UNIVERSITY OF BIELSKO-BIAŁA

AKADEMIA TECHNICZNO-HUMANISTYCZNA

Faculty of Mechanical Engineering

and Computer Science

www.ath.bielsko.pl

Safety in Information Technology

(Prof. dr hab. inż. Mikołaj Karpiński)

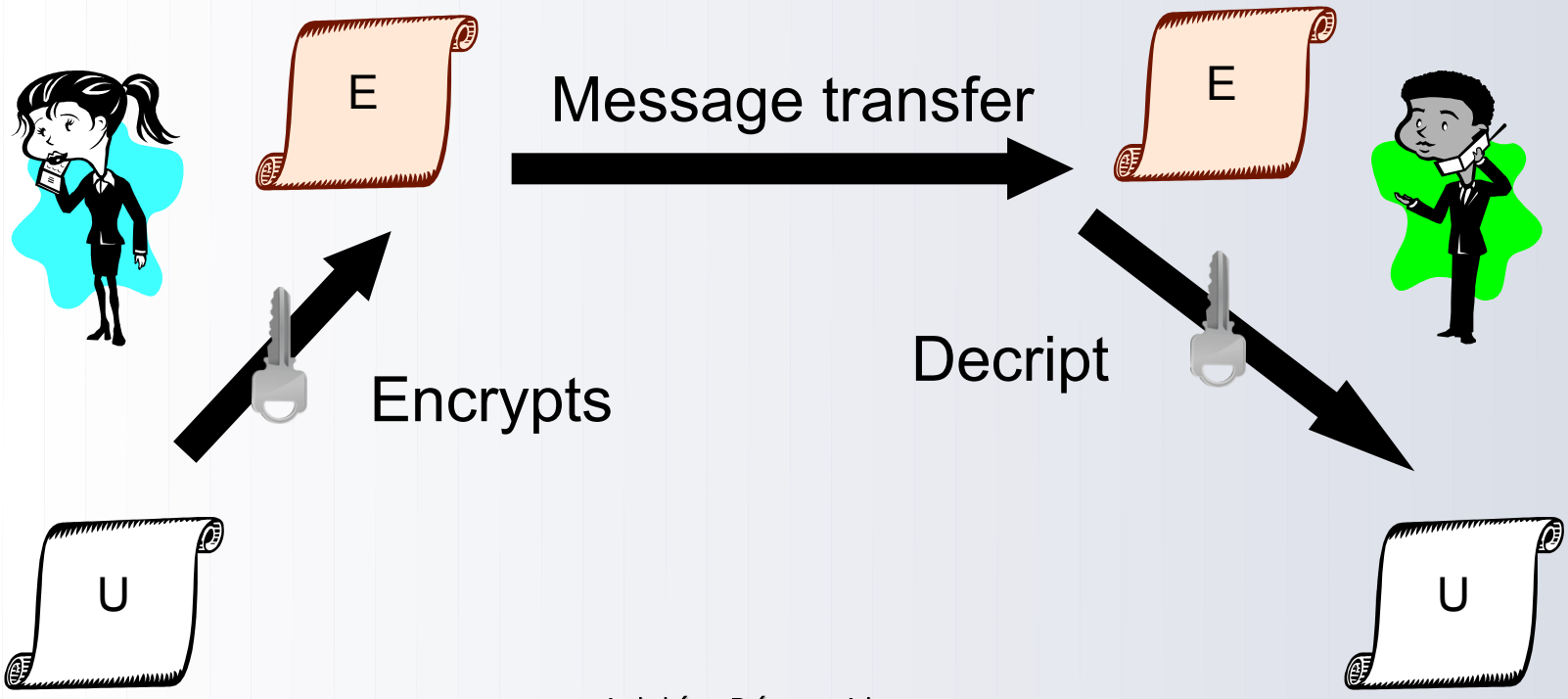
Subject:

Symmetric Cryptograpy – *DES (Data Encryption Standard)*

Editor: Adrián Pérez Alonso, 1.12.2011

Symmetric criptography

The same key is used to encryption of plaintext and decryption of ciphertext



DES (Data Encryption Standard)

1972 - NBS (National Bureau of Standards) needs cipher information

1974 – IBM submitted the Lucifer algorithm

NSA was injustified accused of plant a "back door". But NSA reduce the key size to 128 bits to 56 bits.

1976 – FIPS (Federal Information Processing Standar) choose the final algorithm

Problems with DES?

- The key size is **56bits. Brute force** attack easy
  - Try all posible keys.
  - 1977, Diffie and Hellman proposed a machine (US$20 million) which could find a DES key in 1 day.
  - 1998, the Electronic Frontier Foundation break DES key in less than 3 days
  - 1999, 100.000 PCs working in a network break a DES key in 3 hours, trying 245.000 million keys

Replacement algorithms

- Triple DES (2TDES/3TDES)
- DES-X (XOR & 2 keys)

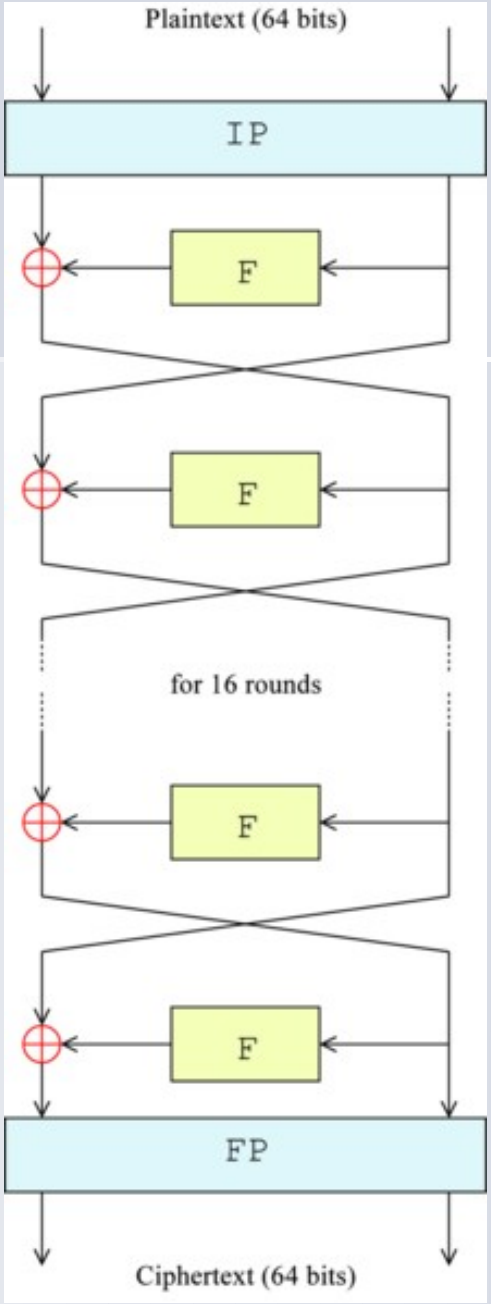
$$(DES - X = K_2 \circ DES_k(M \circ K_1))$$

- AES (Advanced Encryption Standard) (2002, 128-bit key)

DES encryption

- 56-bit key
- Encrypts data using 64-bit blocks and 64-bit key

  (7bitKey+1bitParity) x8 times = 64b
- The main algorithm is repeated **16 times**
- 2 more steps IP and FP

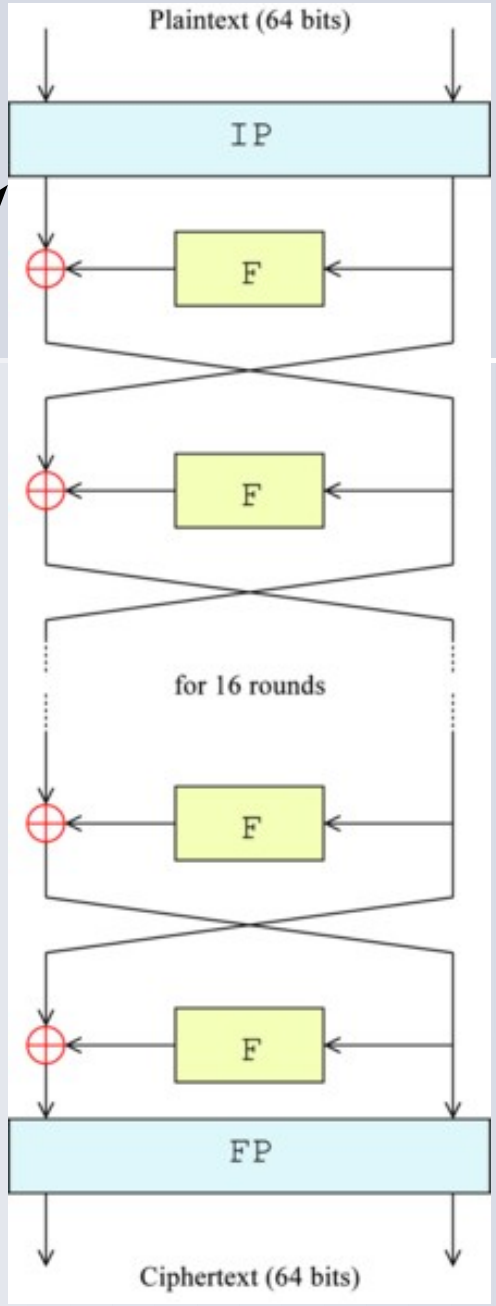


DES encryption

- Initial permutation (get **L0** and **R0** from Half Block)

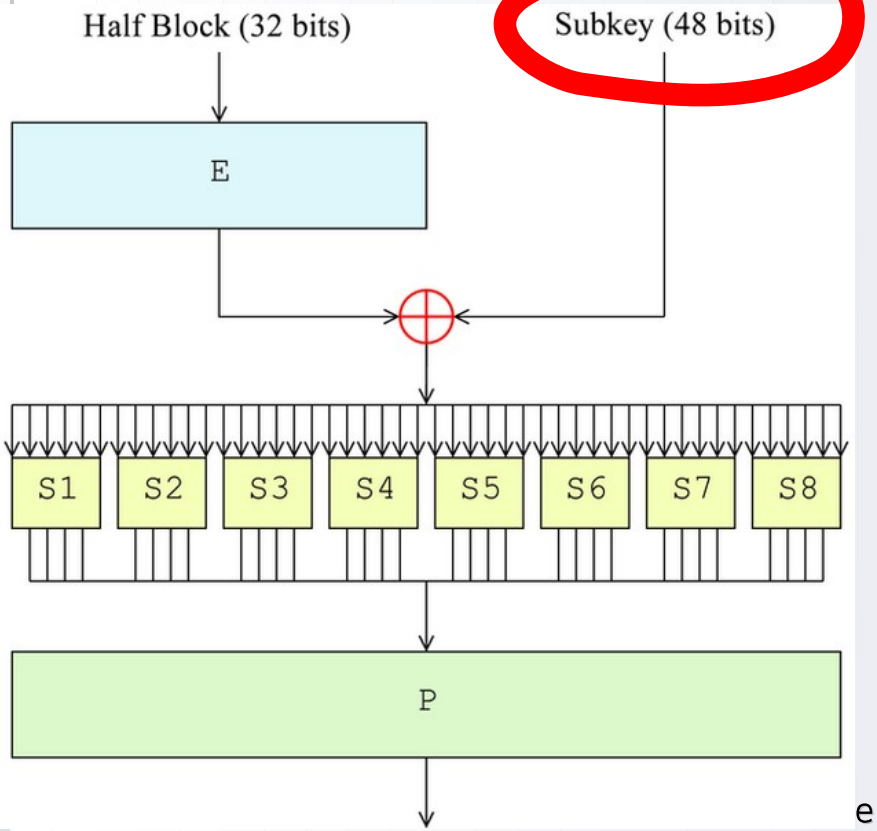
IP

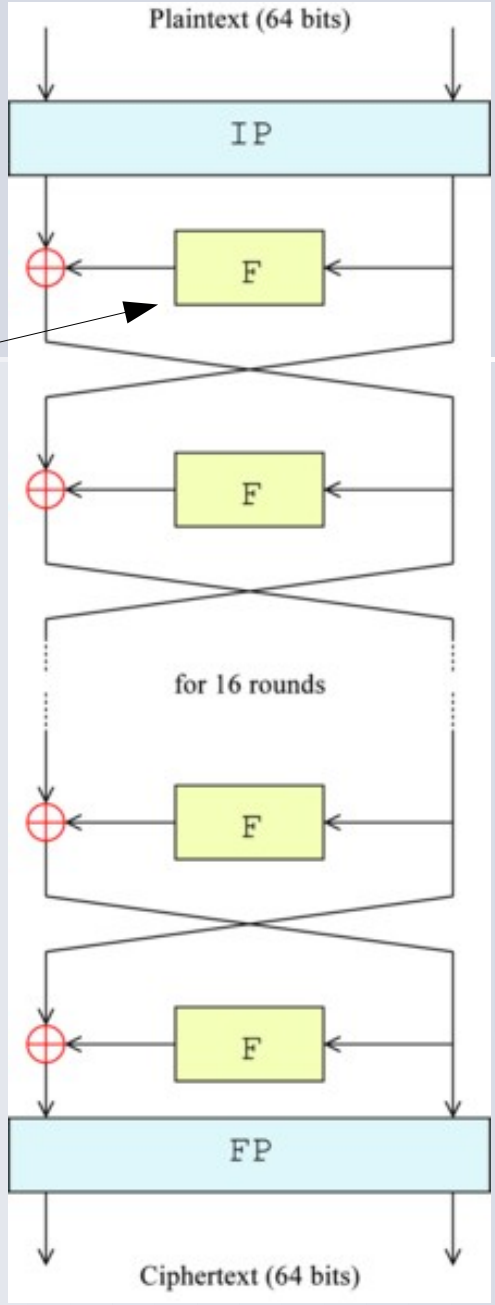
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7



DES core Feistel function (f)

- Each iteration





Create 16 subkeys

Iteration Number	Number of Left Shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

- AES permute the 64-bit **key** (K) to get another 56-bit Key (K+) using PC-1 table.
- Get the 16 **subkeys** (Kn) using the following (left) schedule of "left shifts"

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

Create 16 subkeys

- Permute Kn using PC-2 to get the finals **48-bit** subkeys

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

DES core Feistel function (f)

- Apply **f** for each of the 16 iterations:

Ln = Rn-1

Rn = Ln-1 + f(Rn-1,Kn)

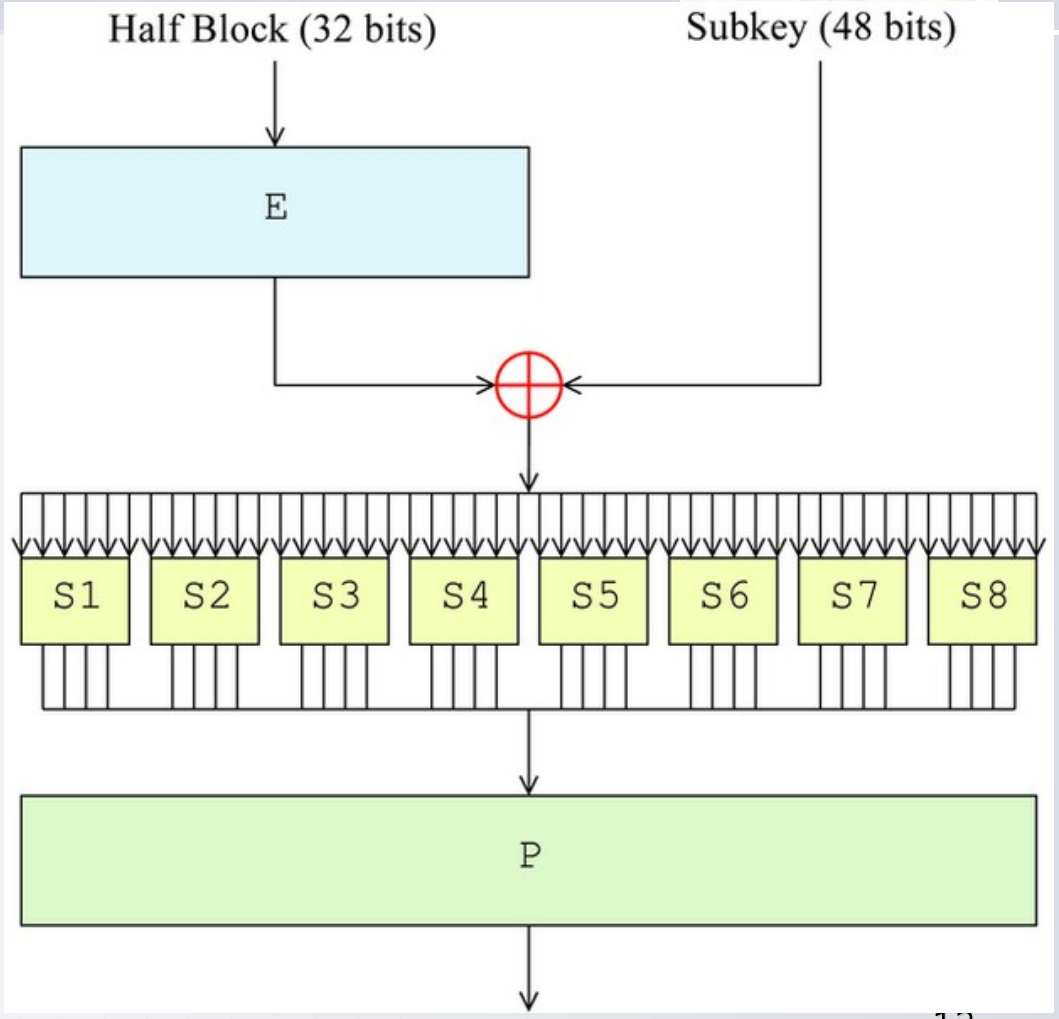
For example:

N=1

K1

L1 = R0

R1 = L0 + f(R0,K1)



DES core Feistel function (f)

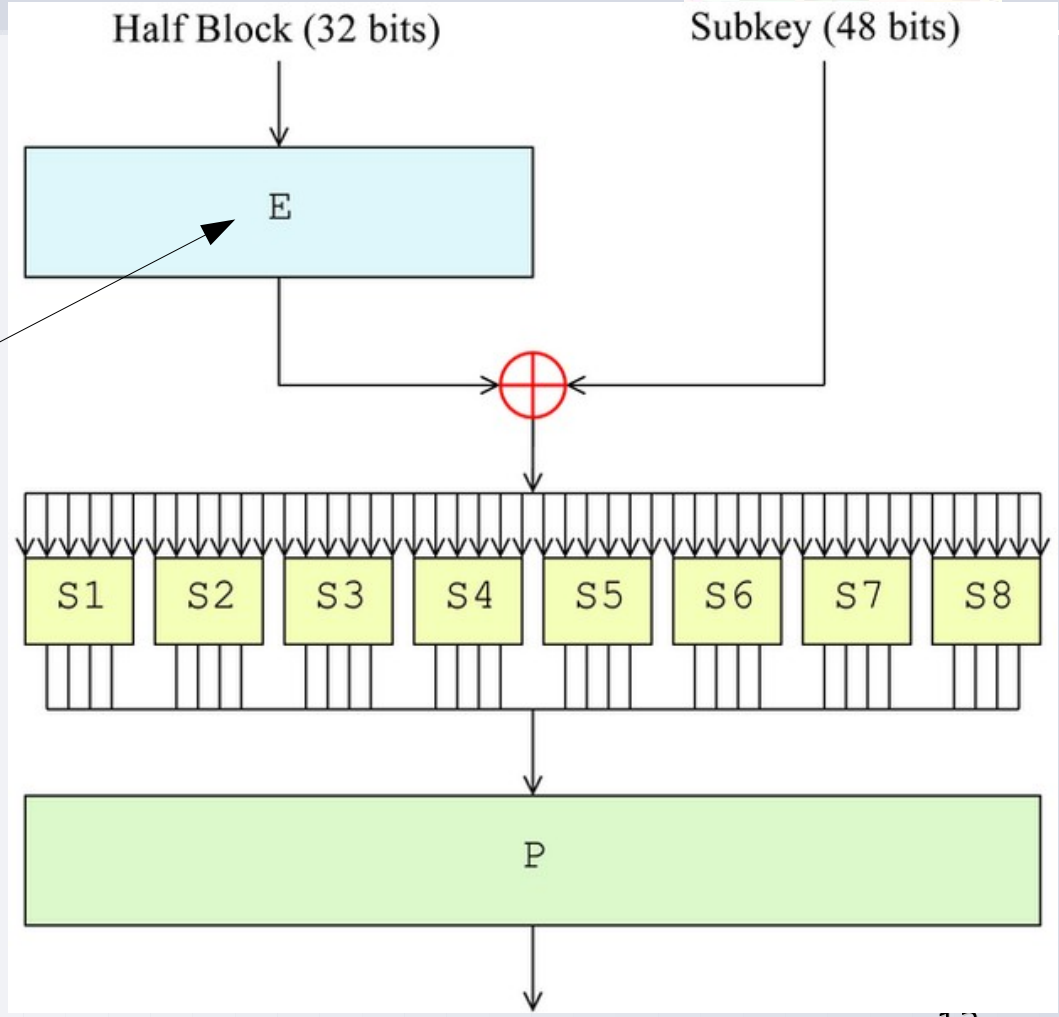
Ln = Rn-1

Rn = Ln-1 + f(Rn-1,Kn)

- First expand **Rn-1** from 32 bits to 48 bits (**E(Rn-1)**)

E BIT-SELECTION TABLE

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

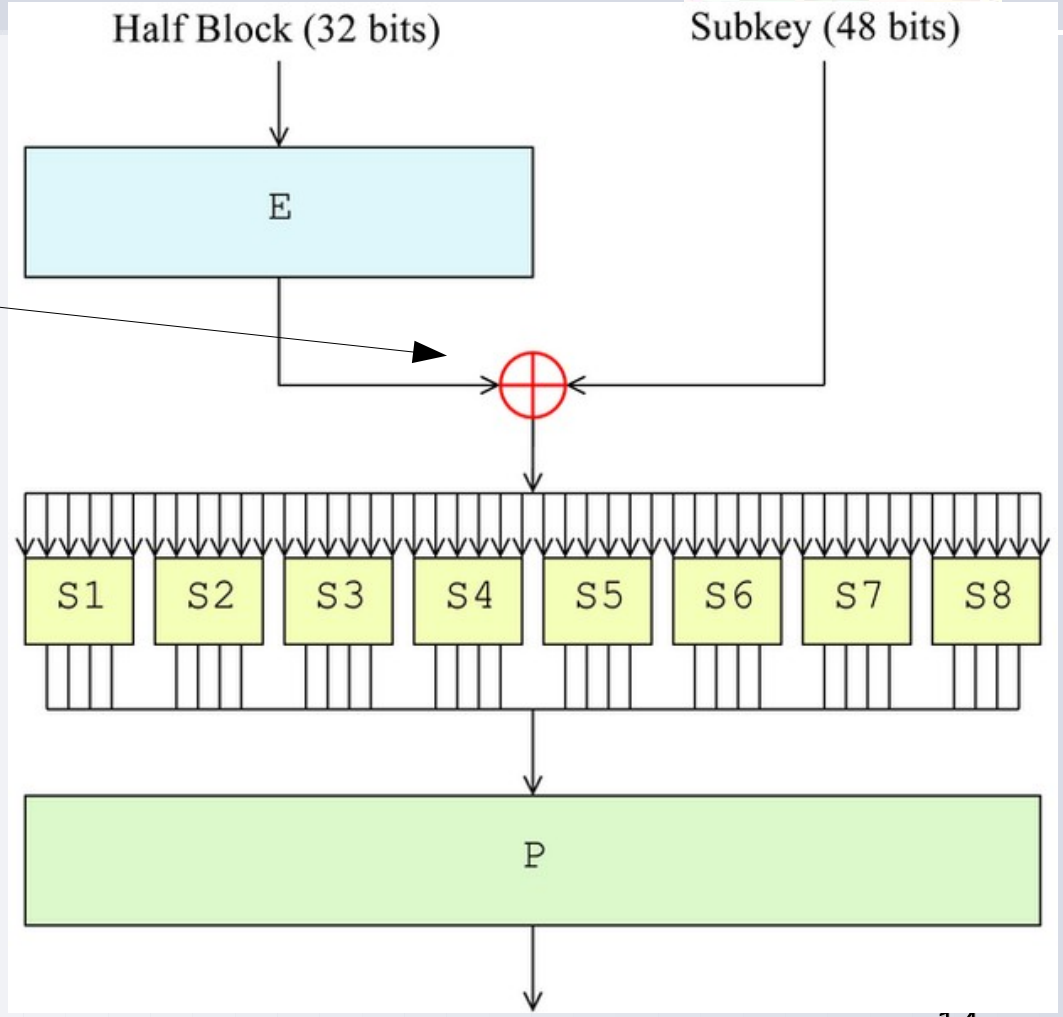


DES core Feistel function (f)

Ln = Rn-1

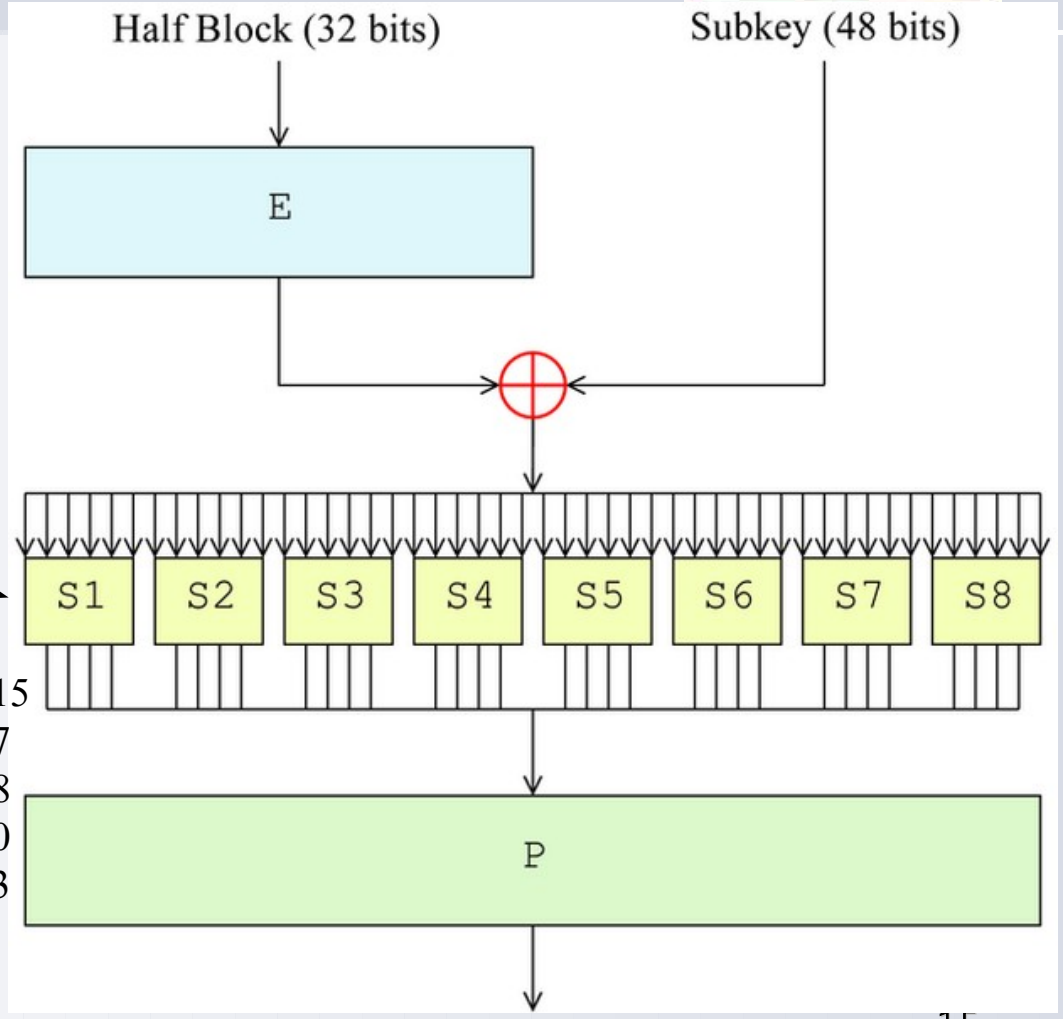
Rn = Ln-1 + f(Rn-1,Kn)

- **Rn-1** XOR **Kn**



DES core Feistel function (f)

- Bi(6bit) is address in S-Box table
- Si(Bi) (4bit) is the number in S-Box table in Bi address



S1

Column Number

Row No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

All S-box tables

S1

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

S2

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

S3

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

S4

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

S5

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

S6

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

S7

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

S8

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

DES core Feistel function (f)

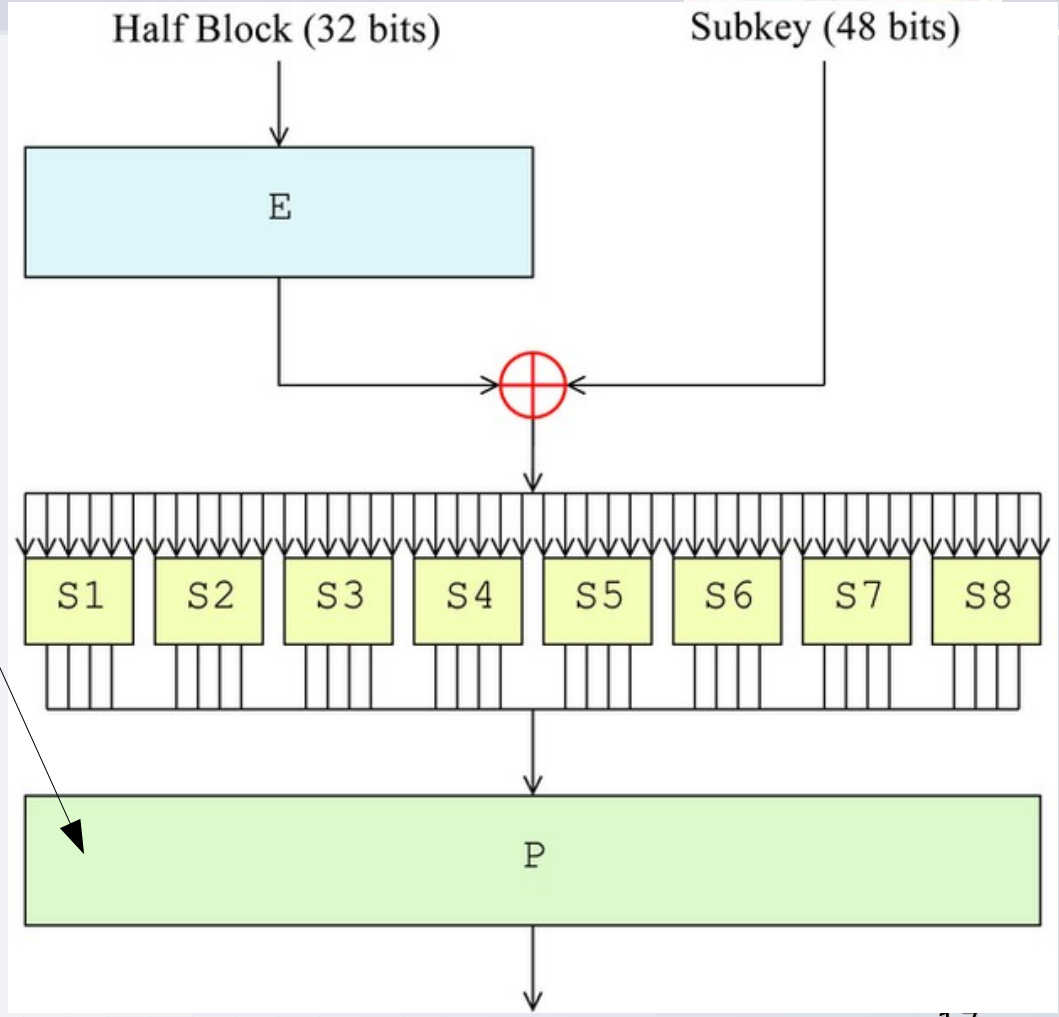
Ln = Rn-1

Rn = Ln-1 + f(Rn-1,Kn)

- Permutation P of the S-box output

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

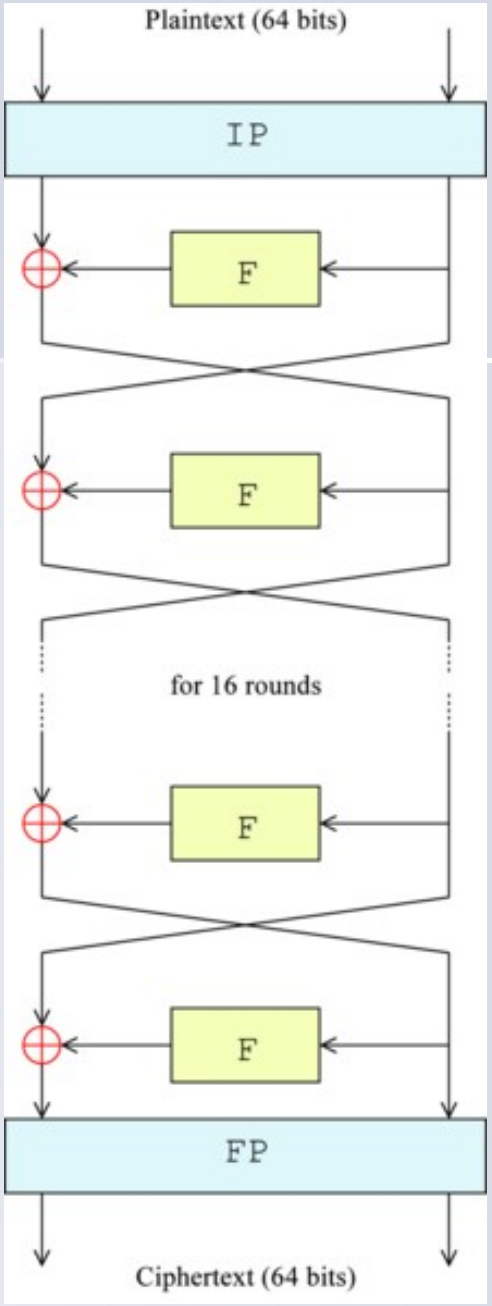


DES encryption

- Apply a final permutation (FP)

FP

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



DES modes of operation

- Electronic Code Book (ECB)

Each 64-bit block is encrypted individually

DES modes of operation

- Chain Block Coding (CBC)
- Cipher Feedback (CFB)

Encrypted ciphertext is XORed with the next plaintext block to be encrypted

Safety in Information Technology

(Prof. dr hab. inż. Mikołaj Karpiński)

Thanks for your Attention!
Any Questions?

References

- http://www.tropsoft.com/strongenc/des.htm
- http://orlingrabbe.com/des.htm
- http://en.wikipedia.org/wiki/Data_Encryption_Standard