Criptografia FIB

DES: Data Encryption Standard

Anna Rio

Departament de Matemàtica Aplicada II • Universitat Politècnica de Catalunya

DES

Data Encryption Standard

- Dissenyat por IBM
- Sistema de xifratge en bloc: blocs de 64 bits, claus de 56 bits
- El 1998 va ser trencat (*DES Cracker* de la Electronic Frontier Foundation)
- Estàndard FIPS 46-3 des de 1976. Retirat el 19 de maig de 2005

  > *because FIPS 46-3, DES, no longer provides the security that is needed to protect Federal government information.*

- Encara vigent Triple DES (clau de 112 bits)

  NIST Special Publication 800-67: Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Maig 2004)

DES: Data Encryption Standard

Xifra blocs de 64 bits amb una clau de 56 bits

Història

1973 El NBS (National Bureau of Standards) demana públicament propostes de sistemes criptogràfics, que:

- Proporcionin un alt nivell de seguretat i siguin eficients.
- La seguretat depengui només del secret de la clau (no del secret de l'algoritme).
- Puguin adaptar-se a diverses aplicacions.
- La implementació en dispositius electrònics sigui barata.

1974 Segona crida: IBM presenta LUCIFER. La NSA (National Security Agency) proposa canvis i són acceptats.

1975 El 17 de març el NBS publica els detalls del DES.

1976 El 23 de novembre és adoptat pel govern USA per a la transmisió i emmagatzematge d'informació no classificada. Es revisarà cada cinc anys.

1981 Diversos organismes privats l'adopten com a estàndard.

1983 Es ratifica com a estàndard sense problemes.

1987 La NSA s'oposa a una nova ratificació però, por motius econòmics, finalmente es renova.

1992 Per manca d'alternatives es torna a renovar.

1997 El 17 de juny el DES es trenca. A començaments d'any RSA llença el repte i en quatre mesos es troba la solució, havent examinat aproximadament el 25% de les claus.

1998 El 26 de febrer el DES es torna a trencar. Només han calgut 39 dies, per examinar aproximadamente el 85% de les claus. El 17 de juliol la Electronic Frontier Foundation (EFF) presenta el seu DES craker, que pot trencar el DES utilitzant la cerca exhaustiva en un temps mitjà de 4.5 dies.

1999 El 19 de gener la EFF trenca el DES en menys de 23 hores.

2001 Substituit pel AES (Advanced Encryption Standard).

DES: Descripció de l'algoritme

1. A un bloc X (64 bits), se li aplica una permutació inicial IP,

$$x_0 = IP(X) \equiv L_0 R_0$$

2. Es realitzen 16 iteracions del tipus:

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

3. S'aplica la permutació inversa de IP a $R_{16}L_{16}$,

$$Y = IP^{-1}(R_{16}L_{16})$$

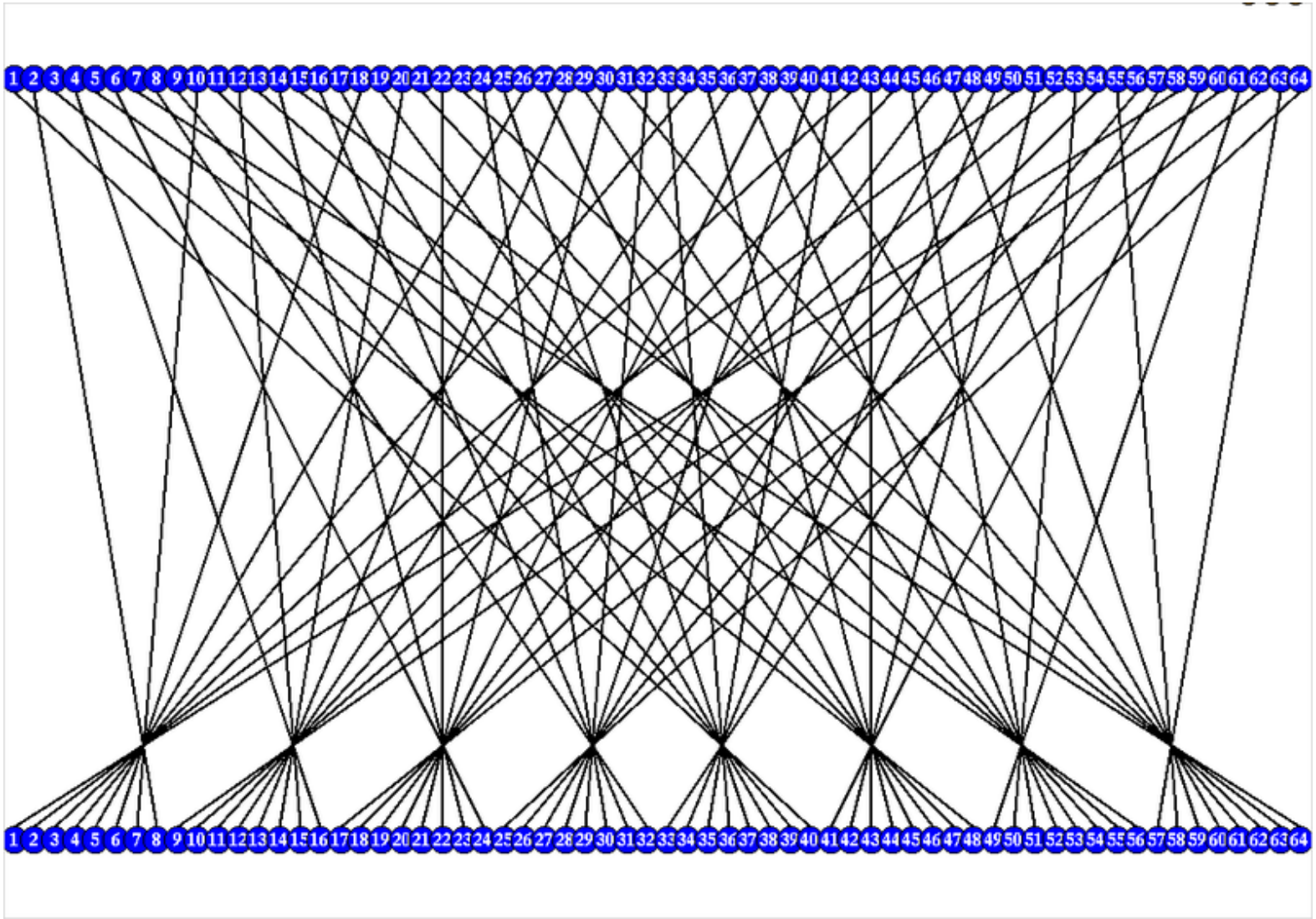
Transformació inicial IP

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	29	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

$$64! = 126886932185884164103433389335161480802865516174545192198801894375214704230400000000000000$$

Transformació inicial IP



DES: Descripció de l'algoritme

Sobre blocs de 64 bits, definim les funcions:

- $\theta =$ intercanvi de les parts esquerra i dreta
- $\lambda_{f_i} : x \longrightarrow y \qquad$ on $\begin{array}{ll} L_y & = L_x \oplus f(R_x, k_i), \\ R_y & = R_x, \end{array}$

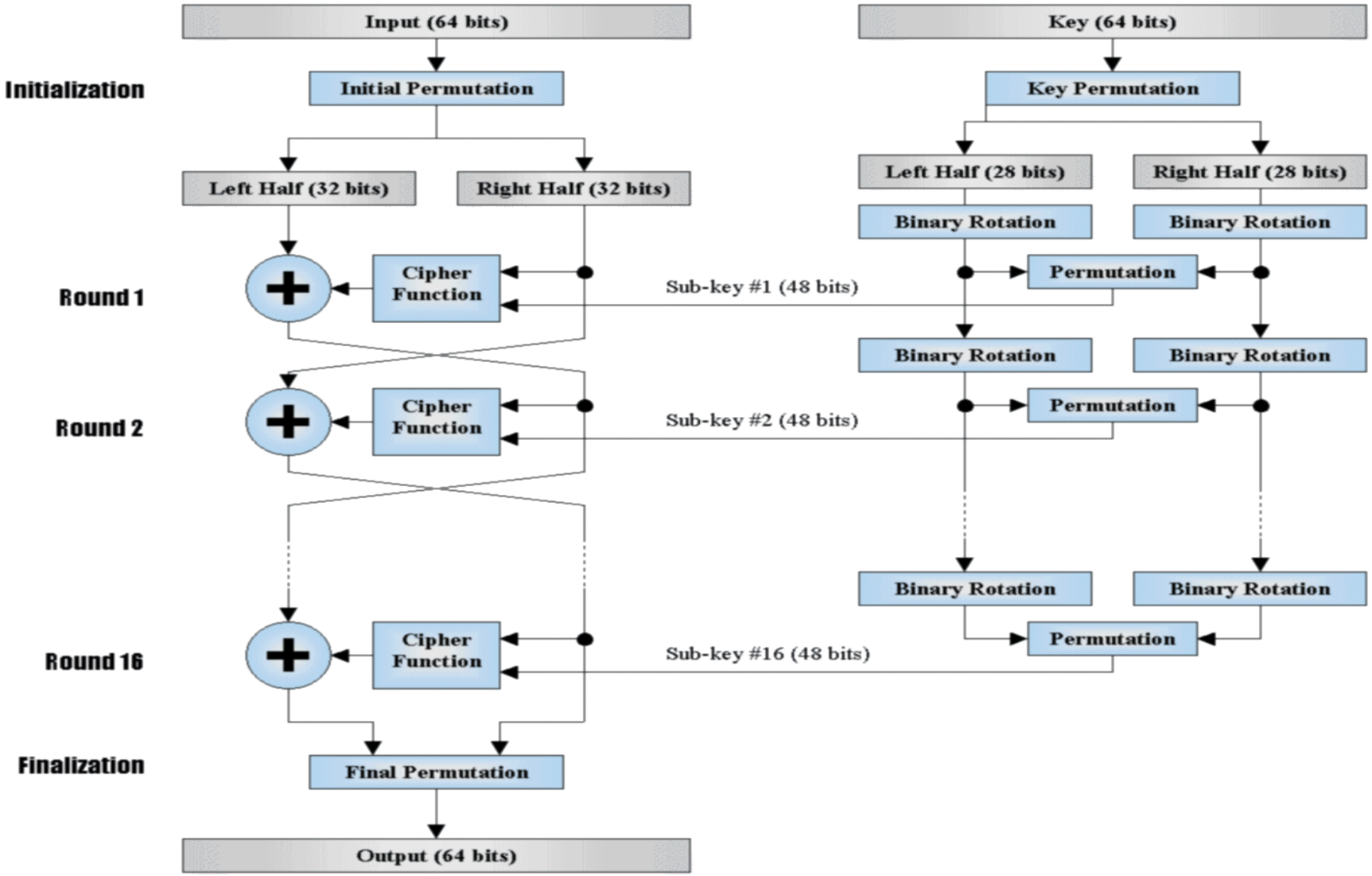
Xifrat DES

$$IP^{-1}\lambda_{f_{16}}\theta\lambda_{f_{15}}\theta\lambda_{f_{14}}\theta\ldots\theta\lambda_{f_3}\theta\lambda_{f_2}\theta\lambda_{f_1}IP,$$

Desxifrat DES

$$IP^{-1}\lambda_{f_1}\theta\lambda_{f_2}\theta\lambda_{f_3}\theta\ldots\theta\lambda_{f_{14}}\theta\lambda_{f_{15}}\theta\lambda_{f_{16}}IP.$$

DES: Descripció de l'algoritme



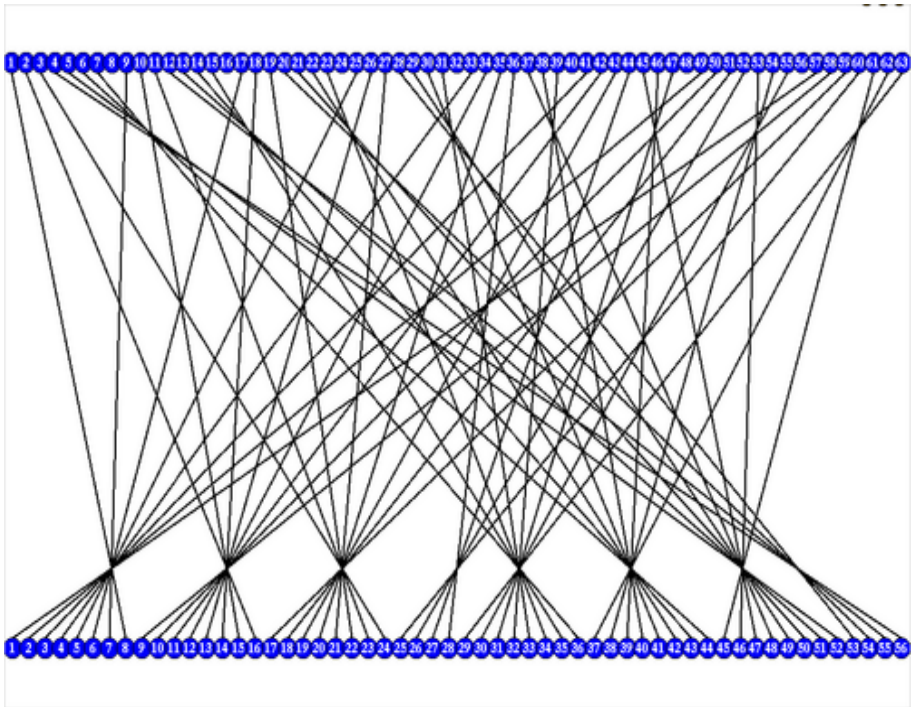
▸ Funció *f*

DES: Generació de subclaus

1. A la clau K de 56 bits (un cop suprimits els bits 8,16,24,. . . ,64, que són bits de paritat), se li aplica

Permutació P_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



DES: Generació de subclaus

2. S'escriu $P_1(K) \equiv C_0 D_0$ (blocs de 28 bits) i per a $1 \leq i \leq 16$

$$\begin{aligned} C_i &= LS_i(C_{i-1}) \\ D_i &= LS_i(D_{i-1}) \end{aligned}$$

LS_i és una rotació a l'esquerra d'una posició si $i = 1, 2, 9, 16$ i de dues posiciones per a qualsevol altre valor de i

Subclau de la volta $i-$èsima

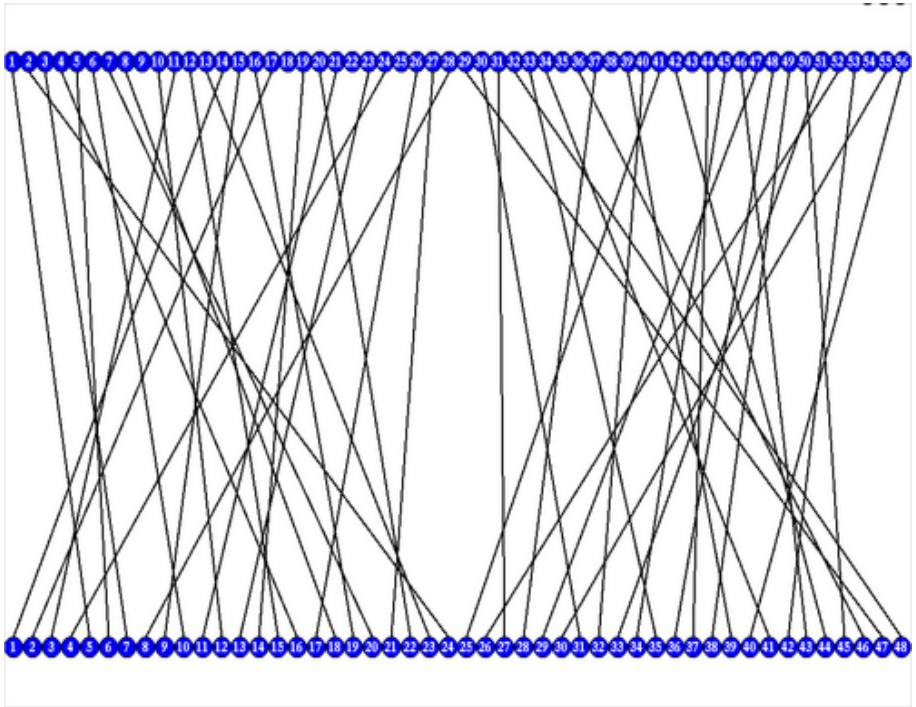
$$k_i = P_2(C_i D_i)$$

P_2 és una permutació de compressió: dels 56 bits es trien 48

DES: Generació de subclaus

P_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



P_2 no utilitza els bits de les posicions 9,18,22,25,35,38,43,54

$k_1, k_2, \ldots, k_{16}$ subclaus de 48 bits cadascuna

▸ DES

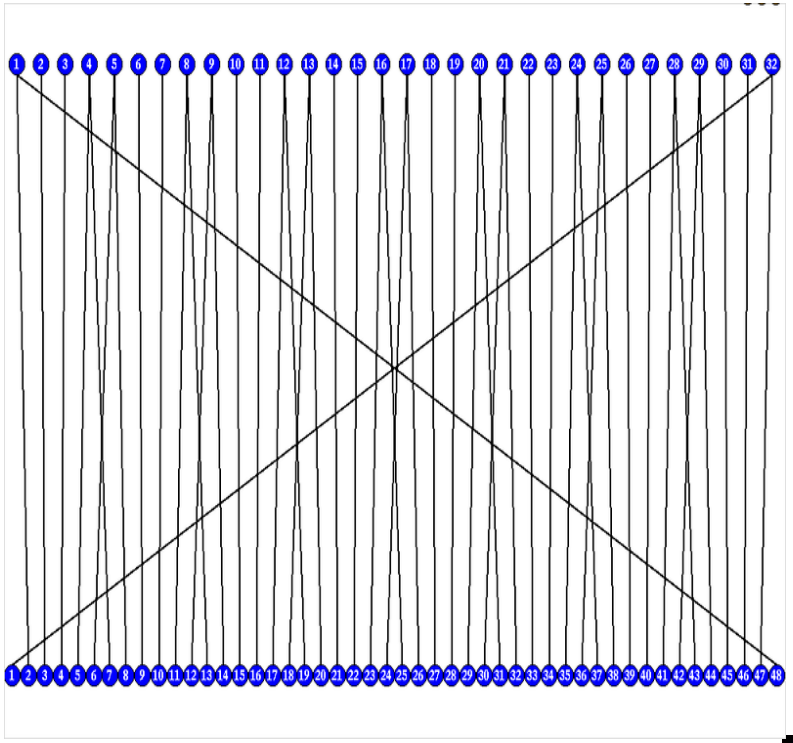
DES: La funció f

Depèn de dos paràmetres: un bloc x de 32 bits i una subclau k de 48 bits. Retorna un bloc de 32 bits

1. x se expandeix a 48 bits

Permutació d'expansió 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

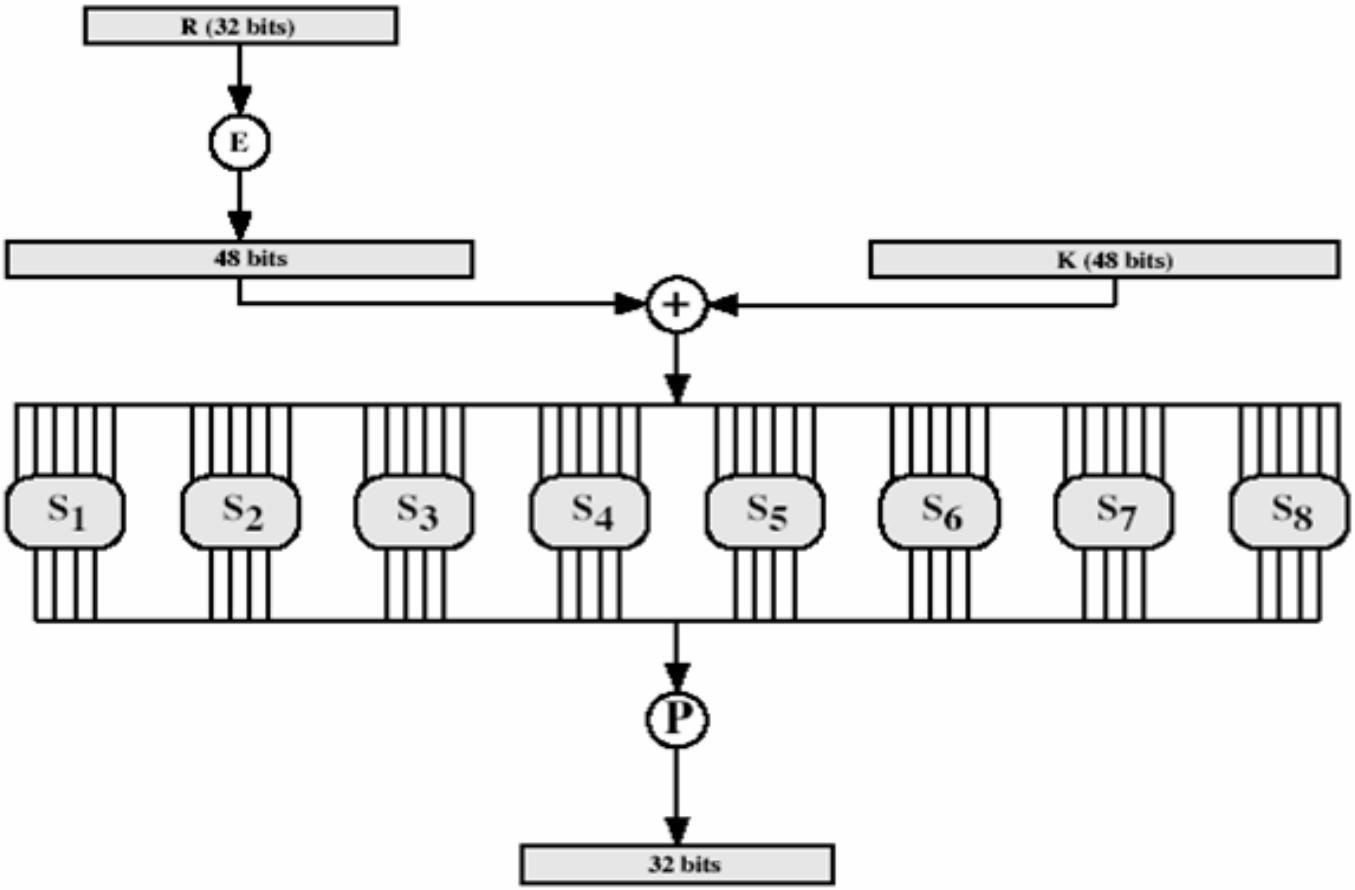


DES: La funció f

2. $B = E(x) \oplus k \equiv B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8$ (de 6 bits cadascun)
3. $C_i = S_i(B_i)$. A les caixes S_i (S-boxes) entren 6 bits i en surten 4
4. $C \equiv C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8$ és un bloc de 32 bits
5. $f(x, k) = P(C)$, on P és la permutació

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: La funció *f*



DES: S-boxes (S_1)

							0110					1010				
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$$B_1 = \mathbf{101101} \qquad S_1(B_1) = 1 = 0001$$

$$\tilde{B}_1 = 110100 \qquad S_1(\tilde{B}_1) = 9 = 1001$$

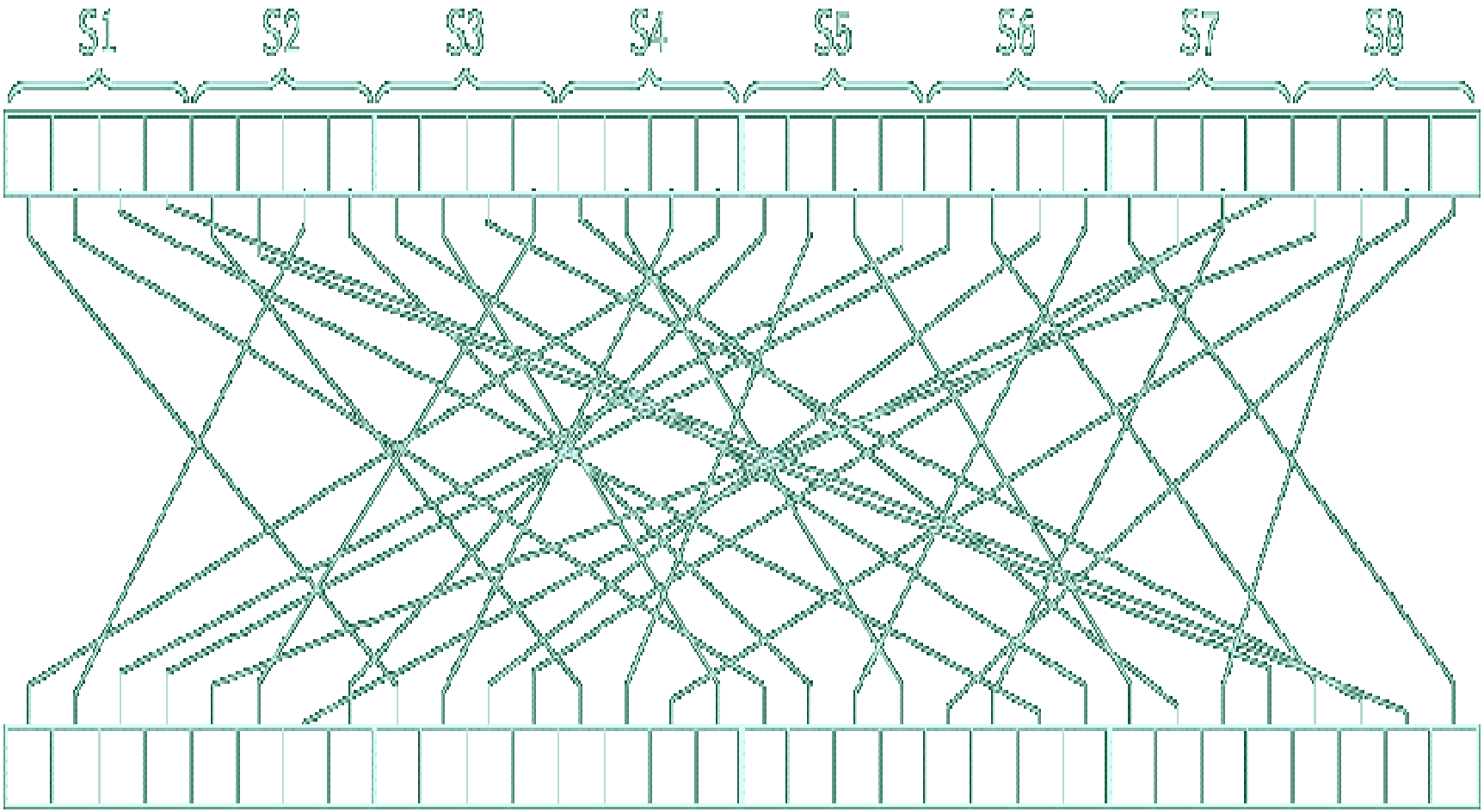
DES: S-boxes

- Cada fila és una permutació dels enters 0,..,15

$$\binom{16!}{4} = 79848568271286346497780546492797988146627337185280000$$

- Cap S-box és una funció lineal o afí de les entrades
- Un canvi d'un bit en l'entrada de una S-box modifica com a mínim dos bits de la sortida
- Per a qualsevol S-box, si fixem un dels sis bits d'entrada i ens mirem un bit determinat de la sortida, el número d'entrades que donen lloc a un 0 és aproximadament igual al número d'entrades que donen lloc a un 1

DES: Permutació P



DES: Permutació P

$$32! = 263130836933693530167218012160000000$$

- Els quatre bits de sortida d'una S-box a la volta i són distribuits de manera que dos afectin a bits intermedis de S-boxes en la volta següent i els altres dos afectin a bits dels extrems
- Els quatre bits de sortida de una S-box afecten a sis S-boxes diferents. A més, no hi ha dos que afectin a la mateixa S-box
- Si un bit d'una S-box afecta a un bit intermedi d'una altra S-box, llavors un bit de la segona S-box no pot afectar a un bit intermedi de la primera S-box

DES: Seguretat

- Tamany de la clau: massa petit
- No es coneix cap tècnica de criptoanàlisi per atacar-lo més eficient que la cerca exhaustiva
- El DES no té estructura de grup. Es pot augmentar la seguretat mitjançant aplicacions sucessives del DES amb diferents claus.

Triple DES

$$C = E_{k_1} D_{k_2} E_{k_1}(M)$$

Dobla la longitud efectiva de la clau (112 bits) al preu de triplicar el nombre d'operacions de xifratge

Crypt(3): xifratge de passwords en unix

8 caràcters de password = clau DES condimentat amb sal (12 bits)
Iniciant amb un bloc de 64 zeros, 25 iteracions de l'algoritme