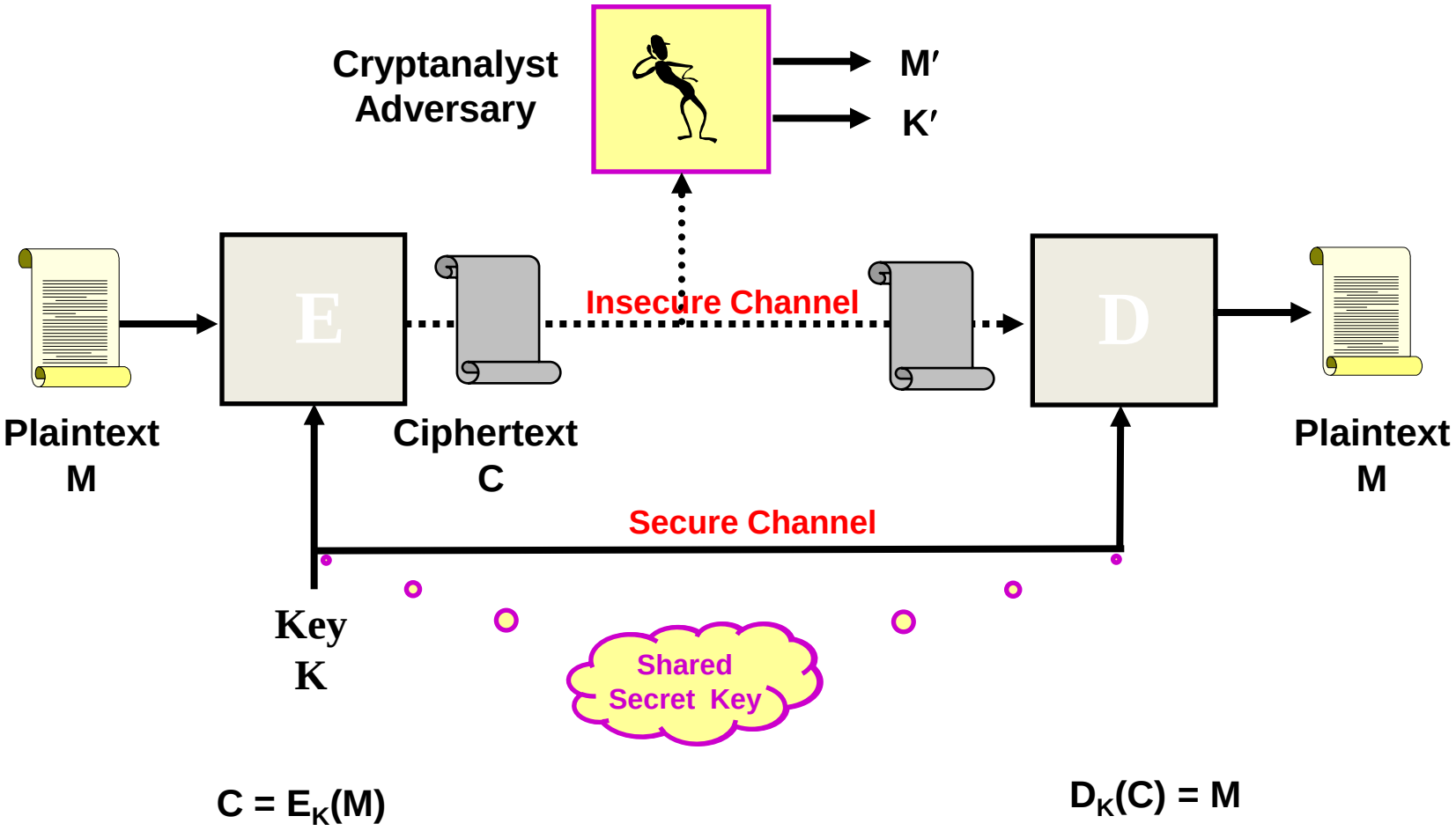
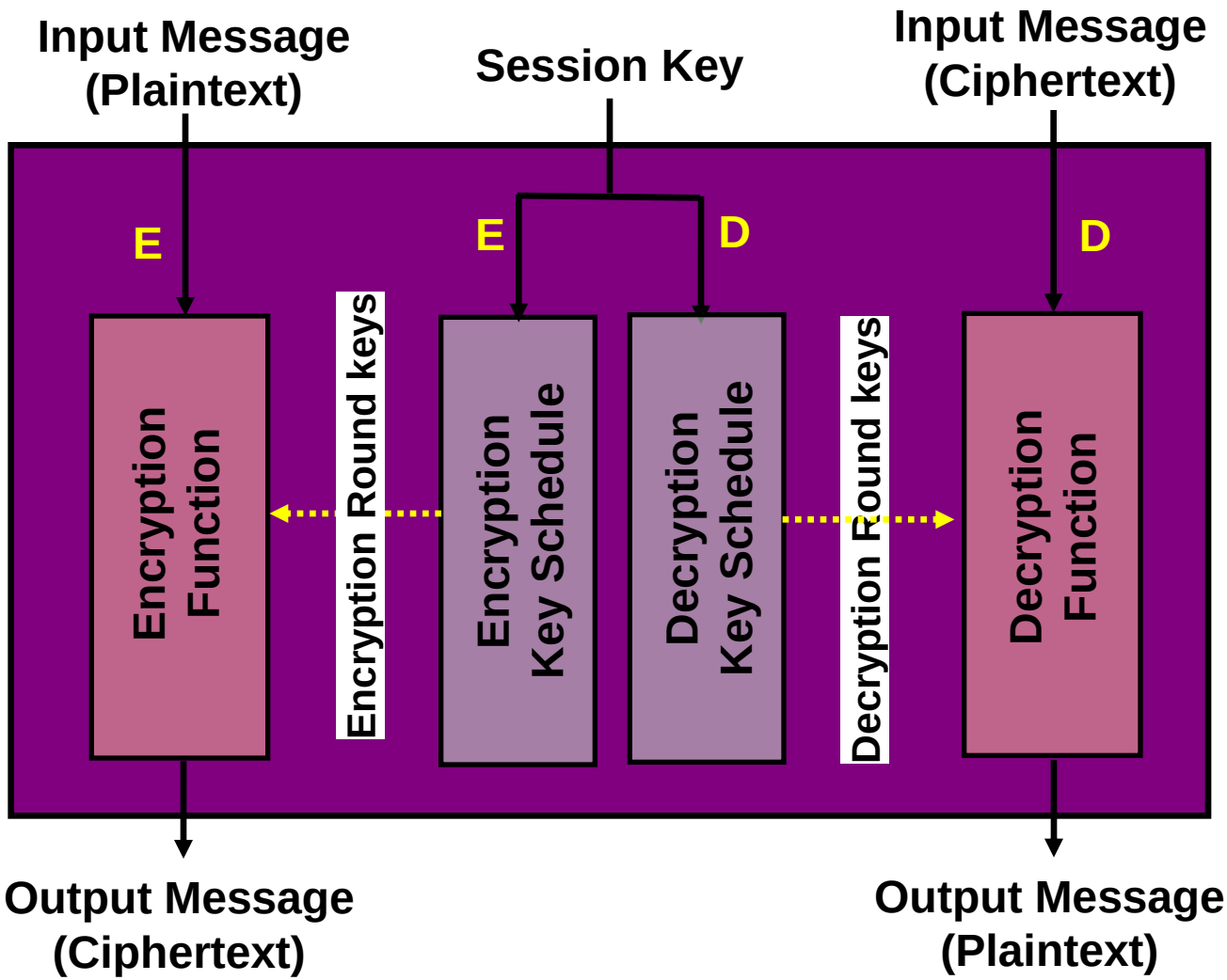
Week 4. : Block Ciphers and DES

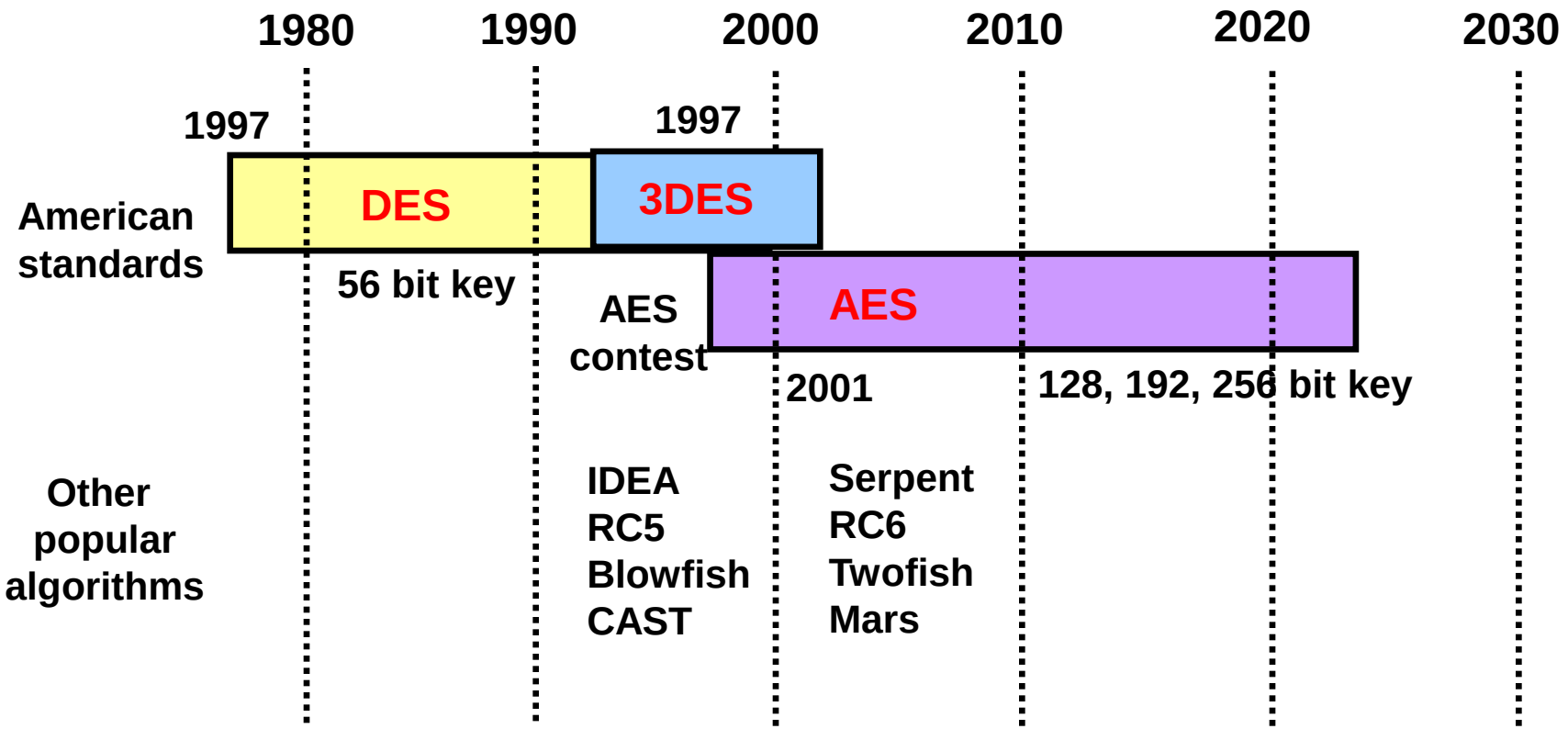
Model of Symmetric Cryptosystem



Block Cipher – A Simplified View



Most Popular Symmetric Ciphers



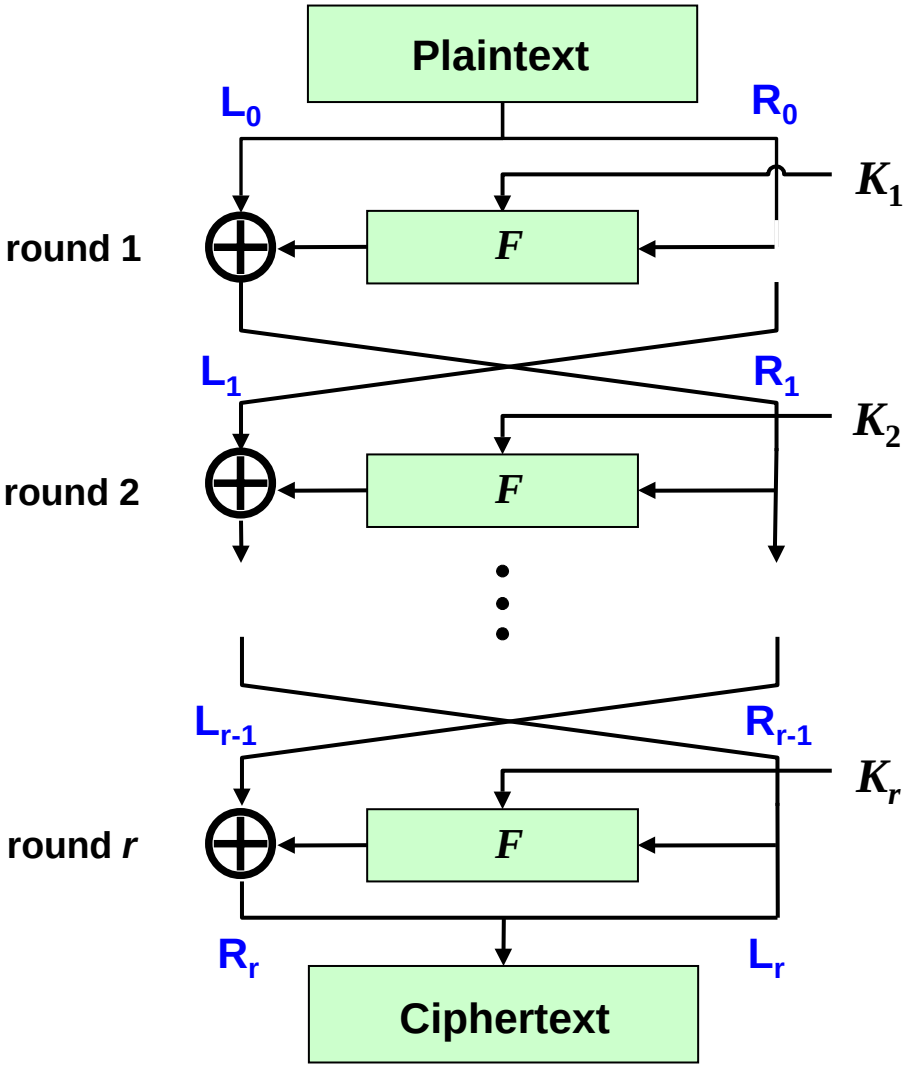
Feistel-type Ciphers

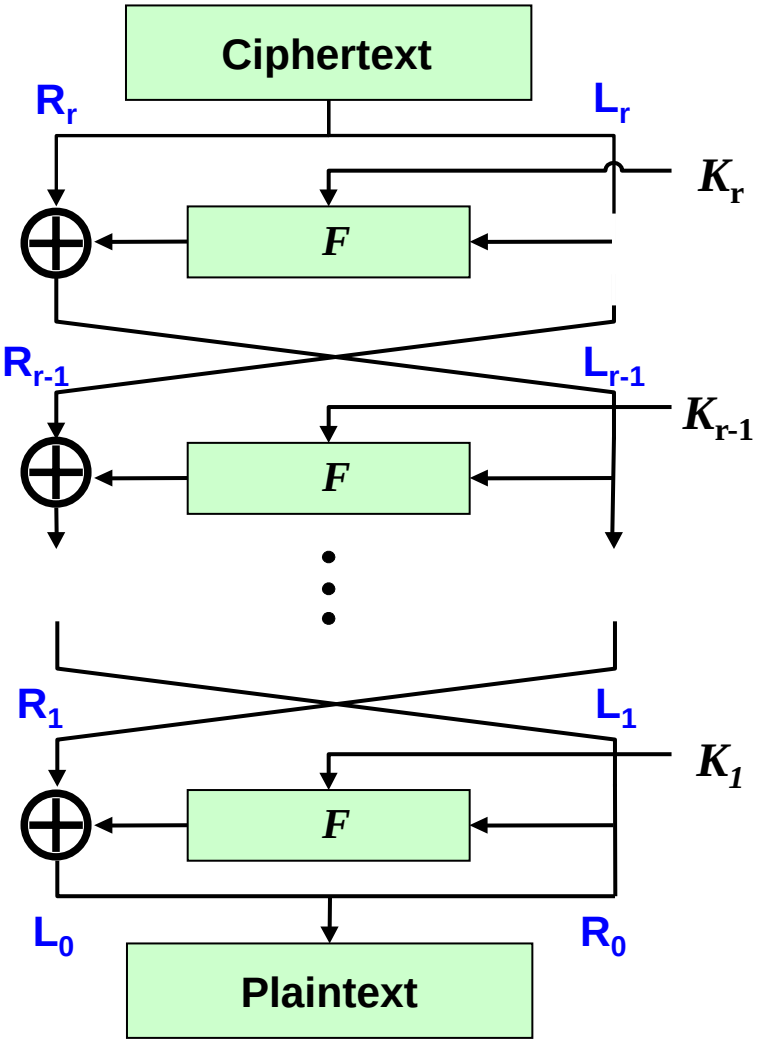
- **Feistel network**
  - **An elegant variant of S-P networks that could be implemented using a single algorithm for both encryption and decryption**
  - ***F( )* does not need to be invertible**

Horst Feistel is best known for his work on the Feistel network construction – a common method for constructing encryption algorithms.

In 1977, he was recognized at the IBM Corporate Technical Recognition Event (CTRE) for
"devising a scheme encrypting binary data which is especially significant to IBM products and is the basis for the recently announced Federal Information Processing Standard adopted by the U.S. Commerce Department."
His work at IBM led to the development of the pioneering Lucifer and Data Encryption Standards (DES) ciphers, and as a result of his efforts, IBM announced the 3845
and 3846 data encryption devices and the IBM cryptographic subsystem.
Feistel earned a bachelor's and a master's degree in physics from MIT and Harvard, respectively. Before joining IBM, he worked with the U.S. Air Force Cambridge Research Center (AFCRC), MIT's Lincoln Laboratory and the Mitre Corporation

Block Cipher Architecture - Feistel-type (Enc & Dec)





Design of Feistel-type Ciphers

- **Design of F-function**
  - ✓ The only non-linear part in the Feistel-type cipher
  - ✓ Need not to be invertible
  - ✓ Typically uses S-boxes (Substitution boxes) for non-linearity
  - ✓ May also contain mixing (permutation) part of the S-box outputs
  - ✓ Determines the ultimate security

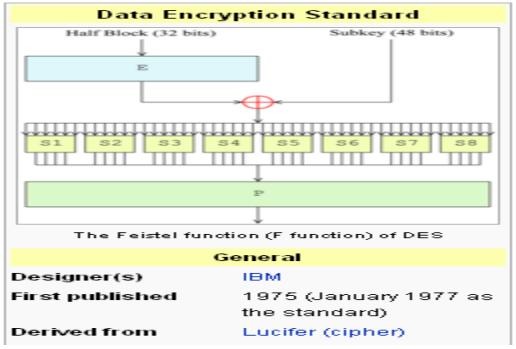
- **Design of Key scheduling algorithm**
  - ✓ Algorithm for deriving as many round keys as necessary from a fixed user key
  - ✓ On-the-fly vs. off-line calculation

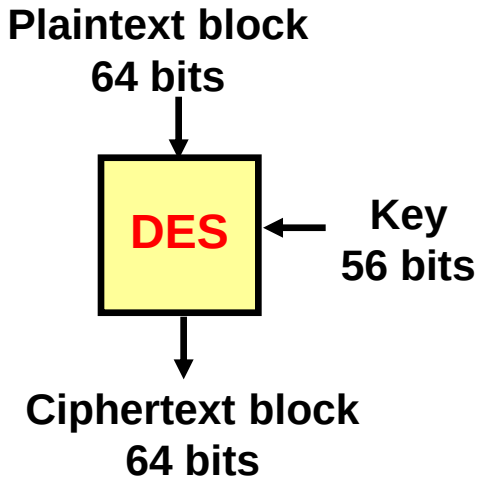
- **Number of rounds**
  - ✓ Depends on the strength of round function (F-function)
  - ✓ A safety margin should be considered for long-term security
  - ✓ Determined through the analysis of the whole algorithm against most powerful known cryptanalysis techniques

Data Encryption Standard (DES)

- **DES - History**
  - ✓ 1976 – adopted as a federal standard
  - ✓ 1977 – official publication as FIPS PUB 46
  - ✓ 1983, 1987, 1993 – recertified for another 5 years

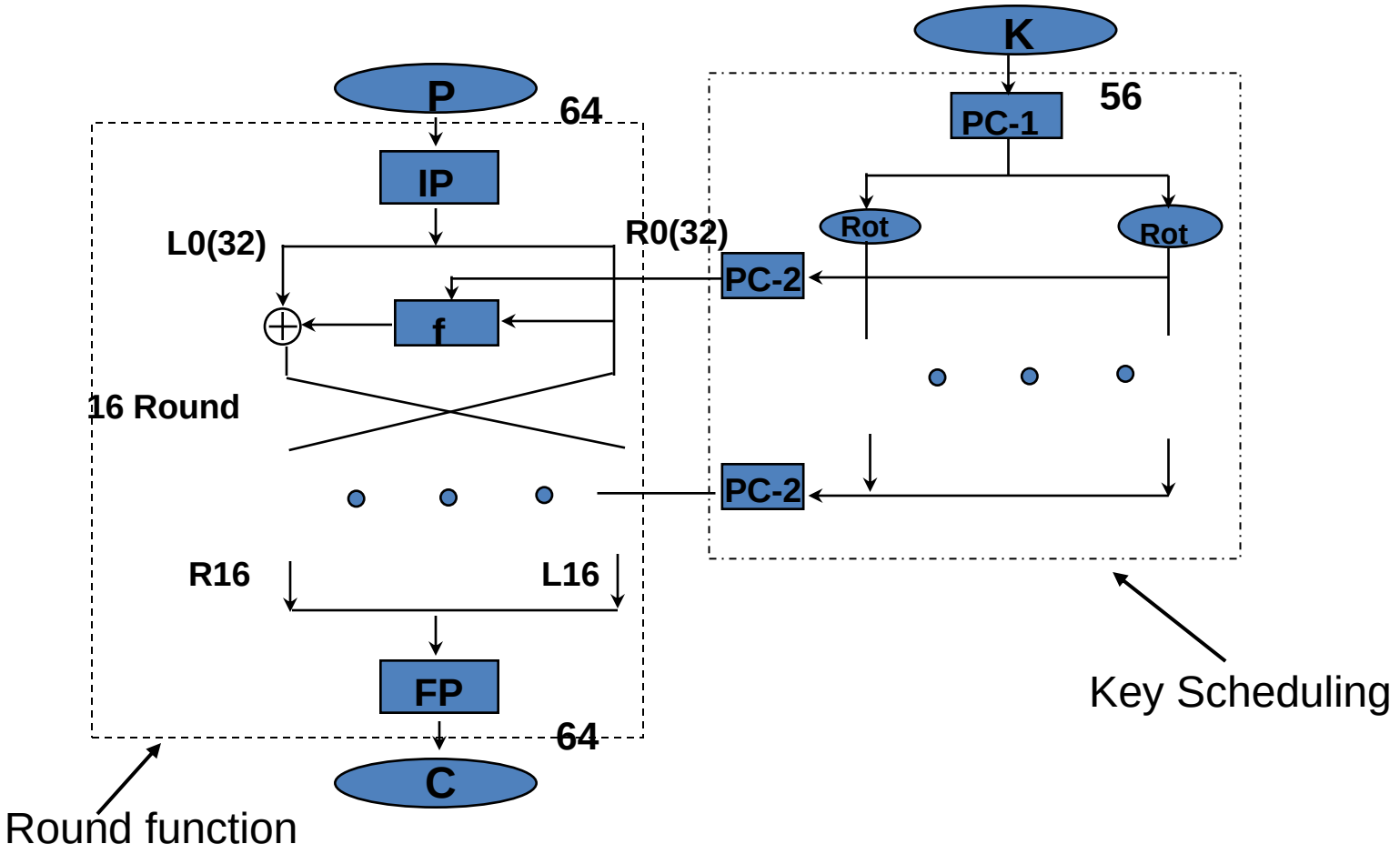
- **Design Criteria of DES**
  - ✓ Provide a high level of security
  - ✓ Completely specify and easy to understand
  - ✓ *Security must depend on hidden key, not algorithm*
  - ✓ Available to all users
  - ✓ Adaptable for use in diverse applications
  - ✓ Economically implementable in electronic device
  - ✓ Able to be validated
  - ✓ Exportable



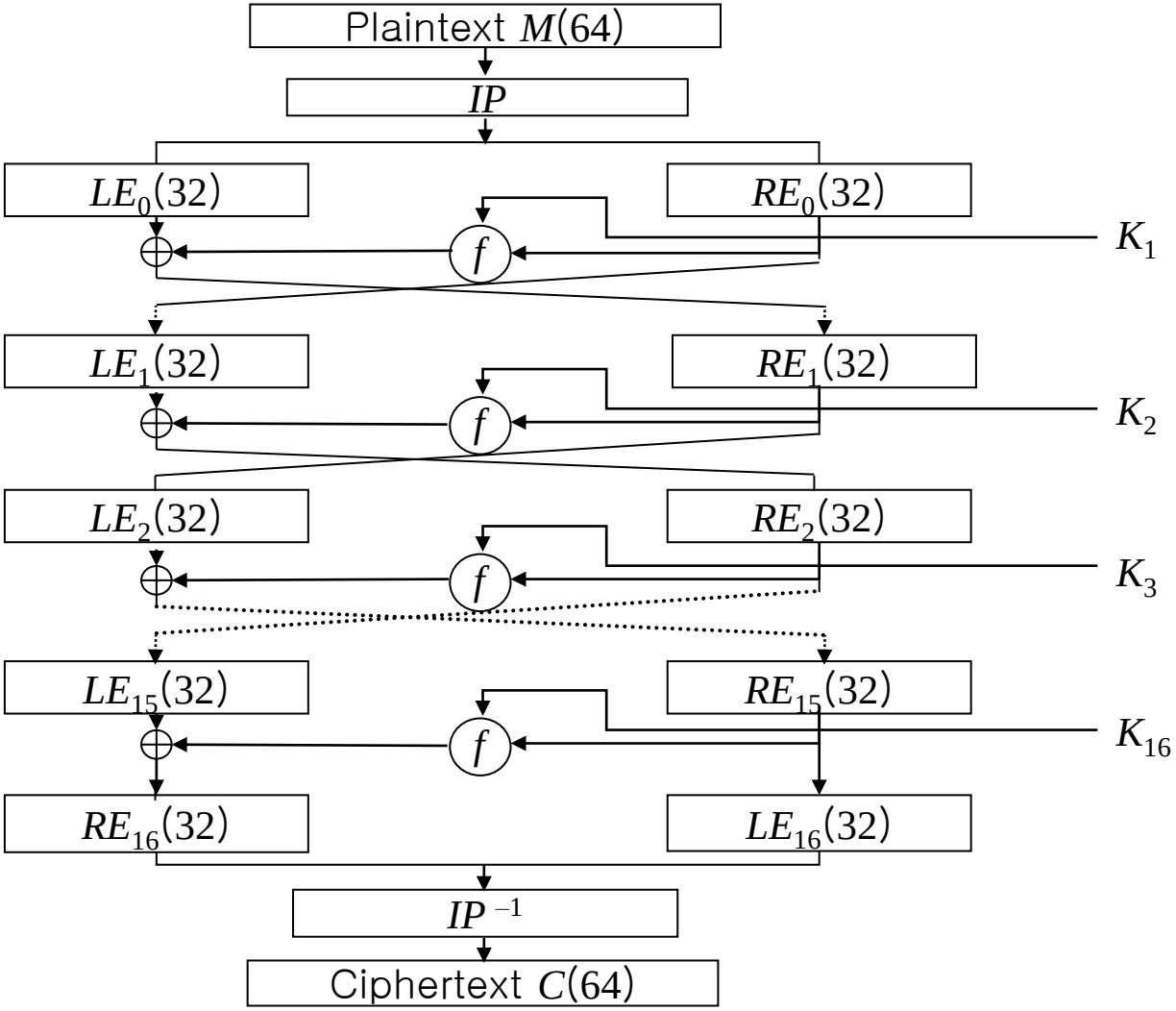


* FIPS: Federal Information Processing Standards

2 Main Blocks of DES



DES – Round Function



Initial Permutation & Final Permutation

_IP_ (Initial permutation)

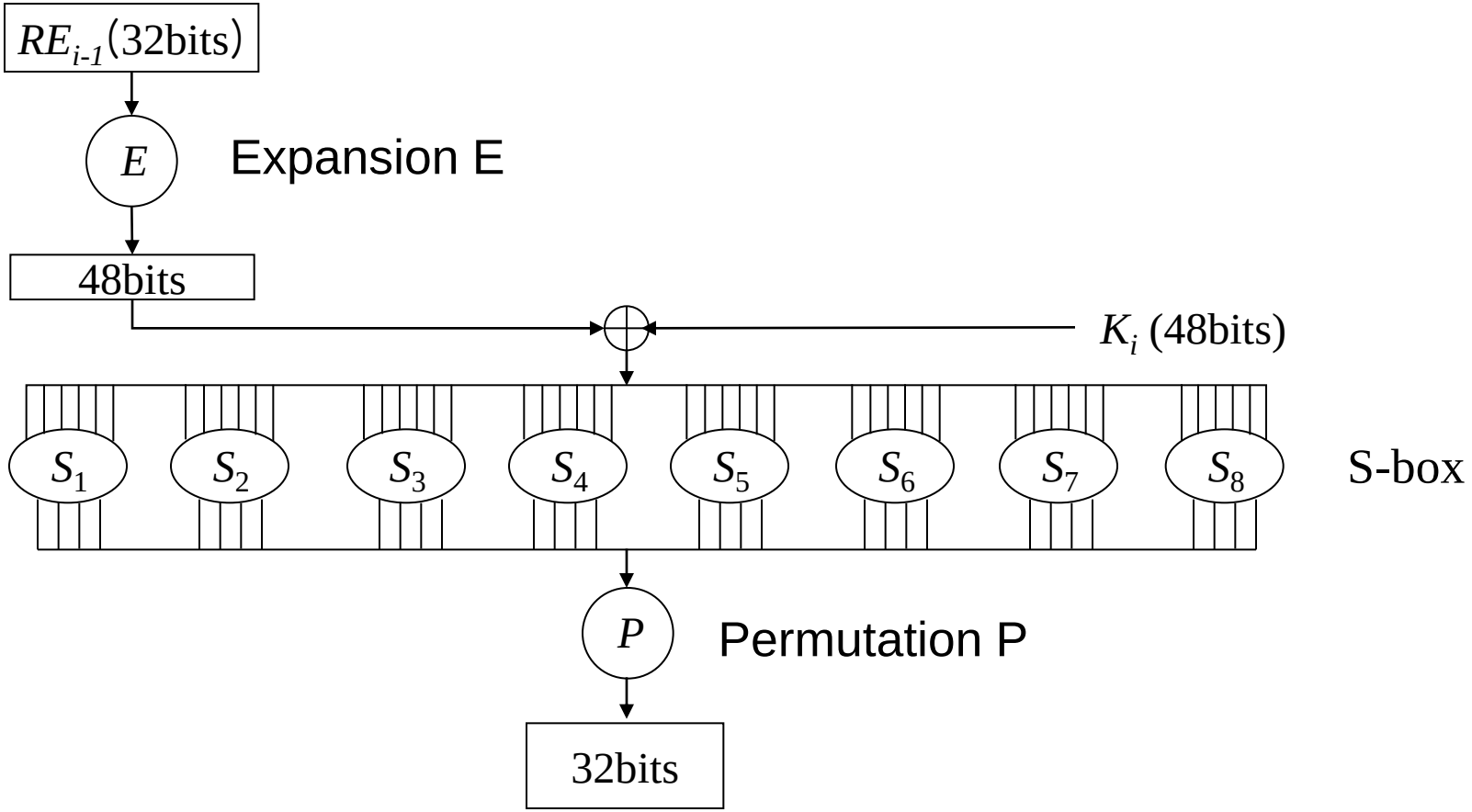
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

_IP_ $^{-1}$ (Final permutation)

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

cf.) The 58th bit of x is the first bit of IP(x)

Function $f(k_i, RE_{i-1})$



Expansion E & Permutation P

Expansion *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

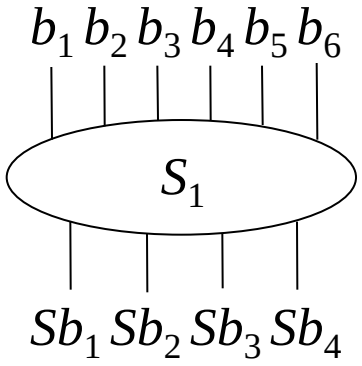
cf.) 32-bits are expanded into 48-bits.
Some bits are selected more than once.

Permutation *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

32-bit → 32-bit permutation

DES S-box (substitution box) (1/3)



Look-up a value from the table using

$b_1\ b_6$: row

$b_2\ b_3\ b_4\ b_5$: column

$b_1\ b_6$: row

S_1-box table

	Sb_1															
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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

$b_2\ b_3\ b_4\ b_5$: column

DES S-boxes(2/3)

- 8 S-boxes (6 → 4 bits)
- some known design criteria
  - ✓not linear
  - ✓Any one bit of the inputs changes at least two output bits
  - ✓S(x) and S(x ⊕ 001100) differs at least 2 bits
  - ✓S(x) ≠ S(x ⊕ 11*ef*00) for any *ef*
  - ✓Resistance against DC etc.
  - ✓The actual design principles have never been revealed (US classified information)

DES S-Boxes(3/3) - examples

S_3-box

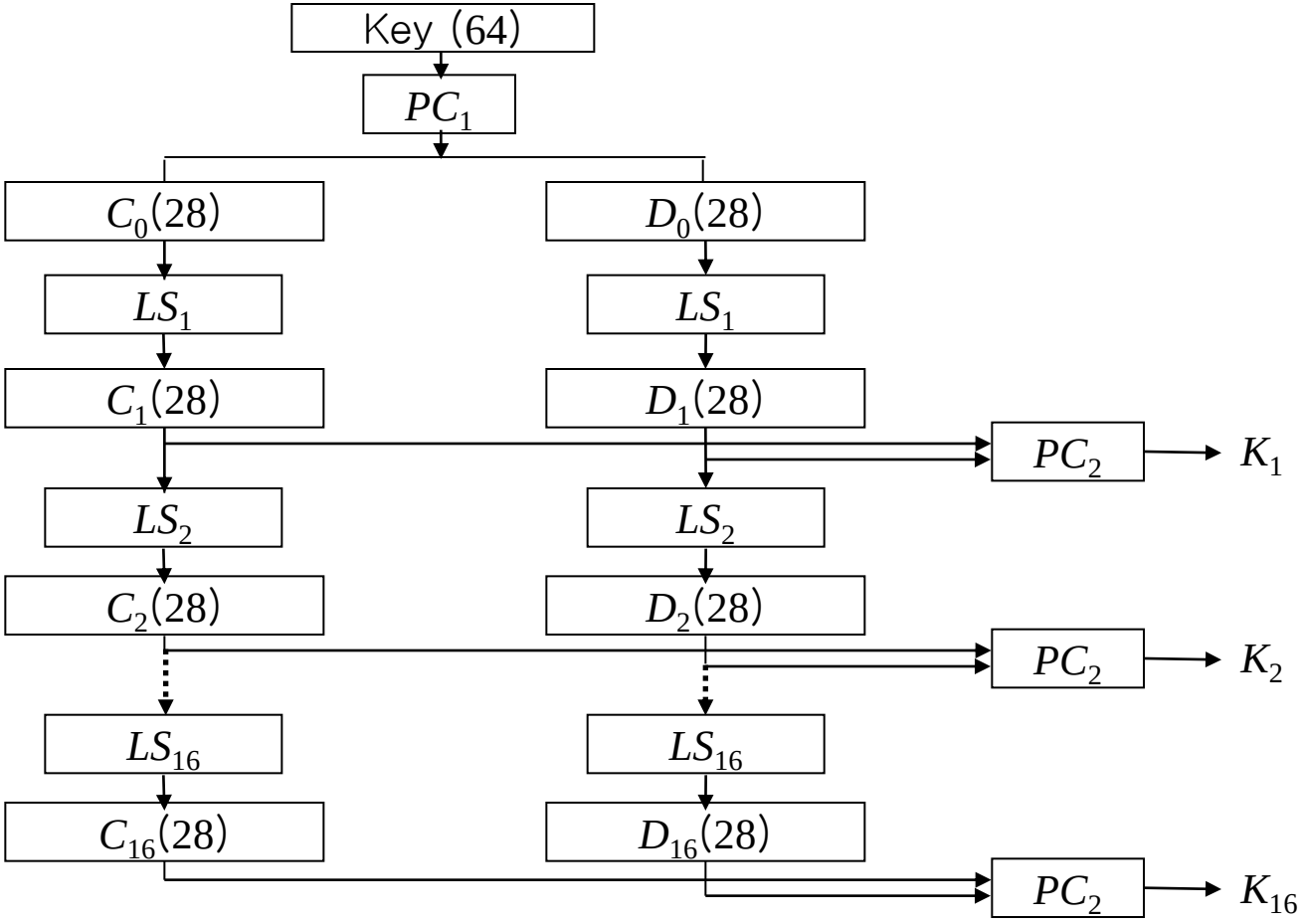
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4-box

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

HW : For the S_4-box, check whether the following property holds
$S_5(x)$ and $S_5(x \oplus 001100)$ differs at least 2 bits

Key Scheduling



Permuted Choice 1 (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

64 bit -> 56 bit (Actual key size of DES is 56-bit)

cf.) Do not use the parity check bits preventing from input error.

8 16 24 32 40 48 56 64 was not selected.

Permuted Choice 2 (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

56 bit -> 48 bit

Note that 9, 18, 22, 25, 35, 38, 43 and 54-th bits were not selected reserved for parity check

Left Shift LS_s

Iteration	Shift	Iteration	Shift
LS_1	1	LS_9	1
LS_2	1	LS_{10}	2
LS_3	2	LS_{11}	2
LS_4	2	LS_{12}	2
LS_5	2	LS_{13}	2
LS_6	2	LS_{14}	2
LS_7	2	LS_{15}	2
LS_8	2	LS_{16}	1

Known Weakness of DES

- Complementary Prop.
  - ✓ If $C = E(K,P)$, $\overline{C} = E(\overline{K}, \overline{P})$
- Weak Key : 4 keys
  - ✓ $E(K, E(K,P))=P$
- Semi-weak Keys : 12 keys (6 pairs)
  - ✓ $E(K_1, E(K_2,P))=P$
- Key Exhaustive Search : 2^{55}

DES Cracking Machine (I)

- **DES - Controversies**
  - ✓ **Unknown design criteria**
  - ✓ **Slow in software**
  - ✓ **Too short key size – 56 bits**

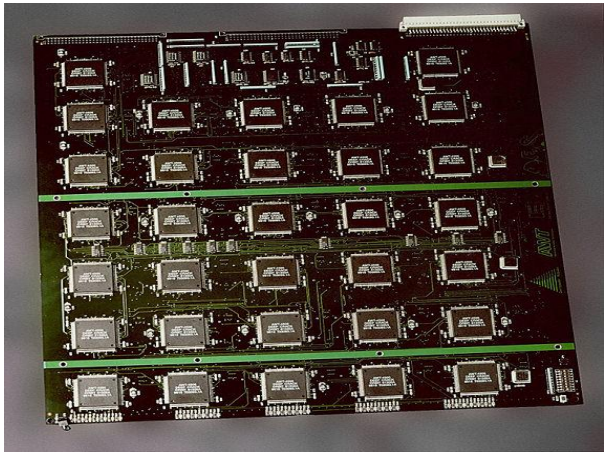
- **DES Crack Machine**
  - ✓ **Can test over 90 billion keys per second**
  - ✓ **EFF's "Deep Crack" and the Distributed.Net computers were testing 245 billion keys per second**
  - ✓ **On Jan. 19, 1999, RSA DES-III Challenge was deciphered after searching 22hr and 15min.**

http://www.rsa.com/rsalabs/node.asp?id=2108

Identifier: DES-Challenge-III
Cipher: DES
Start: January 18, 1999 9:00 AM PST
Prize: $10,000
IV: da 4b be f1 6b 6e 98 3d
Plaintext: See you in Rome (second AES Conference, March 22-23, 1999)

DES Cracking Machine (II)

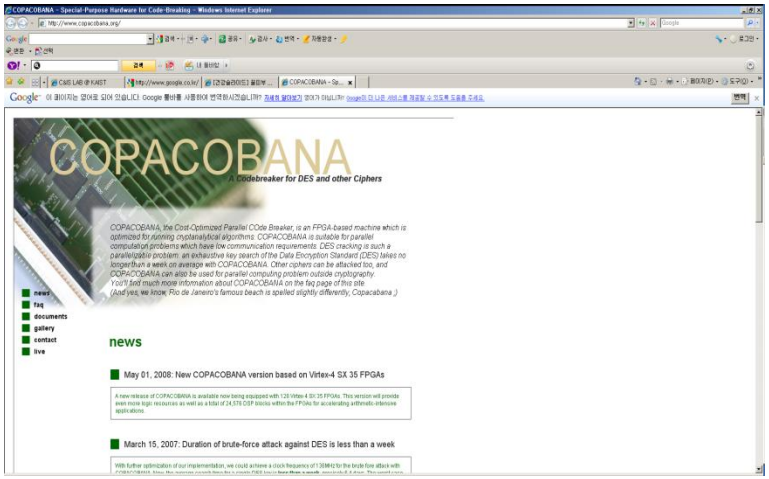
- Distributed.Net + EFF
  - 100,000 PC on Network
  - 56hr
  - http://www.distributed.net/Main_Page
- EFF(Electronic Frontier Foundation), 1989
  - Specific tools
  - 22hr 15min
  - 250,000$
  - http://en.wikipedia.org/wiki/EFF_DES_cracker

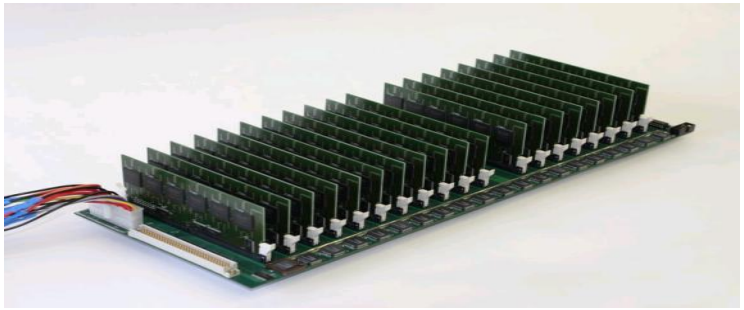


P. Kocher

DES Cracking Machine(III)

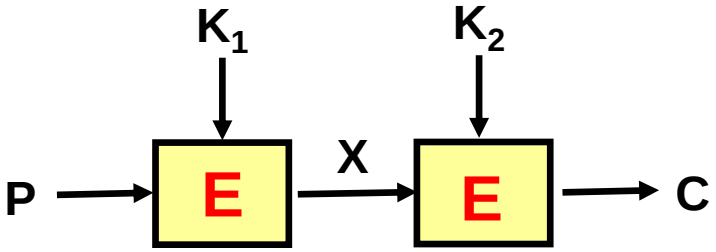
- COPACOBANA) Cost-Optimized Parallel COde Breaker is an FPGA Machine by Univ. of Bochum, Germany
- Commercially available 120 FPGA's of type XILINX Spartan3-1000 run in parallel
- 10,000$ of ¼ of EFF project
  - http://en.wikipedia.org/wiki/EFF_DES_cracker

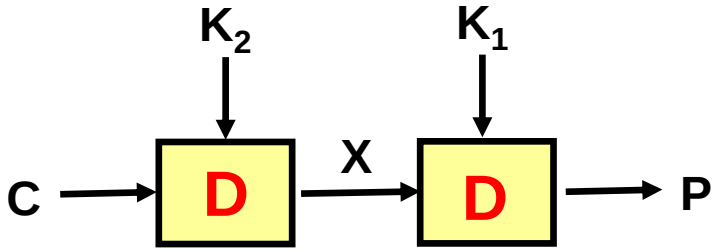




Double DES & 3DES

- How to strengthen existing DES implementations ?
- Double DES
  - Essentially no security increase: $E_{K1}(P) = X = D_{K2}(C)$ Meet-in-the-middle attack !





- 3DES
  - Three-key or Two-key 3DES: $K_1 = K_3$