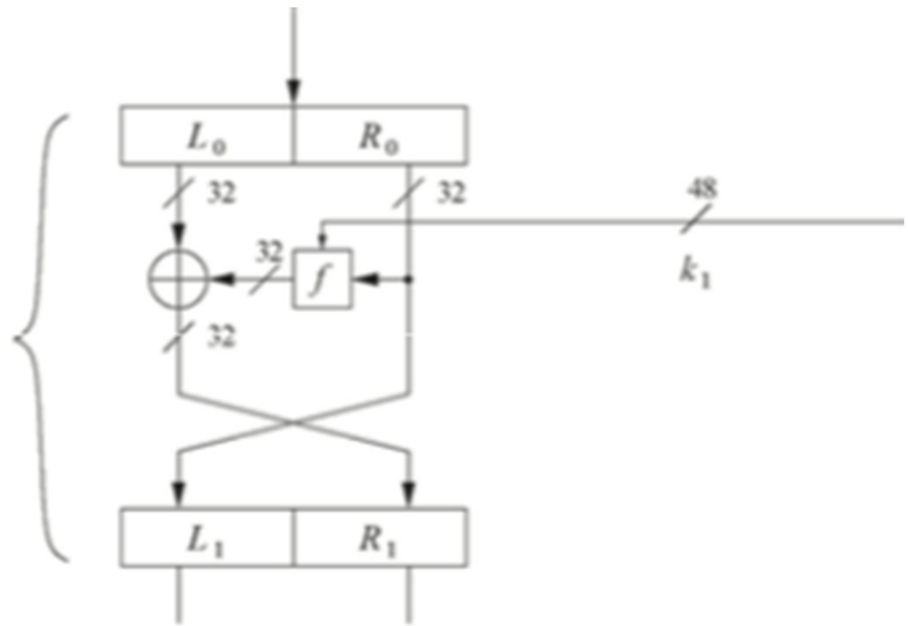
- Find the output of the initial permutation.

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Rounds

- DES uses 16 rounds. Each round of DES is a Feistel cipher.
- F function:

$$f(R_{i-1}, k_i)$$

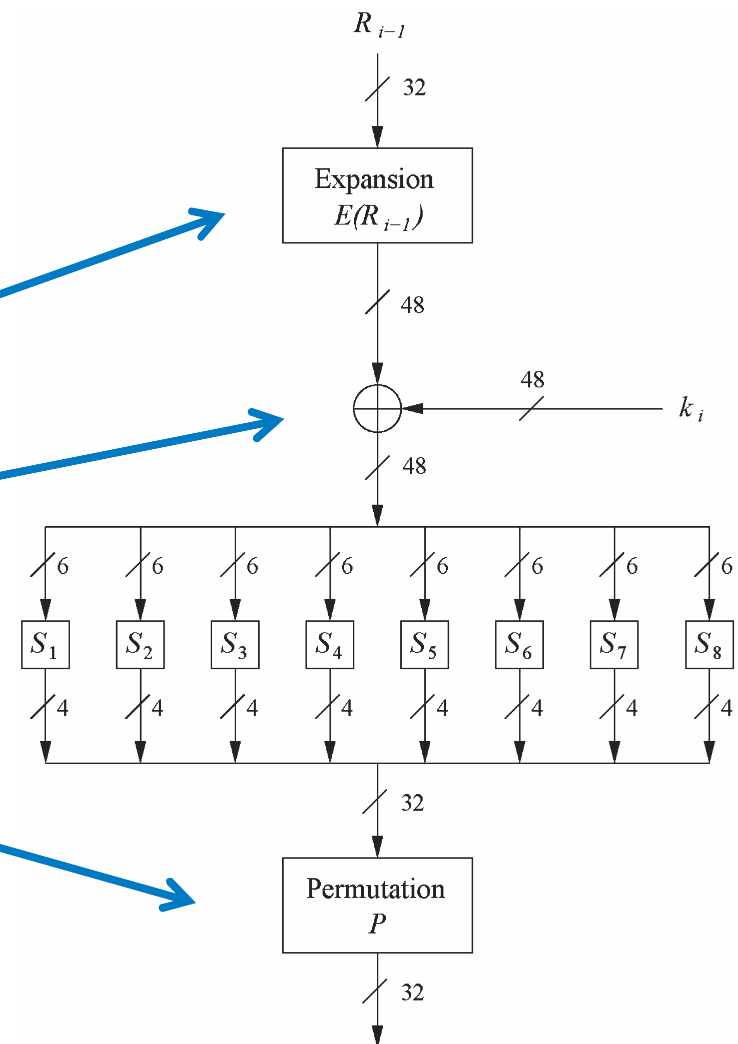


Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

The f-Function

- **main operation of DES**
- *f*-Function inputs:
  R_{i-1} and round key k_i
- **4 Steps**:
  1. Expansion *E*
  2. XOR with round key
  3. S-box substitution
  4. Permutation



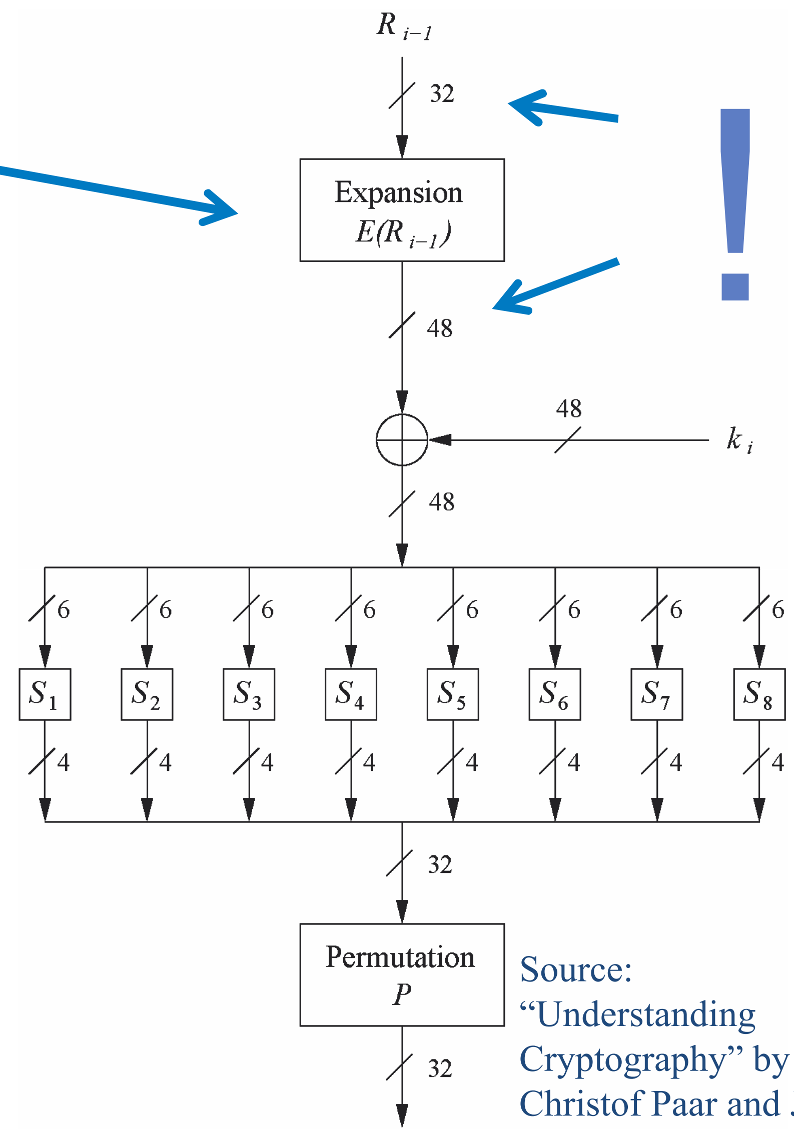
Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Knowledge Component

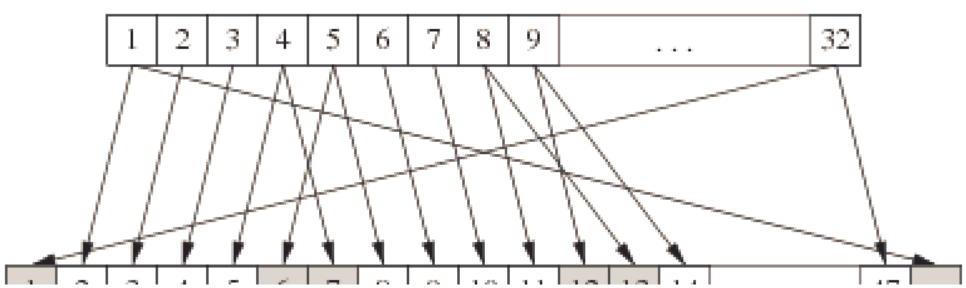
The Expansion Function E

1. **Expansion *E***
- **main purpose: increases diffusion**

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1



!



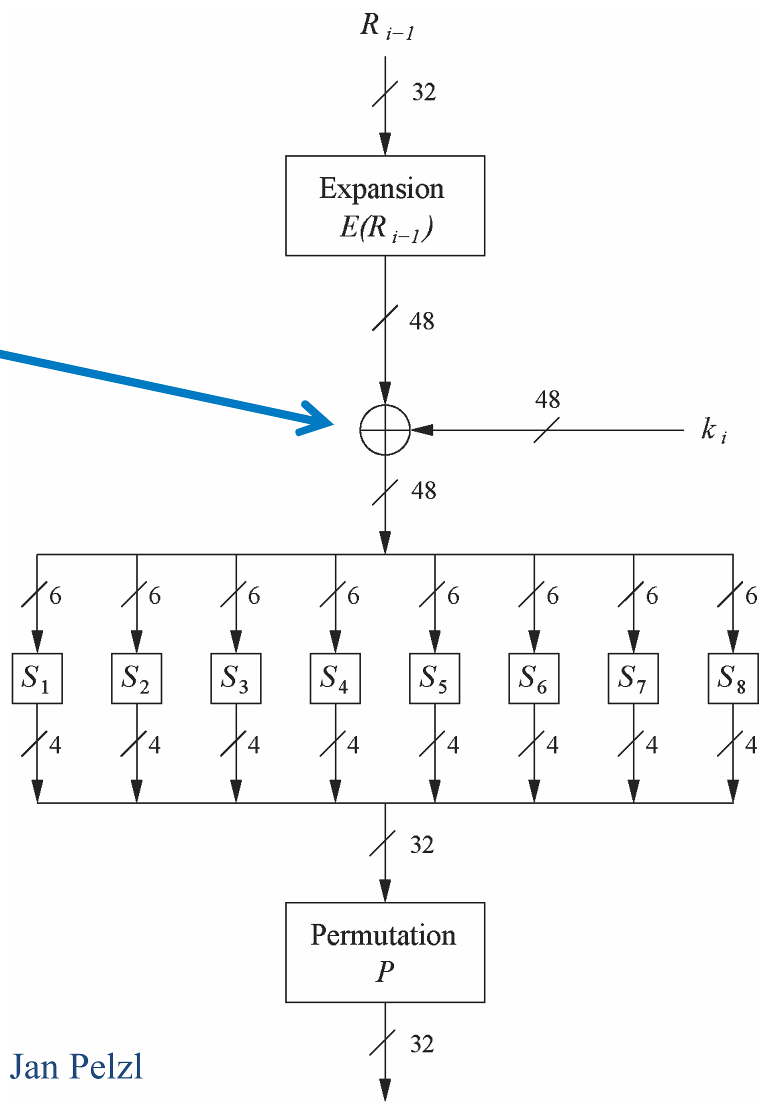
Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Knowledge Component

Add Round Key

2. XOR Round Key

- **Bitwise XOR of the round key and the output of the expansion function *E***
- **Round keys are derived from the main key in the DES keyschedule (in a few slides)**



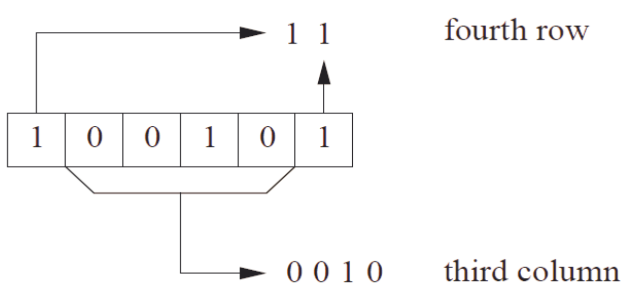
Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Knowledge Component

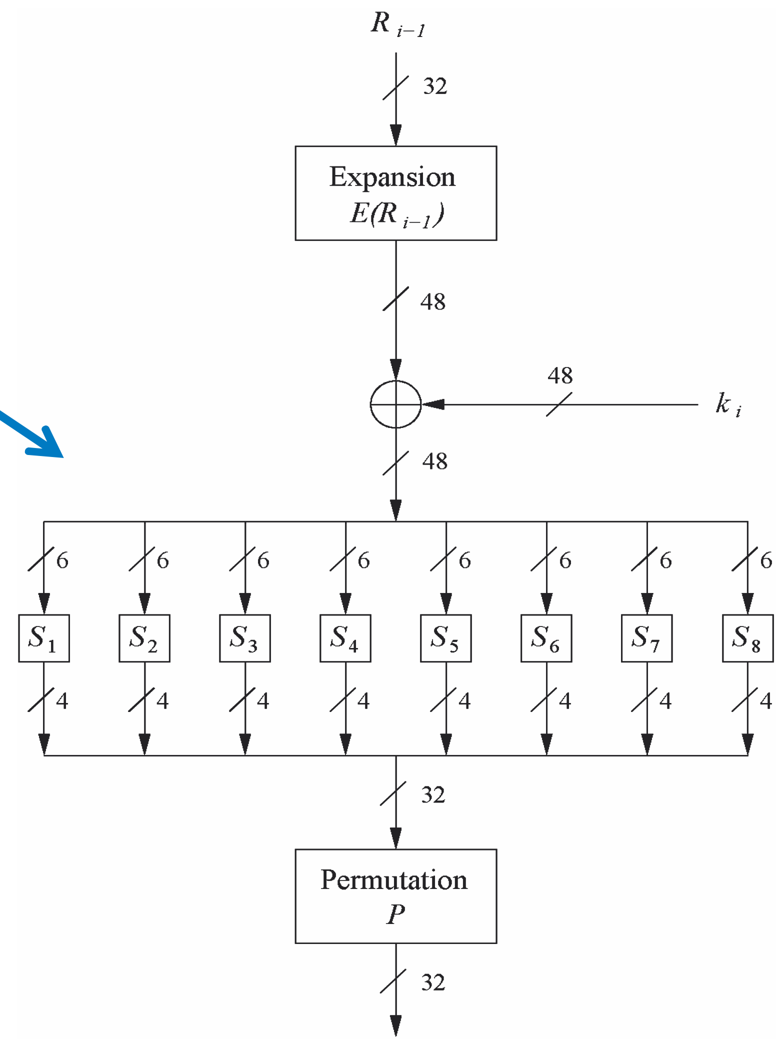
The DES S-Boxes

3. S-Box substitution

- Eight substitution tables.
- 6 bits of input, 4 bits of output.
- Non-linear and resistant to differential cryptanalysis.
- Crucial element for DES security!
- Find all S-Box tables and S-Box design criteria



S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13



Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

S-Boxes

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Exercise

- The input S-box is 100011. What is the output?

- The input to S-box 8 is 000000. What is the output?

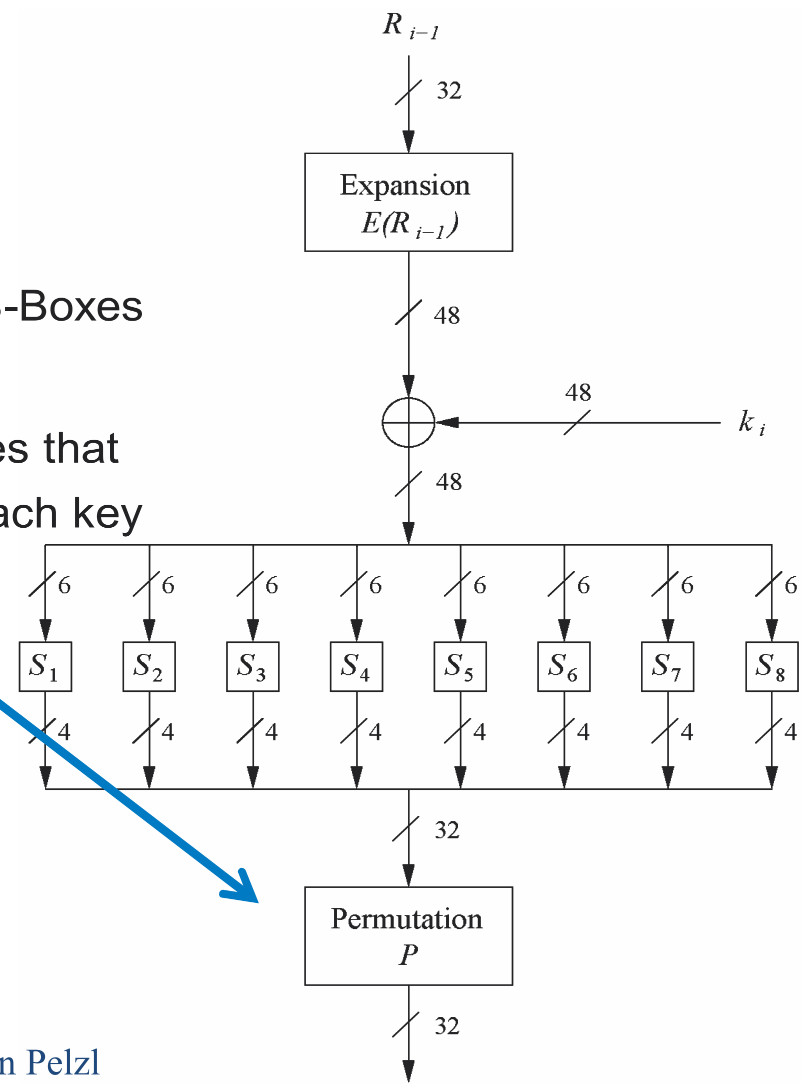
Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

The Permutation P

4. Permutation P

- Bitwise permutation.
- Introduces diffusion.
- Output bits of one S-Box effect several S-Boxes in next round
- Diffusion by E, S-Boxes and P guarantees that after Round 5 every bit is a function of each key bit and each plaintext bit.

P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25



Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Key Schedule (1)

- Derives 16 round keys (or *subkeys*) k_i of 48 bits each from the original 56 bit key.
- The input key size of the DES is 64 bit: **56 bit key** and 8 bit parity:

P = parity bit

- **Parity bits are removed** in a first **permuted choice** *PC-1*:
  (note that the bits 8, 16, 24, 32, 40, 48, 56 and 64 are not used at all)

$PC-1$							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	10	2
59	51	43	35	27	19	11	3
60	52	44	36	63	55	47	39
31	23	15	7	62	54	46	38
30	22	14	6	61	53	45	37
29	21	13	5	28	20	12	4

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

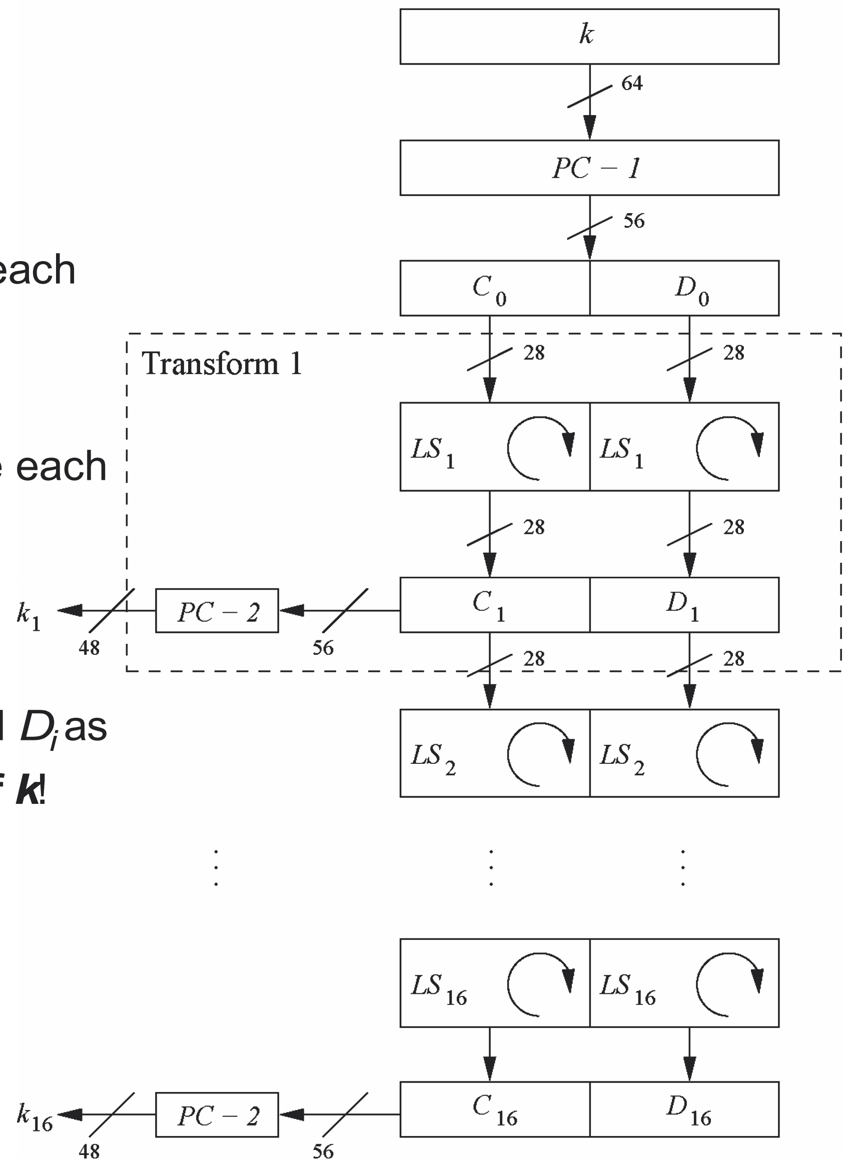
Key Schedule (2)

Key Schedule (2)

- Split key into 28-bit halves C_0 and D_0.
- In **rounds** $\boldsymbol{i}$ **= 1, 2, 9 ,16,** the two halves are each rotated left by **one bit**.
- In **all other rounds** where the two halves are each rotated left by **two bits**.
- *In each round i permuted choice* ***PC-2*** selects a permuted subset of 48 bits of C_i and D_i as round key k_i, i.e. **each** $\boldsymbol{k_i}$ **is a permutation of** $\boldsymbol{k}$!

PC − 2							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

- **Note:** The total number of rotations: $4 \times 1 + 12 \times 2 = 28 \Rightarrow D_0 = D_{16}$ and $C_0 = C_{16}$!

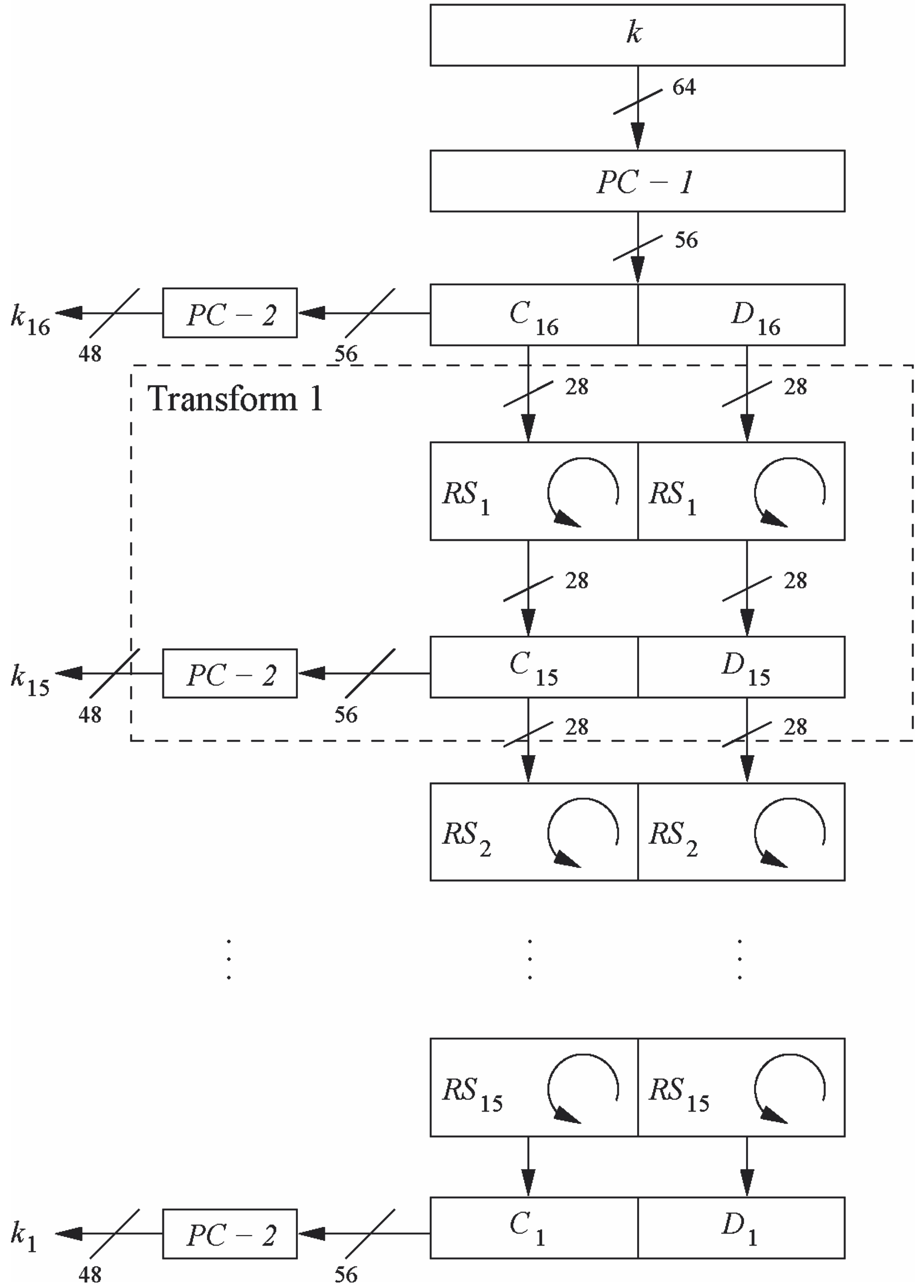


Source: “Understanding Cryptography” by Christof Paar and Jan Pelzl

Decryption

Decryption

- In **Feistel ciphers** only the keyschedule has to be modified for decryption.
- Generate the same 16 round keys in reverse order.
- **Reversed key schedule:**
  As $D_0=D_{16}$ and $C_0=C_{16}$ the first round key can be generated by applying *PC-2* right after *PC-1* (no rotation here!).
  All other rotations of *C* and *D* can be reversed to reproduce the other round keys resulting in:
  - No rotation in round 1.
  - One bit rotation **to the right** in rounds 2, 9 and 16.
  - Two bit rotations **to the right** in all other rounds.



Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

27 Security of DES

Security of DES

- After proposal of DES two major criticisms arose:
  - Key space is too small (256 keys)
  - S-box design criteria have been kept secret: Are there any hidden analytical attacks (backdoors), only known to the NSA?
- Exhaustive key search: For a given pair of plaintext-ciphertext (x, y) test all 2^{56} keys until the condition $DES_k^{-1}(x)=y$ is fulfilled.
  - Relatively easy given today's computer technology!

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

History of Attacks on DES

Year	Proposed/ implemented DES Attack
1977	Diffie & Hellman, (under-)estimate the costs of a key search machine
1990	Biham & Shamir propose differential cryptanalysis (2^{47} chosen ciphertexts)
1993	Mike Wiener proposes design of a very efficient key search machine: Average search requires 36h. Costs: $1.000.000
1993	Matsui proposes linear cryptanalysis (2^{43} chosen ciphertexts)
Jun. 1997	DES Challenge I broken, 4.5 months of distributed search
Feb. 1998	DES Challenge II--1 broken, 39 days (distributed search)
Jul. 1998	DES Challenge II--2 broken, key search machine *Deep Crack* built by the Electronic Frontier Foundation (EFF): 1800 ASICs with 24 search engines each, Costs: $250 000, 15 days average search time (required 56h for the Challenge)
Jan. 1999	DES Challenge III broken in 22h 15min (distributed search assisted by *Deep Crack*)
2006-2008	Reconfigurable key search machine *COPACOBANA* developed at the Universities in Bochum and Kiel (Germany), uses 120 FPGAs to break DES in 6.4 days (avg.) at a cost of $10 000.

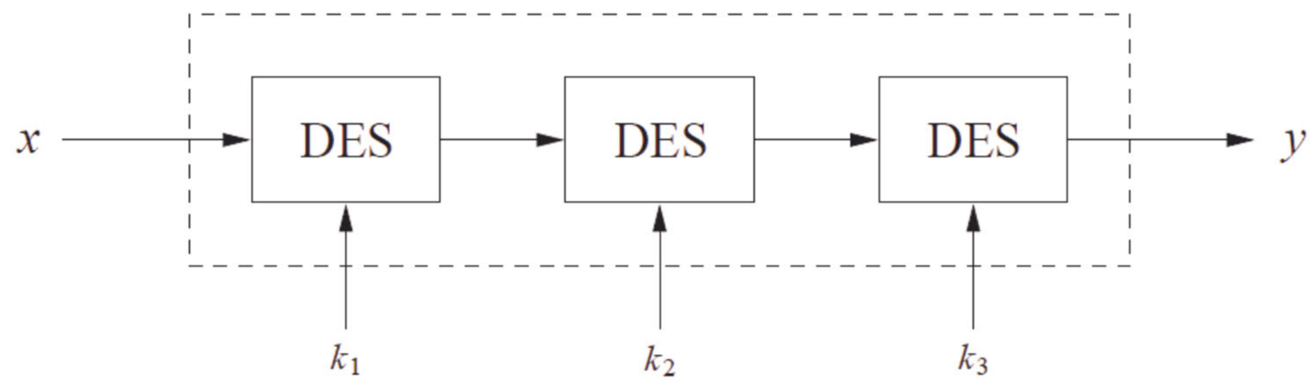
Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

3DES

Knowledge Component

Triple DES – 3DES

- Triple encryption using DES is often used in practice to extend the effective key length of DES to 168 bit key.
  - 3x56 bit keys = 168 bit key
  - Other option also possible: 112 bit key (only 2 keys used K3=K1), 56 bit key (only 1 key is used – backward compatible K1=K2=K3)
- No practical attack known today.
- Used in many legacy applications, i.e., in banking systems.



Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl

Summary

You learnt

- DES was the dominant symmetric encryption algorithm from the mid-1970s to the mid-1990s. Since 56-bit keys are no longer secure, the Advanced Encryption Standard (AES) was created.
- Standard DES with 56-bit key length can be broken relatively easily nowadays through an exhaustive key search.
- DES is quite robust against known analytical attacks: In practice it is very difficult to break the cipher with differential or linear cryptanalysis.
- By encrypting with DES three times in a row, triple DES (3DES) is created, against which no practical attack is currently known.
- The "default" symmetric cipher is nowadays often AES.

Source: "Understanding Cryptography" by Christof Paar and Jan Pelzl