

Алгоритм DES



Історична довідка

- 1974 рік – NIST оголошує конкурс симетричних криптоалгоритмів на стандарт шифрування США;
- 1976 рік – поданий на конкурс алгоритм Lucifer (розробка IBM, Хорст Фейтель) оголошено переможцем;
- 1977 рік – модифікований алгоритм Lucifer прийнято на озброєння як стандарт шифрування США DES (Data Encryption Standard – стандарт шифрування даних)

Порівняння DES-Lucifer

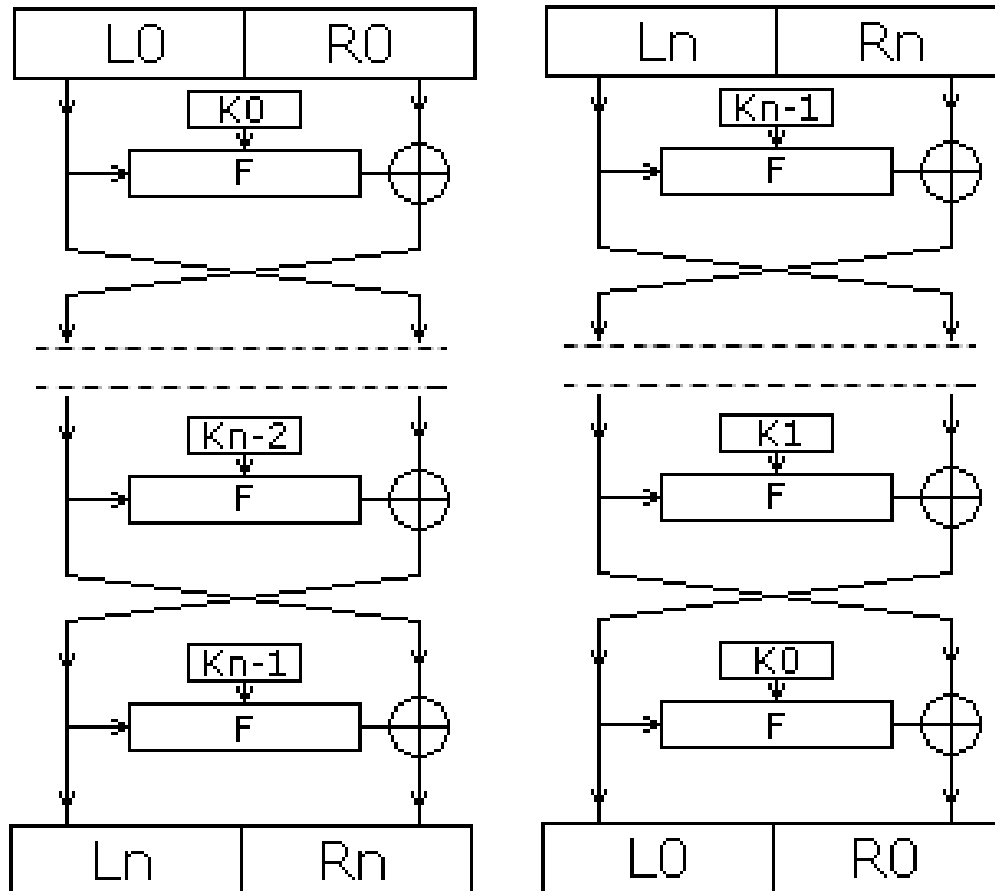
No	Параметр	Lucifer	DES
1.	Архітектура	Мережа Фейстеля	Мережа Фейстеля
2.	Довжина вхідного блоку	128 бітів	64 біти
3.	Довжина ключа	128 бітів	56+8 бітів
4.	Кількість раундів обробки	16	16

Зміни, які внесло АНБ до алгоритму Lucifer:

- Зменшено довжини блоку та ключа;
- Ключ: 56 секретних бітів + 8 бітів парності (кількість одиниць в кожному байті має бути непарною);
- Змінено принципи формування блоків заміни (і засекречено їх!).

Блоки заміни розсекречено лише в 90-х роках.

Мережа Фейстеля



Мережа Фейстеля:
Ліворуч – процес
зашифрування;
Праворуч – процес
розшифрування.

Математично:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \text{ XOR } F(R_{i-1}, K_i).$$

Тоді розшифрування:

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \text{ XOR } F(L_i, K_i).$$

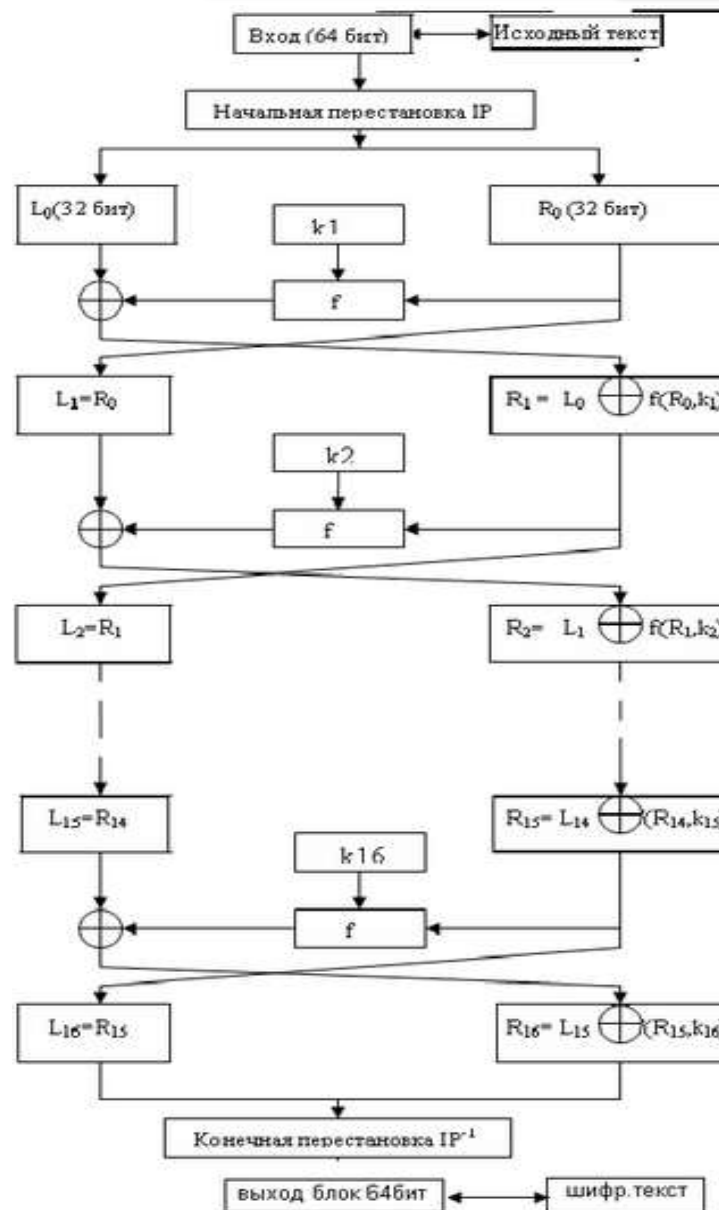
Переваги і недоліки

- Переваги:
 - Висока швидкодія;
 - Можливість використовувати однакові модулі (процедури) при зашифруванні та розшифруванні.
 - Не треба обчислювати обернену функцію, отже єдина вимога – раундова функція має бути незворотною.
- Недоліки:
 - За раунд шифрується лиш половина блоку.

Архітектура DES

Основні параметри алгоритму:

1. Вхідний блок – 64 біти;
2. Ключ – $56 + 8 = 64$ біти;
3. Кількість раундів – 16.
4. Початкова і кінцева перестановки IP та IP^{-1} працюють з усім блоком.
5. Раундова функція – незворотне перетворення з перестановок і замін та підмішування ключа.



Початкова і кінцева перестановки

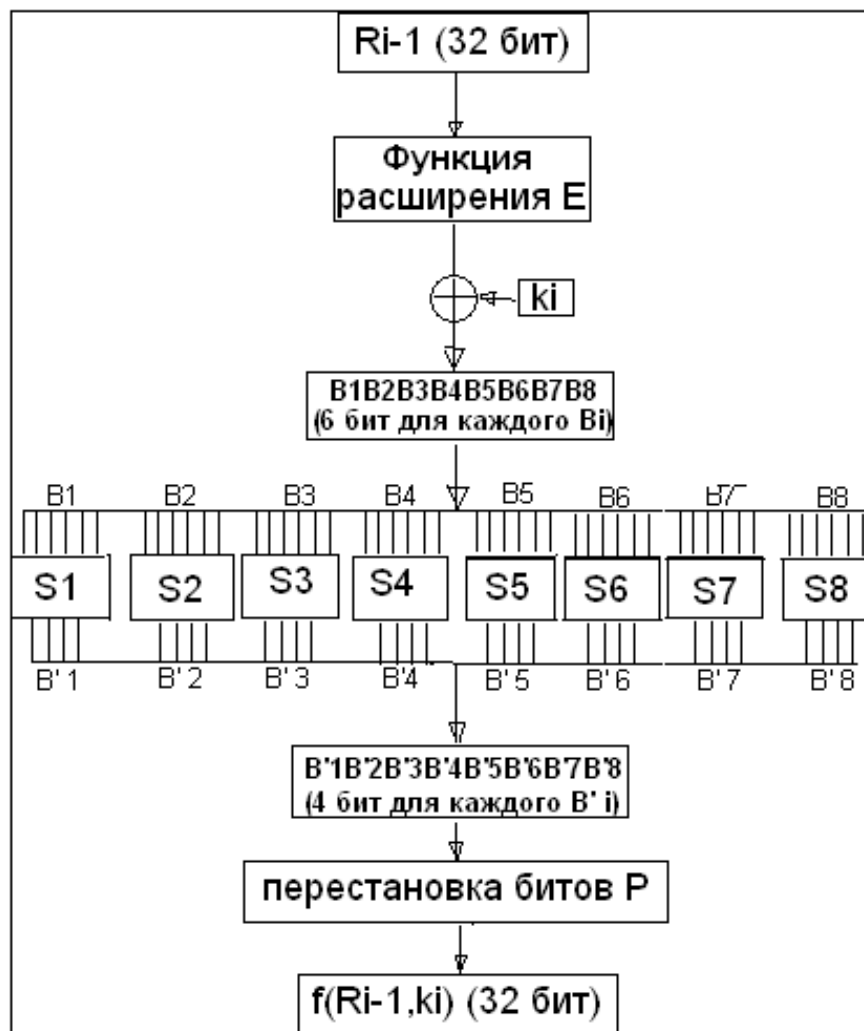
Початкова перестановка IP

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	

Кінцева перестановка 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

Структура одного раунда DES



Перестановка з розширенням

0	1	2	3
4	5	6	7
8	4	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31

Вхід – 32 біти; Вихід – 48 бітів

Результат перестановки додається за правилами XOR до 48-бітового раундового підключа

Використання блоків заміни



Приклад:

Нехай перший блок B_1 має вигляд: 110110.

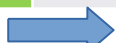
Його буде спрямовано на перший S-бокс S_1 .

Перший та останній біти (1 та 0 – $10 = 2_{10}$) дають двійкове подання другого рядка таблиці.

Внутрішні 4 біти ($1011 = 11_{10}$) дають номер стовпчика таблиці заміни.

Використання блоків заміни

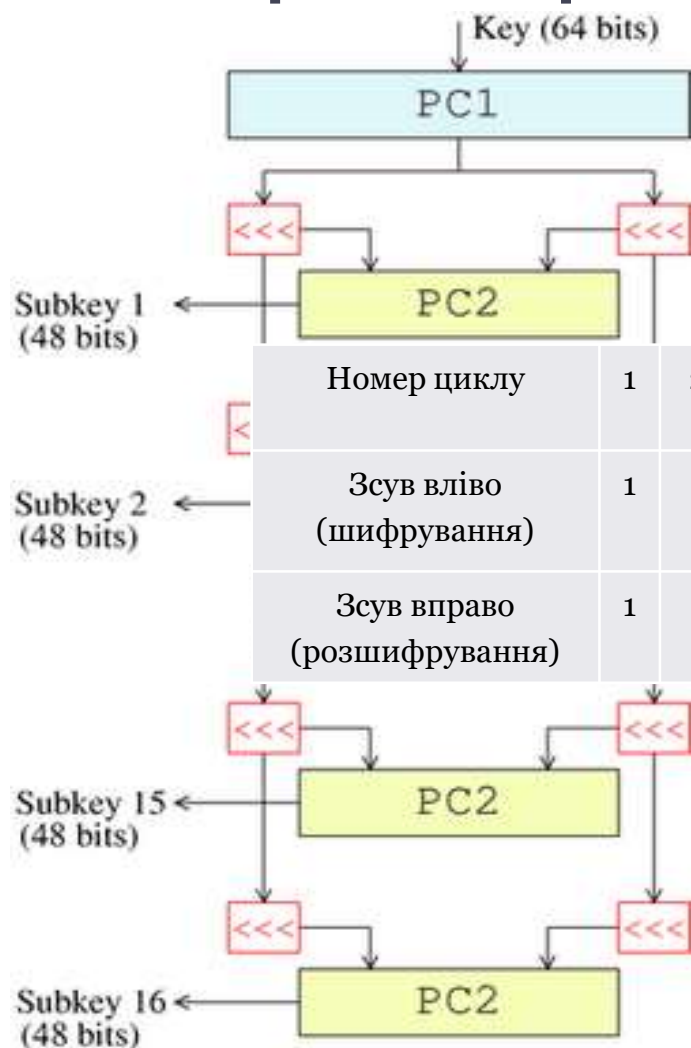
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Результат заміни: вхідний блок: 110110  $7_{10} = 0111$

Результат заміни піддається перестановці (P-перестановка):

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

Операція розгортання ключа



Блок C ₀							Блок D ₀						
57	49	41	33	25	17	9	63	55	47	39	31	23	15
1	58	50	42	34	26	18	7	62	54	46	38	30	22
10	2	59	51	43	35	27	14	6	61	53	45	37	29
3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	2	2	2	2	1	2	2	2	2	2	2	1
2	2	2	2	2	2	1	2	2	2	2	2	2	1
			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			

Слабкі ключі DES





- Слабкими називаються ключі, які задовольняють рівність: $DES_K(DES_K(M))=M$

Слабкі ключі DES (Hex)	C_o	D_o
0101-0101-0101-0101	$[0]^{28}$	$[0]^{28}$
FEFE-FEFE-FEFE-FEFE	$[1]^{28}$	$[1]^{28}$
1F1F-1F1F-0E0E-0E0E	$[0]^{28}$	$[1]^{28}$
E0E0-E0E0-F1F1-F1F1	$[1]^{28}$	$[0]^{28}$

Напівслабкі ключи DES

- Напівслабкими будемо називати такі пари ключів, для яких виконується рівність:

$$DES_{K_1}(DES_{K_2}(M))=M$$

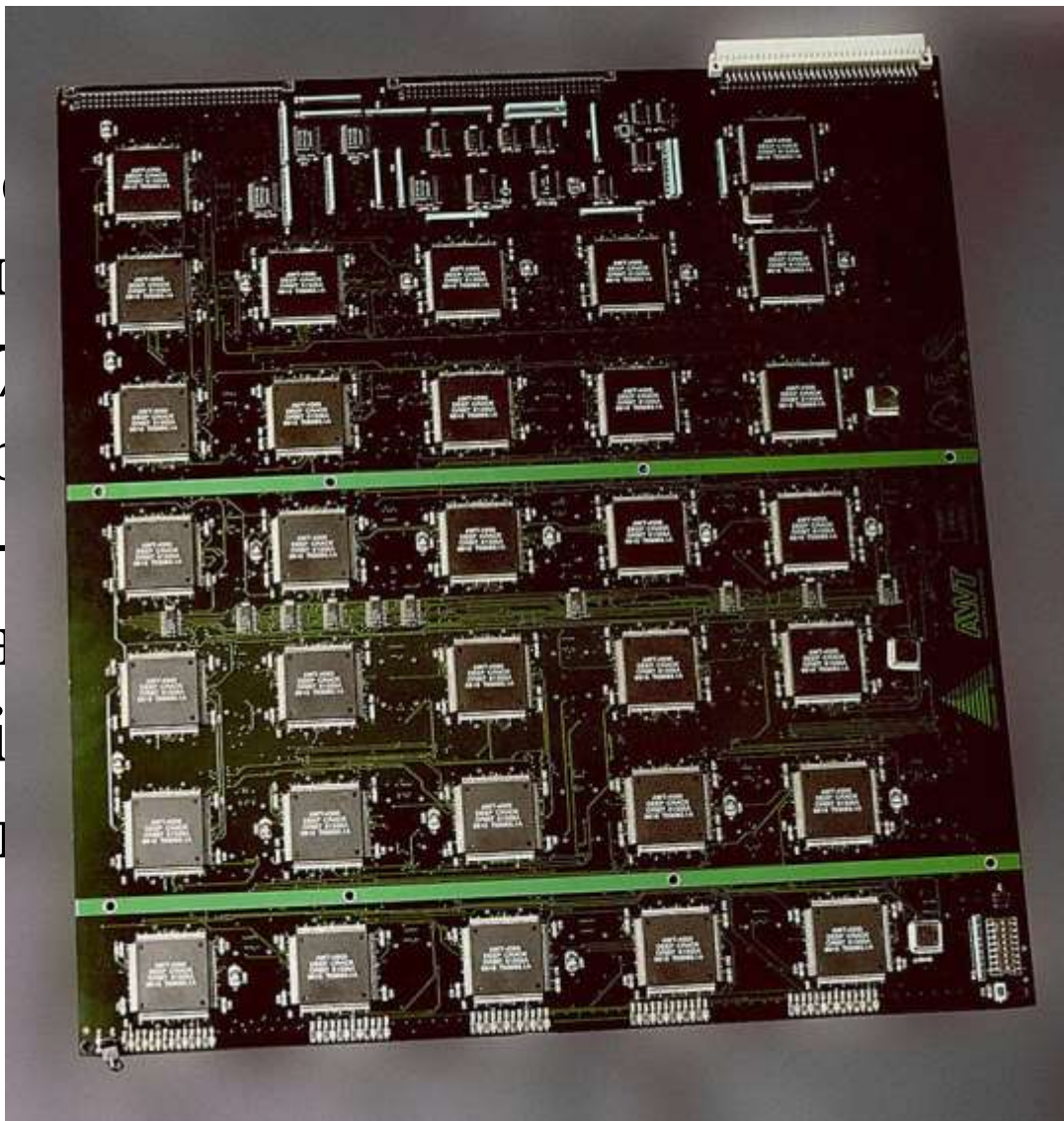
C_o	D_o	Пари напівслабких ключів	C_o	D_o
$[01]^{14}$	$[01]^{14}$	01FE-01FE-01FE-01FE,  FE01-FE01-FE01-FE01	$[10]^{14}$	$[10]^{14}$
$[01]^{14}$	$[01]^{14}$	1FE0-1FE0-1FE0-1FE0,  E0F1-E0F1-E0F1-E0F1	$[10]^{14}$	$[10]^{14}$
$[01]^{14}$	$[0]^{28}$	01E0-01E0-01F1-01F1,  E001-E001-F101-F101	$[10]^{14}$	$[0]^{28}$
$[01]^{14}$	$[1]^{28}$	1FFE-1FFE-0EFE-0EFE,  FE1F-FE1F-FE0E-FE0E	$[0]^{28}$	$[1]^{28}$
$[0]^{28}$	$[01]^{14}$	011F-011F-010E-010E,  1F01-1F01-0E01-0E01	$[0]^{28}$	$[10]^{14}$
$[1]^{28}$	$[01]^{14}$	E0FE-E0FE-F1FE-F1FE,  FEE0-FEE0-FEF1-FEF1	$[1]^{28}$	$[10]^{14}$

Криптостійкість DES

Метод атаки	Відомі відкр. тексти	Обрані відкр. тексти	Об'єм пам'яті	Кількість операцій
Грубою силою	1	-	Незначний	2^{55}
Лінійний КА	2^{43}	-	Для тексту	2^{43}
Дифер. КА	-	2^{47}	Для тексту	2^{47}
Дифер. КА	2^{55}	-	Для тексту	2^{55}

Атаки на DES

- 1997 рік – RSA Security (вартість ~10 тис. доларів) – перша атака на DES грубої сили за ~7 років
- 1997 рік – Distributed.net «грубої силою» на DES – перша атака на DES грубої сили за ~7 років
- 1998 рік – 41 день
- 1999 рік – 2 дні і
- 1999 рік – 22 год



Переваги і недоліки DES

- Переваги:

- Висока швидкодія;
- Можливість використання одних апаратних або програмних модулів для зашифрування і розшифрування.
- =====

- Недоліки:

- Мала довжина ключа;
- За один раунд шифрується лиш половина блоку;
- Наявність слабких ключів;
- Застаріла архітектура.