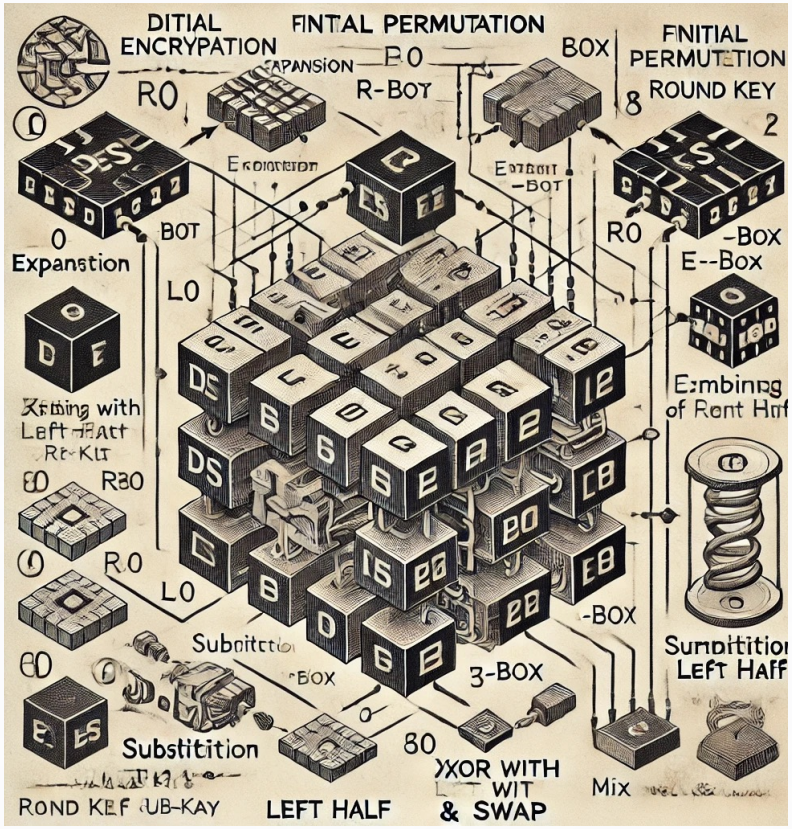


DES: Data Encryption Standard

Budi Rahardjo
@rahard – budi@indocisc.com
2025

Sejarah DES

- Dikenal juga sebagai Data Encryption Algorithm (DEA) oleh ANSI dan DEA-1 oleh ISO
- Pemerintah Amerika (National Bureau of Standards) membuka usulan untuk standar enkripsi (1973)
- Bermula dari **Lucifer**, enkripsi yang dikembangkan oleh **IBM** pada saat itu
- Horst Feistel, pengembang DES dari IBM Watson Laboratory di Yorktown Heights, New York

Tentang Lucifer

```
      ∇DET[⎕]∇
     ∇ Z←DET A;B;P;I
[1]   I←⎕IO
[2]   Z←1
[3]  L:P←(|A[;I])⍳⌈/|A[;I]
[4]   →(P=I)/LL
[5]   A[I,P;]←A[P,I;]
[6]   Z←-Z
[7]  LL:Z←Z×B←A[I;I]
[8]   →(0 1 ∨.=Z,1↑⍴A)/0
[9]   A←1 1 ↓A-(A[;I]÷B)∘.×A[I;]
[10]  →L
[11] ⍝EVALUATES A DETERMINANT
     ∇
```

Algorima yang dikembangkan
IBM menggunakan
bahasa **APL**, dengan nama *"Demonstration"*

Nama terlalu panjang, disingkat menjadi *"Demon"*

Diplesetkan sebagai "hantu" atau "setan"

Versi berikutnya diberi nama guyonan *"Lucifer"*

Sejarah DES

- Diadopsi oleh National Bureau of Standards di tahun 1977
- Dikenal dengan Federal Information Processing Standard 46 (FIPS PUB 46-3)
- Reaffirmed 25 Oktober 1999
- Sekarang sudah dianggap **tidak aman** karena terbatasnya panjang kunci yang dapat di-brute-force

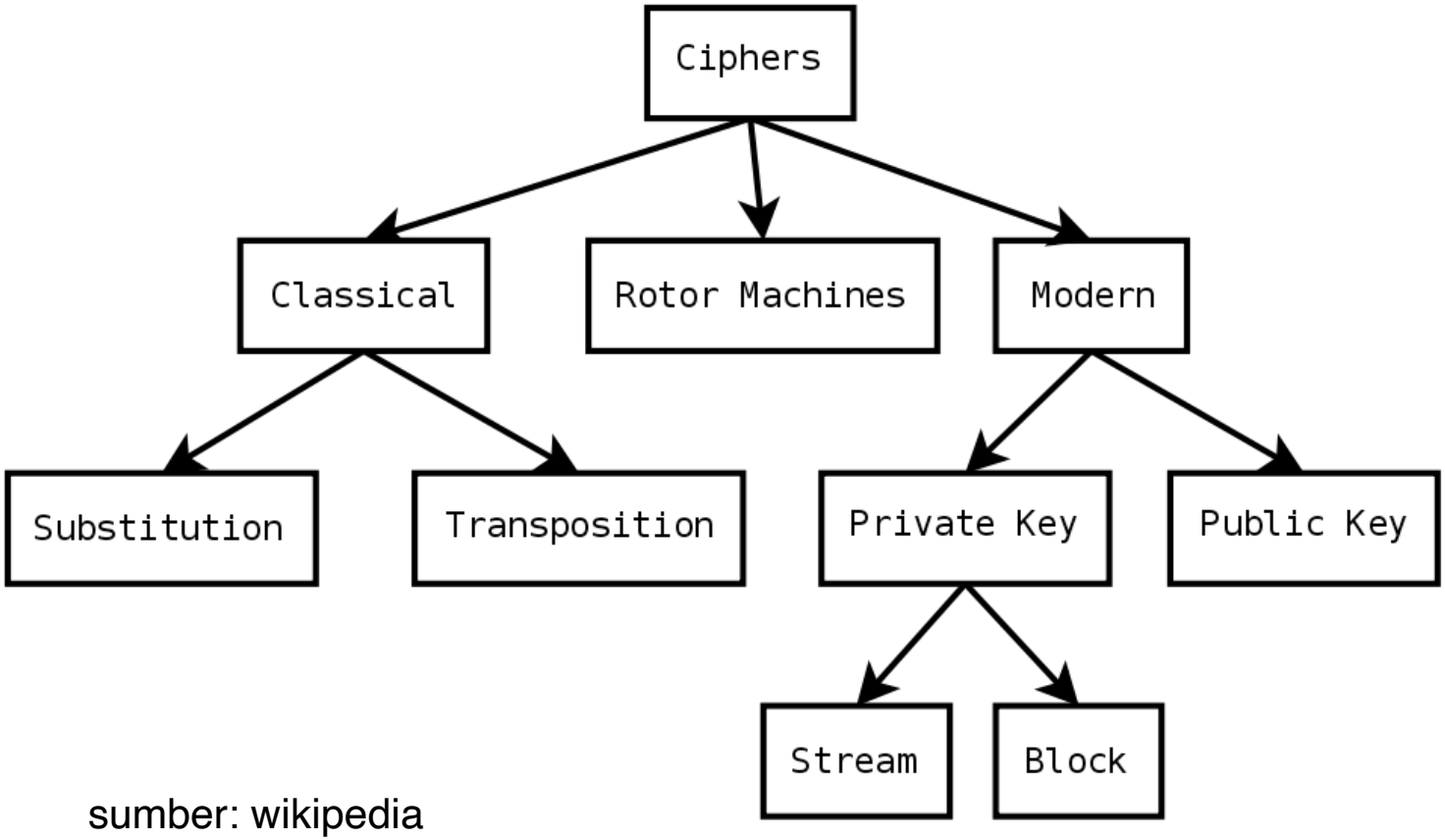
DES

- Block cipher
  - Blok data: 64 bit
  - Kunci: 56 bit (dari 64 bit, 8 bit merupakan checksum – setiap bit yang berada di posisi ke 8 dibuang; 8, 16, 24, 32, 40, 48, 56, 64).

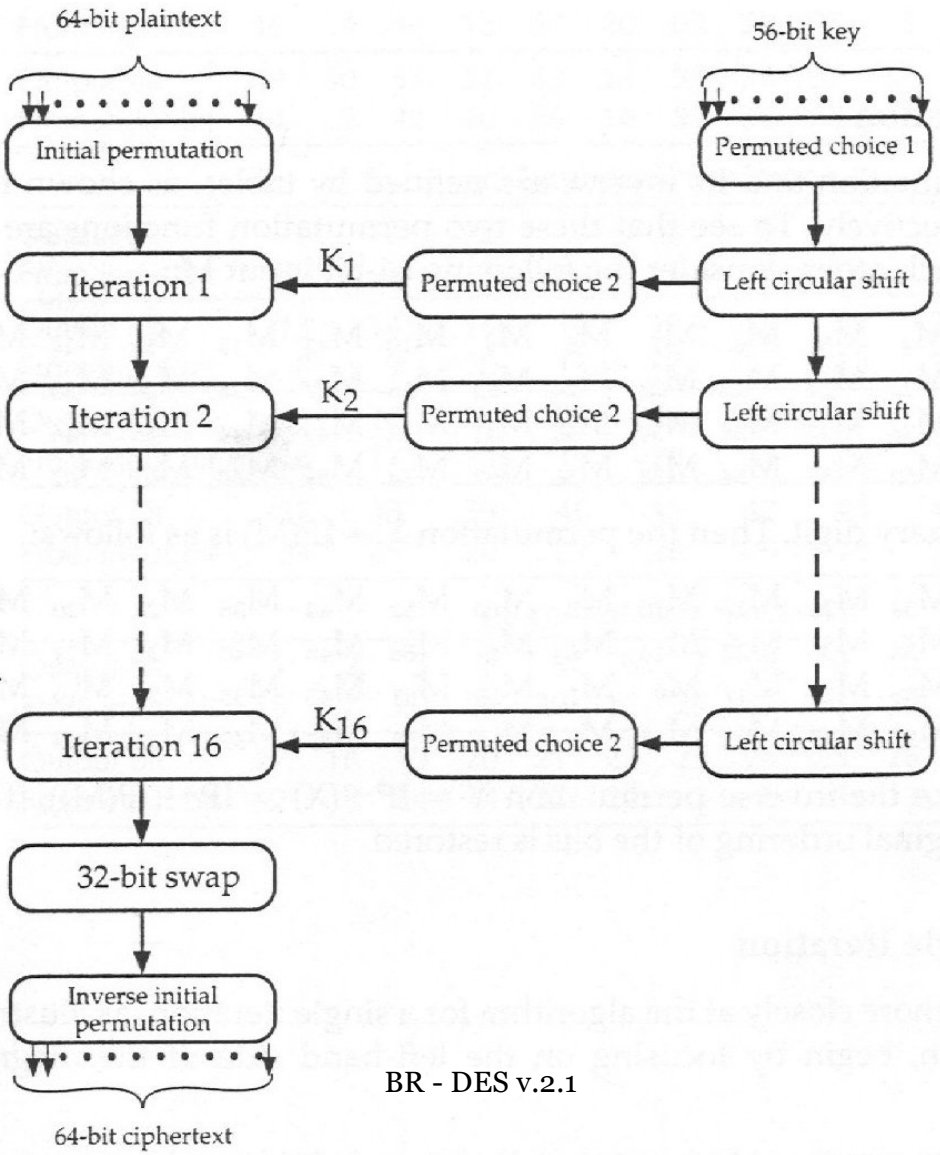
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discording of every 8th bit of original key

Cipher Taxonomy



sumber: wikipedia


64-bit plaintext
56-bit key
Initial permutation
Permuted choice 1
Iteration 1
K1
Permuted choice 2
Left circular shift
Iteration 2
K2
Permuted choice 2
Left circular shift
Iteration 16
K16
Permuted choice 2
Left circular shift
32-bit swap
Inverse initial permutation
64-bit ciphertext

Initial Permutation

(a) Initial Permutation (IP)

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

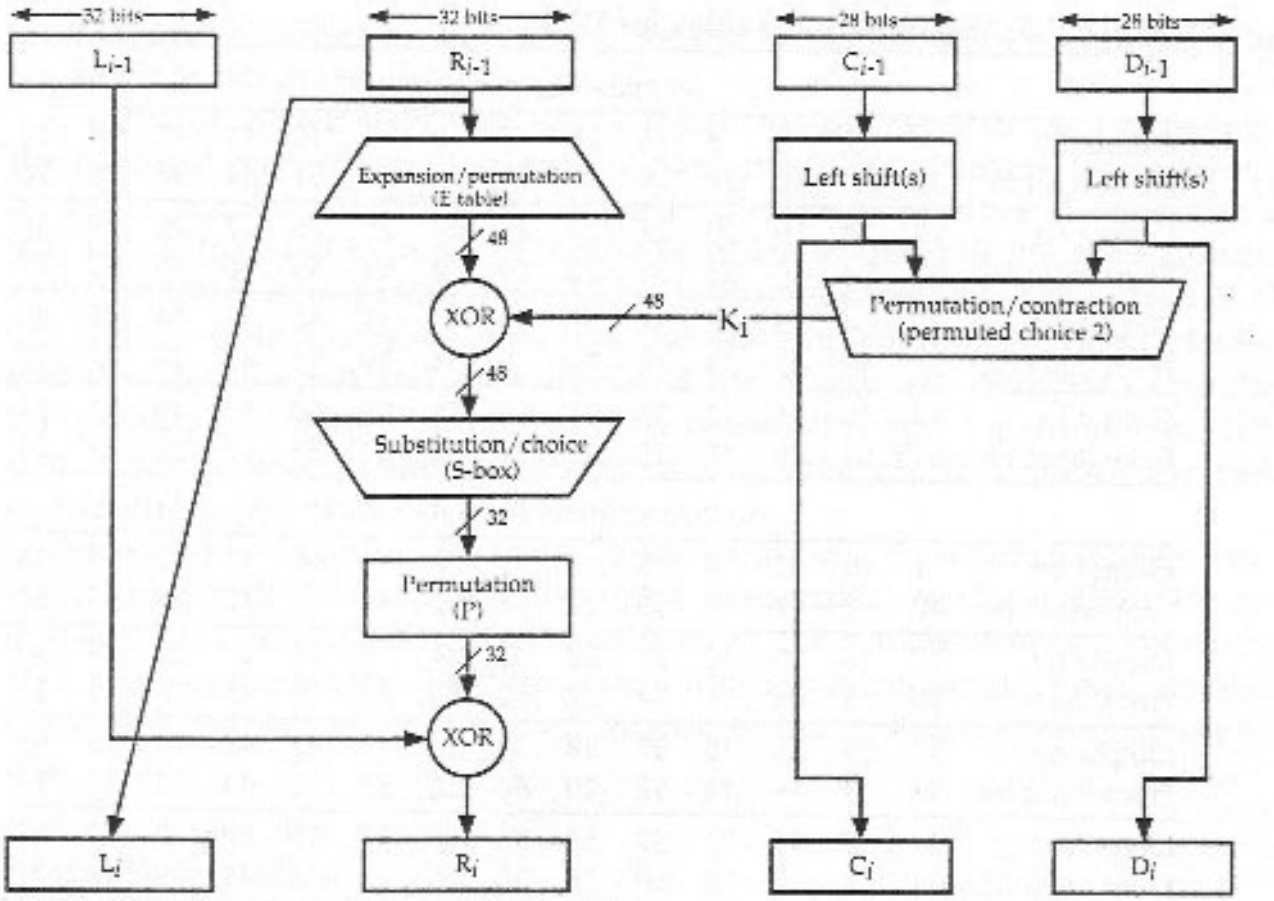
Inverse Initial Permutation

(b) Inverse Initial Permutation (IP^{-1})

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

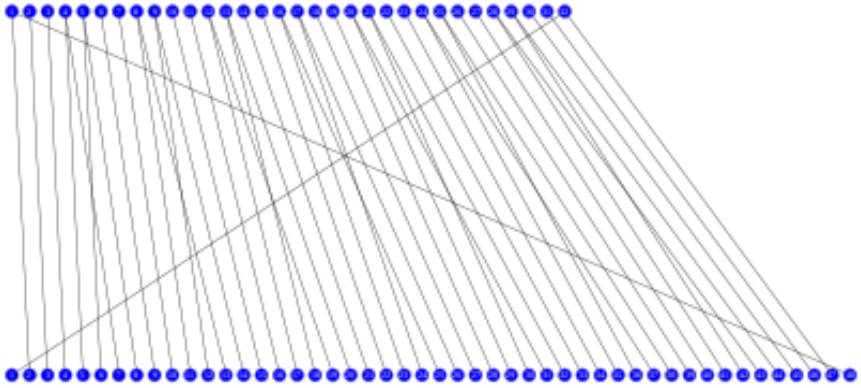
Permuted Choice One (PC-1)

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


32 bits
32 bits
28 bits
28 bits
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
Expansion / permutation (E table)
Left shift(s)
Left shift(s)
48
XOR
48
K_i
Permutation / contraction (permuted choice 2)
48
Substitution / choice (S-box)
32
Permutation (P)
32
XOR
L_i
R_i
C_i
D_i

Expansion

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



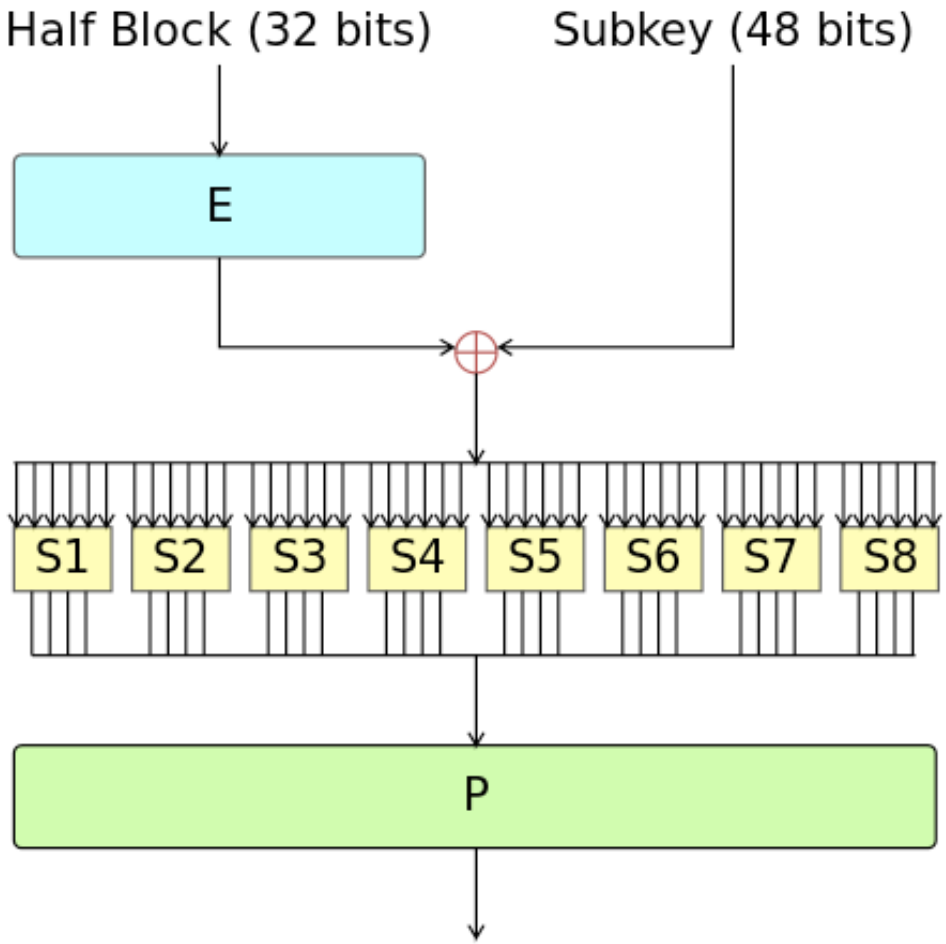
Keys: rotated and compressed

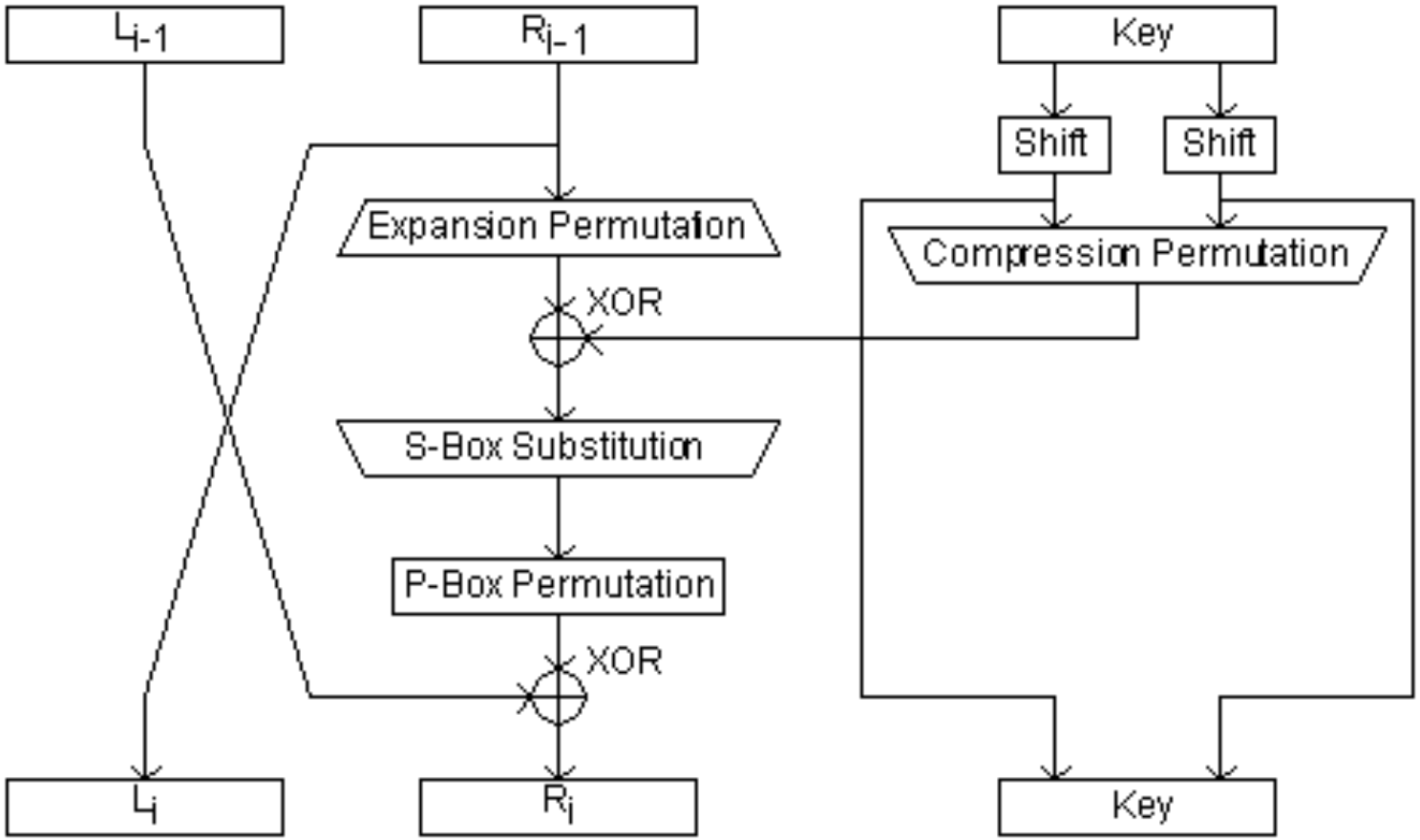
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

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

Figure - compression permutation


Half Block (32 bits)
Subkey (48 bits)
E
S1
S2
S3
S4
S5
S6
S7
S8
P


Li-1
Ri-1
Key
Shift
Shift
Expansion Permutation
Compression Permutation
XOR
S-Box Substitution
P-Box Permutation
XOR
Li
Ri
Key

S-box

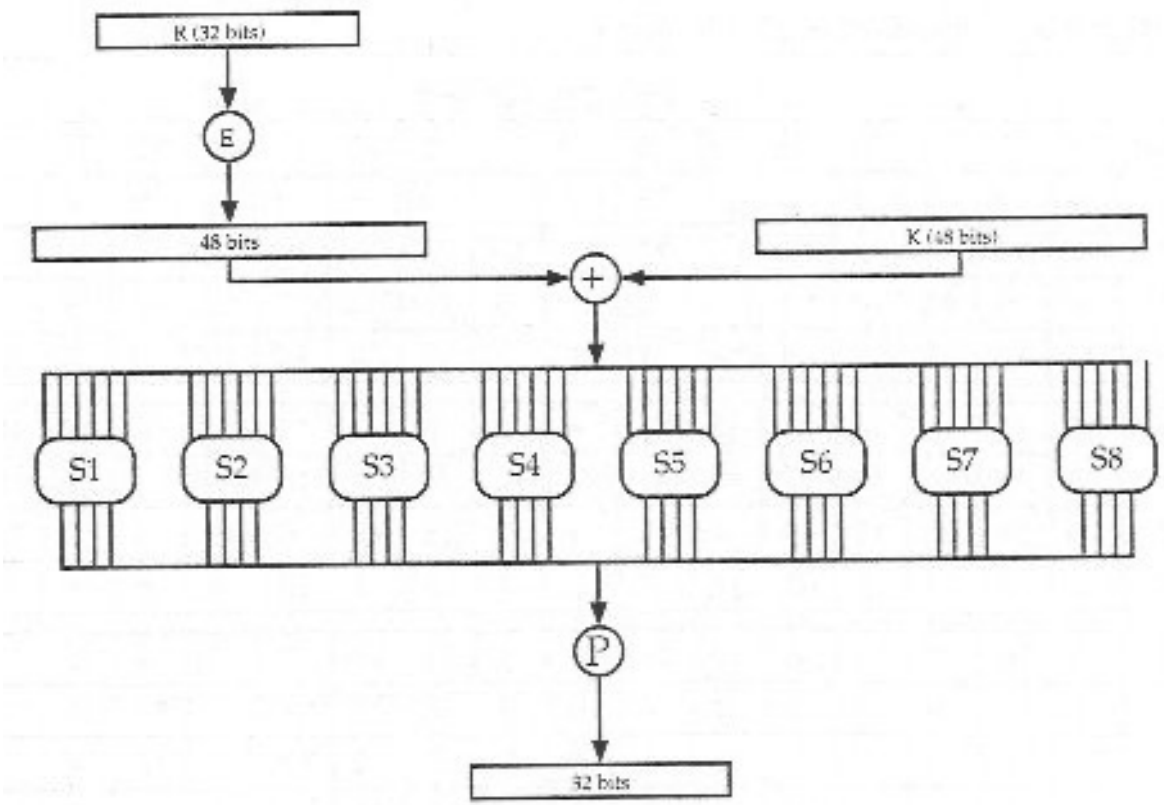
S_1	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

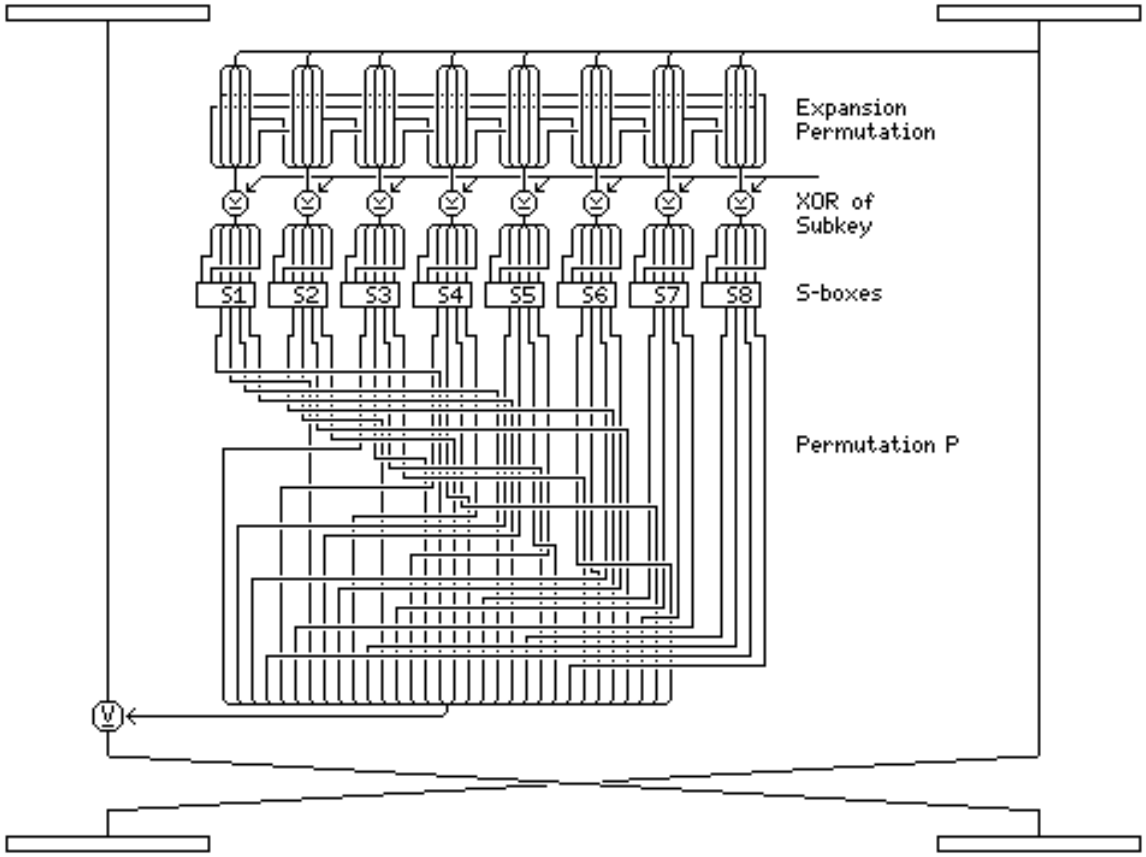
Permuted Choice 2
(Compression Permutation)

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

Scheduled of Left Shifts

Iteration number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1


R (32 bits)
E
48 bits
K (48 bits)
+
S1
S2
S3
S4
S5
S6
S7
S8
P
32 bits


Expansion
Permutation
XOR of
Subkey
S1
S2
S3
S4
S5
S6
S7
S8
S-boxes
Permutation P

S-boxes

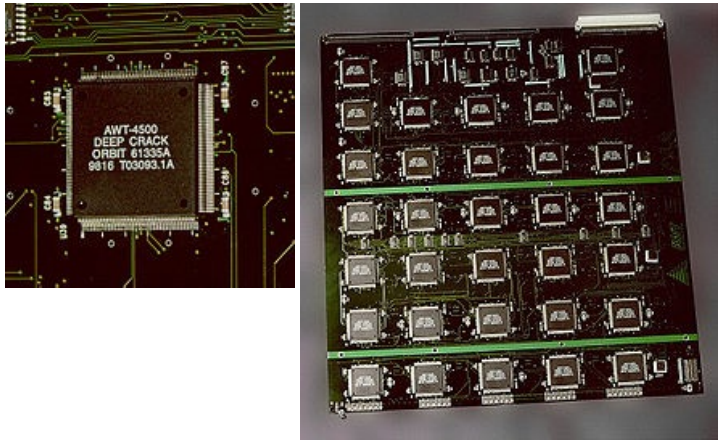
	Column Number																Box
Row	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S_2
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	

Cracking DES

- Kunci 56 bit
- Brute force attack membutuhkan 2^{56} (sekitar 70 juta milyar) kombinasi
- Kemampuan komputasi saat ini sudah dapat memecahkan hal tersebut
- distributed.net memecahkan dalam waktu 30 hari

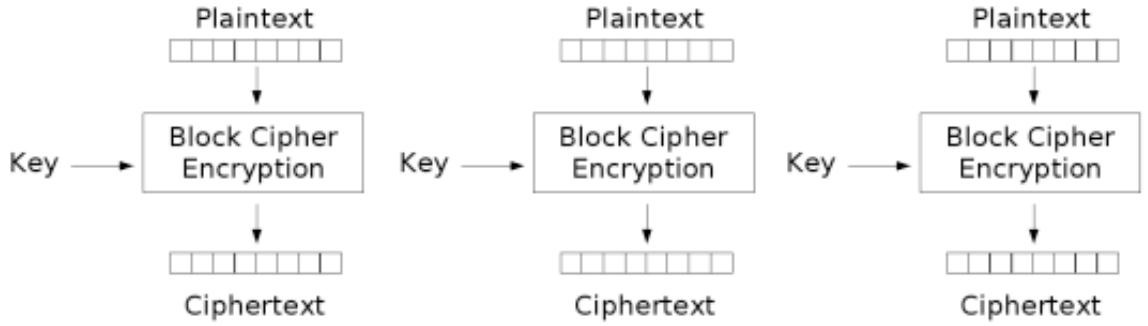
- Electronic Frontier Foundation (EFF) membuat chip DES cracker seharga US$250.000 dan dapat memcahkan DES dalam waktu rata-rata 4 s/d 5 hari

- EFF's Deep Crack

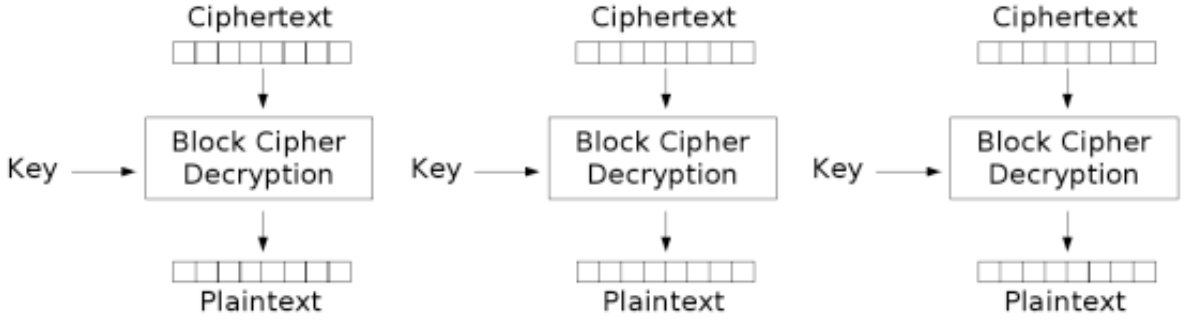


http://en.wikipedia.org/wiki/EFF_DES_cracker
http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

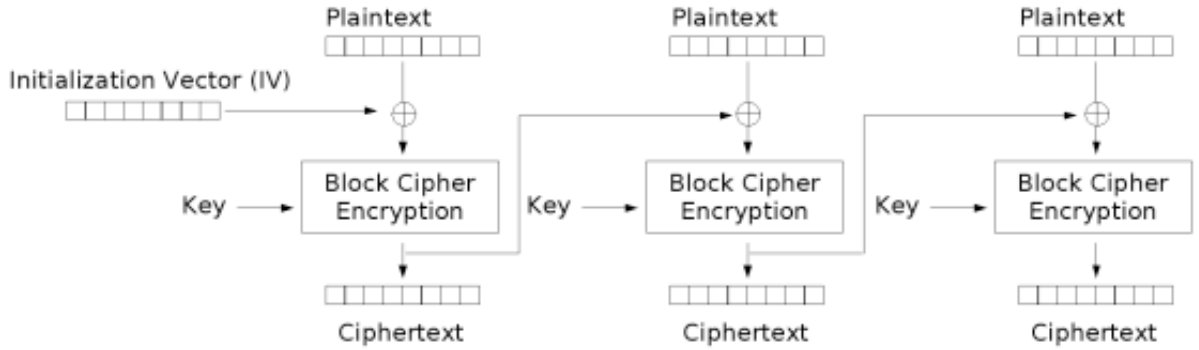


Electronic Codebook (ECB) mode encryption

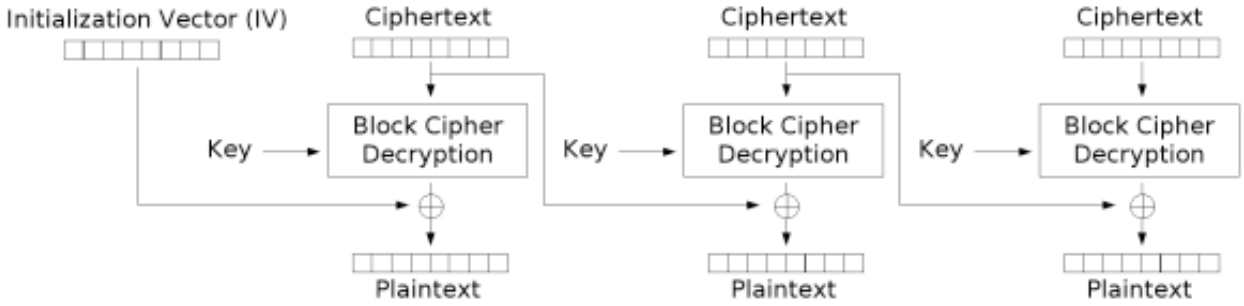


Electronic Codebook (ECB) mode decryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

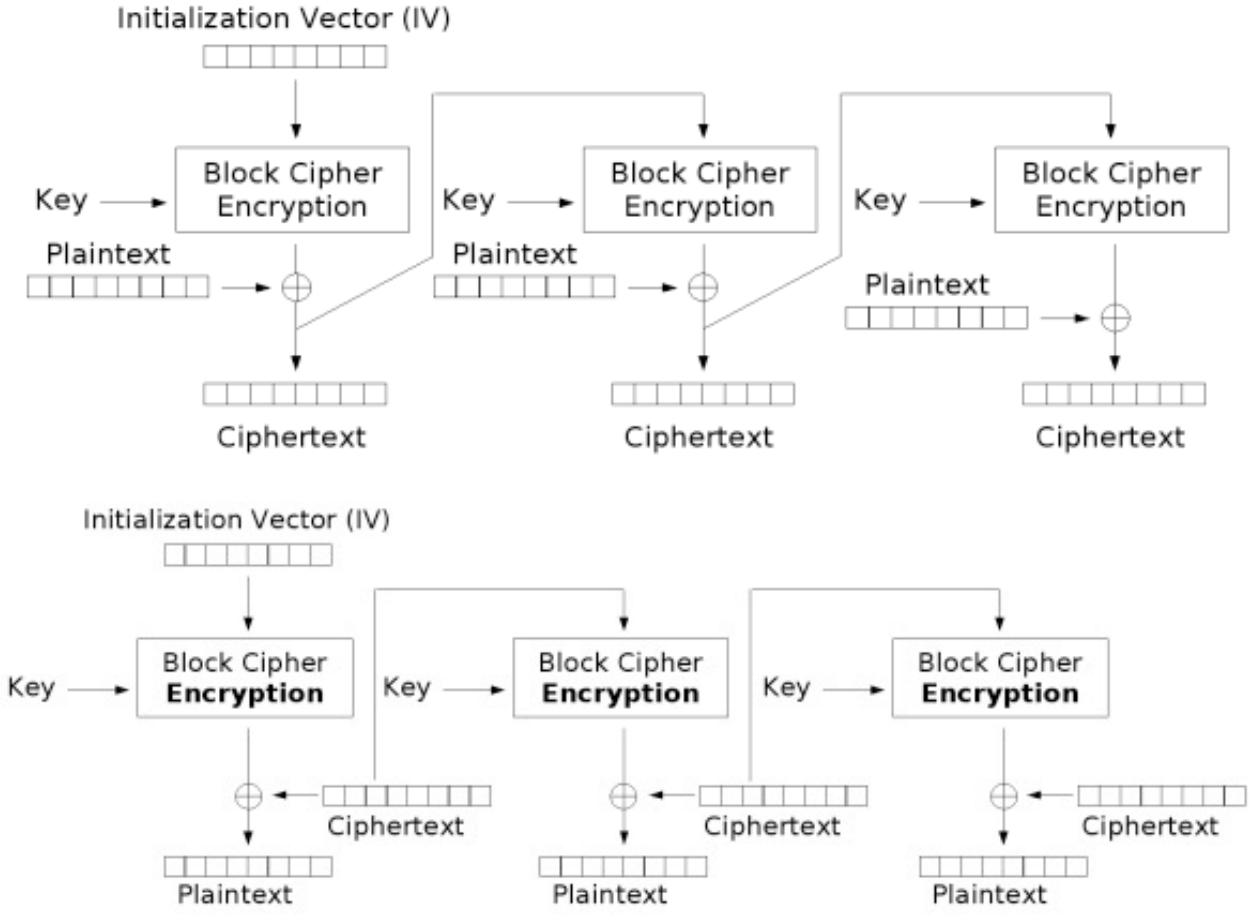


Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation



Cipher Feedback (CFB) mode decryption