НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
Факультет прикладної математики
Кафедра прикладної математики

Звіт
з лабораторної роботи № 3
із дисципліни «Криптографічні методи захисту інформації»
на тему
Стандарт шифрування DES

Виконав:
студентка групи КМ-93
Довгаль Є. О.

Керівник:
ст. викладач Бай Ю. П.

Київ — 2020

ЗМІСТ

Мета роботи: розробити криптосистему на основі стандарту шифрування DES.

Постановка задачі

1. Скласти програму для шифрування та розшифрування за алгоритмом DES 64-бітного блоку інформації, використовуючи 64-бітний ключ. Перевірити роботу програми на контрольних прикладах. Навести скріншоти детального покрокового виконання алгоритму.

1.*а*. Контрольний приклад 1

plaintext = 01 23 45 67 89 AB CD EF (hex)

key = 13 34 57 79 9B BC DF F1 (hex)

ciphertext = 85 E8 13 54 0F 0A B4 05 (hex)

1.*б*. Контрольний приклад 2

plaintext = 01 23 45 67 89 AB CD EF (hex)

key = FE DC BA 98 76 54 32 10 (hex)

ciphertext = ED 39 D9 50 FA 74 BC C4 (hex)

2. Розширити функціональність програми для випадку відкритого тексту довільної довжини та 64-бітного ключа.

3. За стандартом DES зашифрувати текст довжиною від 20 до 80 символів, користуючись 64-бітним ключем. Навести ключ та зашифроване повідомлення в Таблиці в своєму рядку. **Зауваження:** *key* та *ciphertext* надавати у вигляді repr() або hex.

4. Дано зашифроване за стандартом DES повідомлення довжиною від 20 до 80 символів та відомий 64-бітний ключ (див. Таблицю, рядок над своїм). Розшифрувати задане повідомлення. Результат записати в Таблицю, в рядок над своїм.

Основні теоретичні відомості зі стандарту шифрування DES

DES (англ. **Data Encryption Standard**) — це симетричний алгоритм шифрування певних даних , стандарт шифрування прийнятий урядом США із 1976 до кінця 1990-х, з часом набув міжнародного застосування. Ще з часу свого розроблення алгоритм викликав неоднозначні відгуки. Оскільки DES містив засекречені елементи своєї структури, породжувались побоювання щодо можливості контролю з боку Національного Агентства Безпеки США (англ. National Security Agency). Алгоритм піддавався критиці за малу довжину ключа, що, врешті, після бурхливих обговорень та контролю академічної громадськості, не завадило йому стати загальноприйнятим стандартом. DES дав поштовх сучасним уявленням про блочні алгоритми шифрування та криптоаналіз.

Зараз DES вважається ненадійним в основному через малу довжину ключа (56 біт) та розмір блоку (64 біти). У 1999 ключ DES було публічно дешифровано за 22 години 15 хвилин. Вважається, що алгоритм достатньо надійний для застосування у модифікації 3-DES, хоча існують розроблені теоретичні атаки. DES поступово витісняється алгоритмом AES, що з 2002 року є стандартом США.

Опис алгоритму

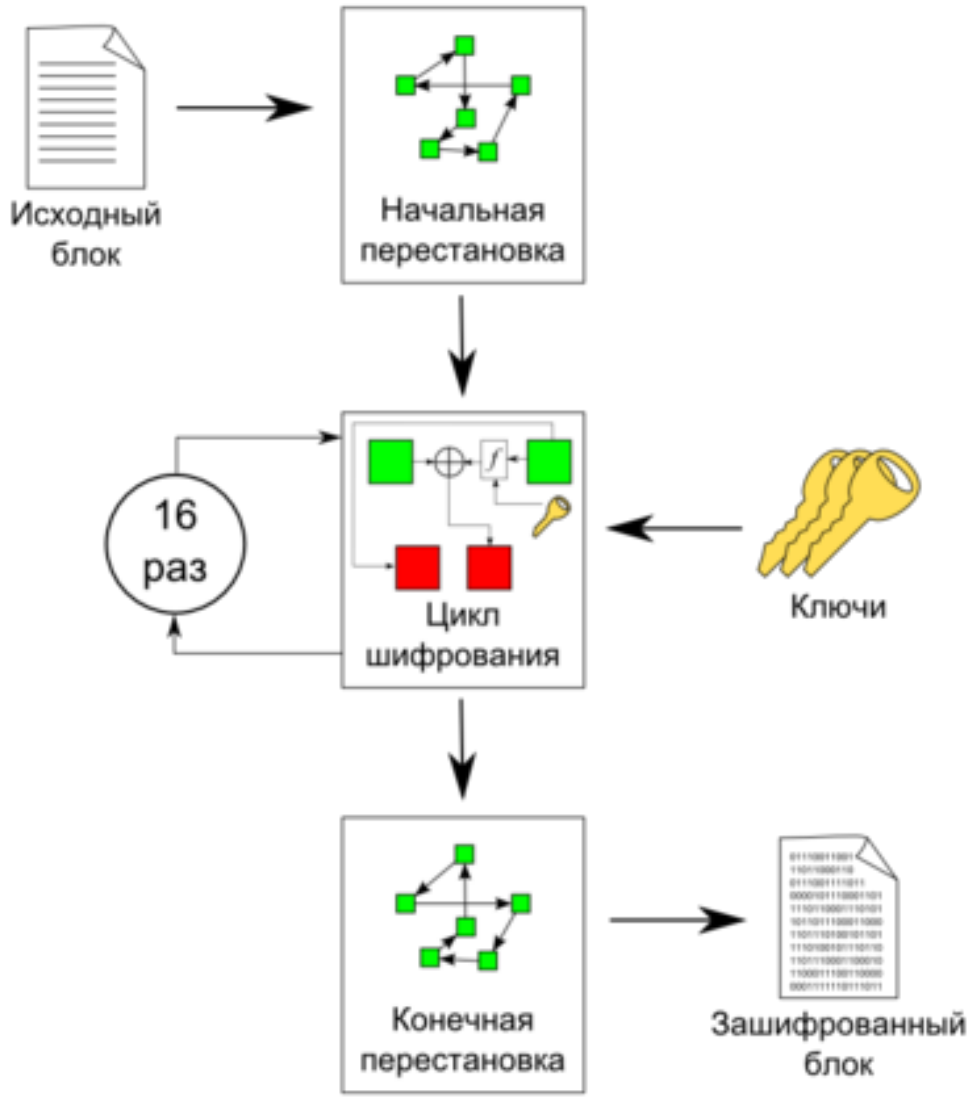
DES є блочним шифром - дані шифруються блоками по 64 біти - 64 бітний блок явного тексту подається на вхід алгоритму, а 64-бітний блок шифрограми отримується в результаті роботи алгоритму. Крім того, як під час шифрування, так і під час дешифрування використовується один і той самий алгоритм (за винятком дещо іншого шляху утворення робочих ключів).

Ключ має довжину 56 біт (як правило, в джерельному вигляді ключ має довжину 64 біти, де кожний 8-й біт є бітом паритету, крім того, ці контрольні біти можуть бути винесені в останній байт ключа). Ключем може бути довільна 64-бітна комбінація, яка може бути змінена у будь-який момент часу. Частина

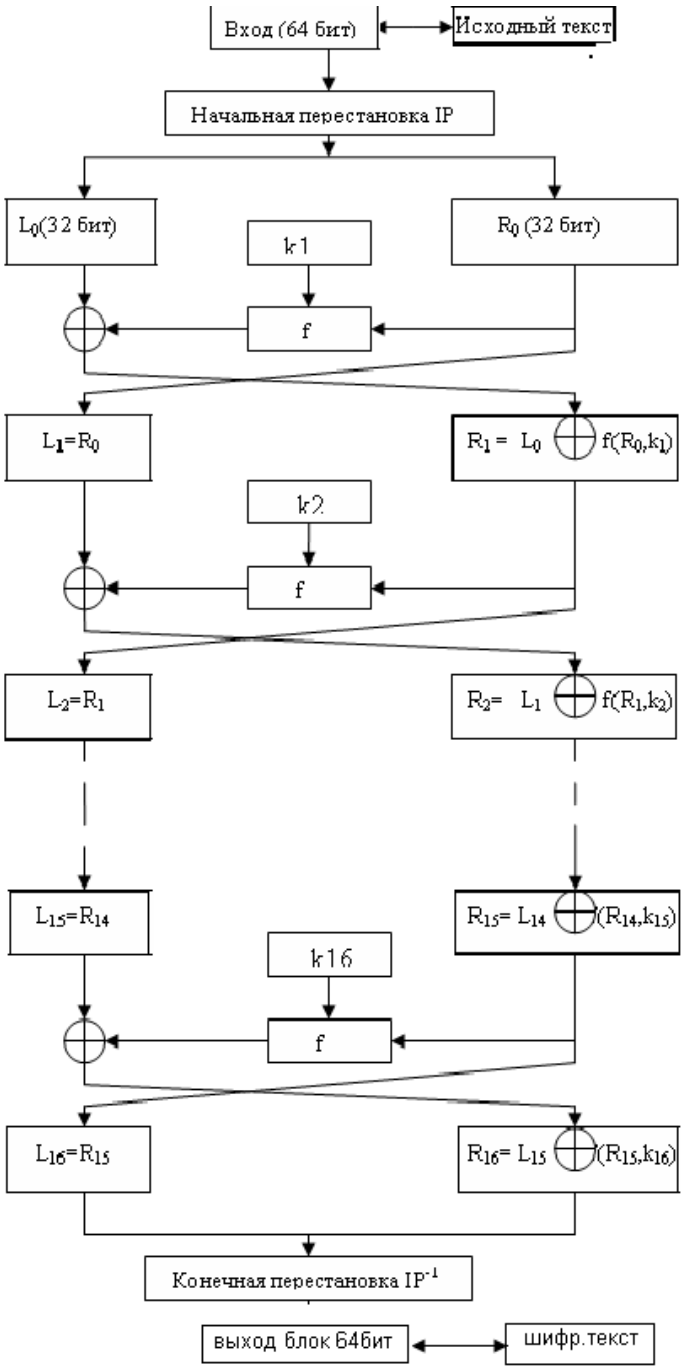
цих комбінацій вважається слабкими ключами, оскільки може бути легко визначена. Безпечність алгоритму базується на безпечності ключа.

На найнижчому рівні алгоритм є ніщо інше, ніж поєднання двох базовних технік шифрування: перемішування і підстановки. Цикл алгоритму, з яких і складається DES є комбінацією цих технік, коли як об'єкти перемішування виступають біти тексту, ключа і блоків підстановок.

Схема:



Розглянемо детальніше:



Details

- IP is initial permutation
- L is left-half of message
- R is right half of message
- $\oplus$ is XOR
- K_i are keys
- f is a function (next slide)
- IP^{-1} is an inverse permutation

Контрольний приклад 1

(M) *plaintext* = 01 23 45 67 89 AB CD EF $_{16}$
$1001000110100010101100111100010011010101111001101111011111_{2}$

(K) *key* = 13 34 57 79 9B BC DF F1 $_{16}$
$1001100110100010101110111100110011011011110011011111111110001_{2}$

(C) *ciphertext* = 85 E8 13 54 0F 0A B4 05 $_{16}$
$1000010111101000000100110101010000001111000010101011010000000101_{2}$

7: Прибираємо кожний 8 біт заданого ключа

The keys

- Keys are 64-bit numbers
  - Every 8th bit is unused
    - Used for parity

KEY: 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001
→ 0001001 0011010 0101011 0111100 1001101 1011110 1101111 1111000

9: Перестановка бітів по заданій таблиці перестановки. 3 приклади наведено.

Step 1a: Permute the key

- Permutation table

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 key
00010011 00110100 01010111 01111001
10011011 10111100 11011111 11110001

56-bit permutation
1111000 0110011 0010101 0101111
0101010 1011001 1001111 0001111

- 64-bit key: K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001
- 56-bit permutation: $K+$ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

10: В C_0 йде перші 4*7 біти, в D_0 останні 4*7 біти

Step1b: Split the permuted key

- Two halves: C_0 and D_0
  - Each is 28 bits
- Example:

$K+$ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

C_0 = 1111000 0110011 0010101 0101111

D_0 = 0101010 1011001 1001111 0001111

11: На кожному раунді робиться циклічний здвиг цих ключей. Ступінь здвигу всюди =2, окрім 1, 2, 9 та 16 ітераціях, там =1 (продемонстровано на скріншоті)

Iteration:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
# of shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

- Example: Starting from C_0 and D_0

$C_0 = 11110000110011001010101011111$
$D_0 = 01010101011001100111100011111$

$C_1 = 11100001100110010101010111111$
$D_1 = 10101010110011001111100011110$

$C_2 = 11000011001100101010101111111$
$D_2 = 01010101100110011110001111101$

12: Аналогічні п.9 дії. C_1D_1 з'являється шляхом конкатенації C_1 та D_1 та стає ключем даного раунду

$C_1 = 11100001100110010101010111111$
$D_1 = 10101010110011001111100011110$

1110000 1100110 0101010 1011111
1010101 0110011 0011110 0011111
C_1D_1

Step 1d: Generate final subkeys

- Concatenate C_iD_i and permute again
  - Permutation table

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

48 bit key

- Example:

$C_1D_1 = 11100001100110\ 0101010\ 1011111\ 1010101\ 0110011\ 0011110\ 0011111$
$K_1 = 000110\ 110000\ 001011\ 101111\ 111111\ 000111\ 000001\ 110010$

1-5 3-6 4-3 7-6

13: Знову перестановка бітів через IP таблицю

Step 2a: Initial data permutation

- The permutation table

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

- Example

M = 00000001 00100011 01000101 01100111 10001001 10101011 11001101 11101111

$= 0123456789ABCDEF_{16}$

IP = 11001100 00000000 11001100 11111111 11110000 10101010 11110000 10101010

14: Розділяємо отримані байти на дві частини: перші 4 вважається Лівим (L_i) блоком, інші 4 вважаються Правим (R_i) блоком.

- Split the IP into halves
  - 32-bit left half
  - 32-bit right half

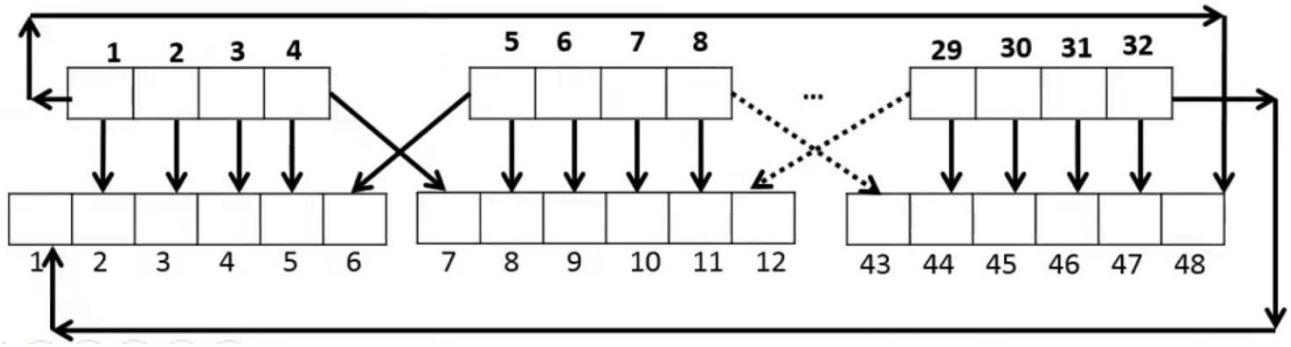
- Example:

IP = 11001100 00000000 11001100 11111111 11110000 10101010 11110000 10101010

L_0 = 11001100 00000000 11001100 11111111

R_0 = 11110000 10101010 11110000 10101010

15: Тільки-но отримана Права частина стає Лівою для наступного раунду. Далі починається обробка. Спочатку розширяємо R з 32 до 48 бітів (тобто до 5 байтів). Це робиться такою схемою:



- Expand R_i from 32 to 48 bits
  - Lookup 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

- Example

R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

Далі робимо XOR з ключем

16: XOR з ключем

- Example

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

$K_1 \oplus E(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111

19: Розбиваємо отримане на 8 блоків по 6 бітів. Кожен блок обробляємо через таблицю S_i блоків

שורה	מס' עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	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	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
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
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
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	S_5															
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	S_6															
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	S_7															
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Приклад для B_1 (S_1):

- $K_1 \oplus E(R_0) =$ 011000 010001 011110 111010 100001 100110 010100 100111
  - Row address is 00
  - Column address is 1100 = 12
  - $S_1(B_1) =$ 5 = 0101
- Example: **S(B)** = 0101 1100 1000 0010 1011 0101 1001 0111

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

S_1

19

20: Знову перестановка через таблицю перестановки, схема така ж

- $f = P(S_1(B_1)S_2(B_2)\ldots S_8(B_8))$
  - The permutation table

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

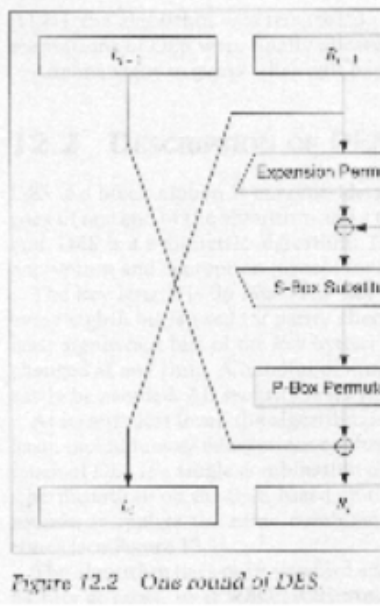


Figure 12.2 One round of DES

- Example:
  - **S(B)** = 0101 1100 1000 0010 1011 0101 1001 0111
  - $f(R_0, K_1) =$ 0010 0011 0100 1010 1010 1001 1011 0011

21: XOR, тут нема що такого пояснювати, усе очевидно

L_0: 1100 1100 0000 0000 1100 1100 1111 1111
f: $\oplus$ 0010 0011 0100 1010 1010 1001 1011 1011
R_1: 1110 1111 0100 1010 0110 0101 0100 0100

22: Обчислюються усі останні блоки. R_1 стає L_2. R_2 отримаємо таким шляхом:

L_1: 1111 0000 1010 1010 1111 0000 1010 1010
R_1: 1110 1111 0100 1010 0110 0101 0100 0100
Key$_2$: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R_2 expanded to 48bits:
0111 0101 1110 1010 0101 0100 0011 0000 1010 1010 0000 1001

R_2 XOR with Key$_2$:
0111 0101 1110 1010 0101 0100 0011 0000 1010 1010 0000 1001 ***Last R_2***
0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101 ***Key$_2$***
0000 1100 0100 0100 1000 1101 1110 1011 0110 0011 1110 1100 ***XOR result***

R_2 apply SBOXes: 1111 1000 1101 0000 0011 1010 1010 1110

R_2 in IP table: 0011 1100 1010 1011 1000 0111 1010 0011

R_2 XOR with L_1: 1100 1100 0000 0001 0111 0111 0000 1001

L_2: 1110 1111 0100 1010 0110 0101 0100 0100 ***(бывший R_1)***
R_2: 1100 1100 0000 0001 0111 0111 0000 1001

…і так далі аналогічно до 16 раунда…

23: Фінальне перетворення:

L_{16}: 0100 0011 0100 0010 0011 0010 0011 0100
R_{16}: 0000 1010 0100 1100 1101 1001 1001 0101

$R_{16}L_{16}$: 00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100

Do Final Permutation (тобто прогоняємо через IP):

C_2: 10000101 11101000 00010011 01010100 00001111 00001010 10110100 00000101
C_{16}: 85E813540F0AB405

Контрольний приклад 2

plaintext = 01 23 45 67 89 AB CD EF $_{16}$

key = FE DC BA 98 76 54 32 10 $_{16}$

ciphertext = ED 39 D9 50 FA 74 BC C4 $_{16}$

Процес шифрування:

```
Block: 11001100 00000000 11001100 11111111 11110000 10101010 11110000 10101010
L0: 1100 1100 0000 0000 1100 1100 1111 1111
R0: 1111 0000 1010 1010 1111 0000 1010 1010
///ROUND 1///
Key1: 1111 0100 1111 1101 1001 1000 0110 0100 1011 0110 0101 1010
R1 expanded to 48bits: 0111 1010 0001 0101 0101 0101 0111 1010 0001 0101 0101 0101
R1 XOR with Key1: 1000 1110 1110 1000 1100 1101 0001 1110 1010 0011 0000 1111
R1 apply SBOXes: 1100 0001 1010 0000 1100 1000 1000 0100
R1 in IP table: 0001 0001 1000 0100 1100 0001 0010 0101
R1 XOR with L0: 1101 1101 1000 0100 0000 1101 1101 1010
L1: 1111 0000 1010 1010 1111 0000 1010 1010
R1: 1101 1101 1000 0100 0000 1101 1101 1010
///ROUND 2///
Key2: 1001 0110 0101 1001 1010 0110 1101 1010 1001 0101 1101 1001
R2 expanded to 48bits: 0110 1111 1011 1100 0000 1000 0000 0101 1011 1110 1111 0101
R2 XOR with Key2: 1111 1001 1110 0101 1010 1110 1101 1111 0010 1011 0010 1100
R2 apply SBOXes: 0000 1010 0111 1101 1001 0000 0111 1110
R2 in IP table: 1110 1111 0001 1011 0001 0100 0110 0100
R2 XOR with L1: 0001 1111 1011 0001 1110 0100 1100 1110
L2: 1101 1101 1000 0100 0000 1101 1101 1010
R2: 0001 1111 1011 0001 1110 0100 1100 1110
///ROUND 3///
Key3: 1011 1010 0010 1011 0111 0101 0100 1011 1101 0111 0010 1101
R3 expanded to 48bits: 0000 1111 1111 1101 1010 0011 1111 0000 1001 0110 0101 1100
R3 XOR with Key3: 1011 0101 1101 0110 1101 0110 1011 1011 0100 0001 0111 0001
R3 apply SBOXes: 0001 1011 1011 0101 1000 0100 1011 1111
R3 in IP table: 1100 1111 0000 1010 0101 1101 0010 1111
R3 XOR with L2: 0001 0010 1000 1110 0101 0000 1111 0101
L3: 0001 1111 1011 0001 1110 0100 1100 1110
R3: 0001 0010 1000 1110 0101 0000 1111 0101
///ROUND 4///
Key4: 1000 1101 0111 0110 0010 1101 0101 1010 0111 1101 1010 1000
R4 expanded to 48bits: 1000 1010 0101 0100 0101 1100 0010 1010 0001 0111 1010 1010
R4 XOR with Key4: 0000 0111 0010 0010 0111 0001 0111 0000 0110 1010 0000 0010
R4 apply SBOXes: 0000 1000 0011 1001 1110 1111 1100 0010
R4 in IP table: 1001 0101 0011 1110 0010 0000 1100 1101
R4 XOR with L3: 1000 1010 1000 1111 1100 0100 0000 0011
```

L4: 0001 0010 1000 1110 0101 0000 1111 0101
R4: 1000 1010 1000 1111 1100 0100 0000 0011
///ROUND 5///
Key5: 1100 0011 0001 0111 1111 1100 1110 1000 0101 1001 0011 1101
R5 expanded to 48bits: 1100 0101 0101 0100 0101 1111 1110 0000 1000 0000 0000 0111
R5 XOR with Key5: 0000 0110 0100 0011 1010 0011 0000 1000 1101 1001 0011 1010
R5 apply SBOXes: 0000 0111 0101 1111 1100 1001 1011 0011
R5 in IP table: 1101 0111 0100 0111 0111 1100 0101 0001
R5 XOR with L4: 1100 0101 1100 1001 0010 1100 1010 0100
L5: 1000 1010 1000 1111 1100 0100 0000 0011
R5: 1100 0101 1100 1001 0010 1100 1010 0100
///ROUND 6///
Key6: 1101 1100 1101 1010 1110 0001 1100 0011 0111 1010 1011 1010
R6 expanded to 48bits: 0110 0000 1011 1110 0101 0010 1001 0101 1001 0101 0000 1001
R6 XOR with Key6: 1011 1100 0110 0100 1011 0011 0101 0110 1110 1111 1011 0011
R6 apply SBOXes: 0111 1110 1101 0100 1111 0011 0010 1100
R6 in IP table: 0110 1101 0010 1101 1011 0111 1011 0010
R6 XOR with L5: 1110 0111 1010 0010 0111 0011 1011 0001
L6: 1100 0101 1100 1001 0010 1100 1010 0100
R6: 1110 0111 1010 0010 0111 0011 1011 0001
///ROUND 7///
Key7: 1001 0011 1111 1011 0110 1010 1111 0101 0001 1011 0011 1001
R7 expanded to 48bits: 1111 0000 1111 1101 0000 0100 0011 1010 0111 1101 1010 0011
R7 XOR with Key7: 0110 0011 0000 0110 0110 1110 1100 1111 0110 0110 1001 1010
R7 apply SBOXes: 0101 0101 1100 1101 1111 1010 1010 0000
R7 in IP table: 1011 0001 0010 0101 1101 0101 1101 0011
R7 XOR with L6: 0111 0100 1110 1100 1111 1001 0111 0111
L7: 1110 0111 1010 0010 0111 0011 1011 0001
R7: 0111 0100 1110 1100 1111 1001 0111 0111
///ROUND 8///
Key8: 1010 1000 0111 0111 1100 0111 1001 0011 0001 1010 0111 1110
R8 expanded to 48bits: 1011 1010 1001 0111 0101 1001 0111 1111 0010 1011 1010 1110
R8 XOR with Key8: 0001 0010 1110 0000 1001 1110 1110 1100 0011 0001 1101 0000
R8 apply SBOXes: 1101 0001 0000 1111 0100 1111 0111 1010
R8 in IP table: 1001 1010 1111 0110 1111 0100 0100 1010
R8 XOR with L7: 0111 1101 0101 0100 1000 0111 1111 1011
L8: 0111 0100 1110 1100 1111 1001 0111 0111
R8: 0111 1101 0101 0100 1000 0111 1111 1011
///ROUND 9///
Key9: 0011 1111 0011 0110 0001 0110 1101 1001 0100 0111 1100 0110
R9 expanded to 48bits: 1011 1111 1010 1010 1010 1001 0100 0000 1111 1111 1111 0110
R9 XOR with Key9: 1000 0000 1001 1100 1011 1111 1001 1001 1011 1000 0011 0000
R9 apply SBOXes: 0100 1111 0001 1110 1011 1011 0001 0000
R9 in IP table: 0111 0111 0110 1000 1111 0000 1101 0000
R9 XOR with L8: 0000 0011 1000 0100 0000 1001 1010 0111

L9: 0111 1101 0101 0100 1000 0111 1111 1011
R9: 0000 0011 1000 0100 0000 1001 1010 0111
///ROUND 10///
Key10: 0110 1110 0001 1100 1111 1000 1001 1100 1110 0010 1000 1101
R10 expanded to 48bits: 1000 0000 0111 1100 0000 1000 0000 0101 0011 1101 0000 1110
R10 XOR with Key10: 1110 1110 0110 0000 1111 0000 1001 1001 1101 1111 1000 0011
R10 apply SBOXes: 0000 1011 0111 1111 1011 0011 0010 1111
R10 in IP table: 1110 1101 0110 1011 0111 1100 1110 0100
R10 XOR with L9: 1001 0000 0011 1111 1111 1011 0001 1111
L10: 0000 0011 1000 0100 0000 1001 1010 0111
R10: 1001 0000 0011 1111 1111 1011 0001 1111
///ROUND 11///
Key11: 1101 1110 1110 0000 0111 1100 1111 0010 0111 0110 1100 0101
R11 expanded to 48bits: 1100 1010 0000 0001 1111 1111 1111 1111 0110 1000 1111 1111
R11 XOR with Key11: 0001 0100 1110 0001 1000 0011 0000 1101 0001 1110 0011 1010
R11 apply SBOXes: 0111 0100 1110 1000 1011 0110 0000 0011
R11 in IP table: 0010 0001 0010 0011 1000 1011 1101 1110
R11 XOR with L10: 0010 0010 1010 0111 1000 0010 0111 1001
L11: 1001 0000 0011 1111 1111 1011 0001 1111
R11: 0010 0010 1010 0111 1000 0010 0111 1001
///ROUND 12///
Key12: 1000 1110 1100 1111 0001 1010 1011 1010 1010 0011 1010 1011
R12 expanded to 48bits: 1001 0000 0101 0101 0000 1111 1100 0000 0100 0011 1111 0010
R12 XOR with Key12: 0001 1110 1001 1010 0001 0101 0111 1010 1110 0000 0101 1001
R12 apply SBOXes: 0100 0011 1000 0010 1001 0011 1101 0000
R12 in IP table: 0110 0011 0111 0000 1110 0001 0000 0001
R12 XOR with L11: 1111 0011 0100 1111 0001 1010 0001 1110
L12: 0010 0010 1010 0111 1000 0010 0111 1001
R12: 1111 0011 0100 1111 0001 1010 0001 1110
///ROUND 13///
Key13: 0110 1110 0011 1011 0010 1111 1011 0110 0111 1111 0000 0011
R13 expanded to 48bits: 0111 1010 0110 1010 0101 1110 1000 1111 0100 0000 1111 1101
R13 XOR with Key13: 0001 0100 0101 0001 0111 0001 0011 1001 0011 1111 1111 1110
R13 apply SBOXes: 0111 0100 0000 1001 0110 0001 1100 1000
R13 in IP table: 1000 1000 0001 0100 1010 0010 1101 0011
R13 XOR with L12: 1010 1010 1011 0011 0010 0000 1010 1010
L13: 1111 0011 0100 1111 0001 1010 0001 1110
R13: 1010 1010 1011 0011 0010 0000 1010 1010
///ROUND 14///
Key14: 1010 1011 1011 1100 0100 1001 0111 1110 0010 0011 0111 0010

R14 expanded to 48bits: 0101 0101 0101 0101 1010 0110 1001 0000 0001 0101 0101 0101
R14 XOR with Key14: 1111 1110 1110 1001 1110 1111 1110 1110 0011 0110 0010 0111
R14 apply SBOXes: 1101 0001 0000 1000 0100 0011 0101 0111
R14 in IP table: 0000 0010 1011 0110 1110 1000 0110 0010
R14 XOR with L13: 1111 0001 1111 1001 1111 0010 0111 1100
L14: 1010 1010 1011 0011 0010 0000 1010 1010
R14: 1111 0001 1111 1001 1111 0010 0111 1100
///ROUND 15///
Key15: 0100 1001 0110 1110 1111 1010 1111 0101 1110 1001 0100 1010
R15 expanded to 48bits: 0111 1010 0011 1111 1111 0011 1111 1010 0100 0011 1111 1001
R15 XOR with Key15: 0011 0011 0101 0001 0000 1001 0000 1111 1010 1010 1011 0011
R15 apply SBOXes: 1011 0111 1001 0110 1011 1101 0011 1100
R15 in IP table: 0111 1111 1100 0000 0111 0111 1011 1010
R15 XOR with L14: 1101 0101 0111 0011 0101 0111 0001 0000
L15: 1111 0001 1111 1001 1111 0010 0111 1100
R15: 1101 0101 0111 0011 0101 0111 0001 0000
///ROUND 16///
Key16: 0011 0101 1100 0010 1111 1100 0100 0111 1000 1111 1100 1101
R16 expanded to 48bits: 0110 1010 1010 1011 1010 0110 1010 1010 1110 1000 1010 0001
R16 XOR with Key16: 0101 1111 0110 1001 0101 1010 1110 1101 0110 0111 0110 1100
R16 apply SBOXes: 1011 0110 1101 1100 0100 0100 1000 1110
R16 in IP table: 0100 1100 1000 0111 0001 0011 0111 1011
R16 XOR with L15: 1011 1101 0111 1110 1110 0001 0000 0111
L16: 1101 0101 0111 0011 0101 0111 0001 0000
R16: 1011 1101 0111 1110 1110 0001 0000 0111
Block final permutation: 11101101 00111001 11011001 01010000 11111010 01110100 10111100 11000100 => **ED 39 D9 50 FA 74 BC C4**

Шифрування тексту

Зашифруємо текст

"tebe ban navsegda, pishi nick!!!" ,

використовуючи ключ *key* = “76 73 65 6d 5f 62 61 6e” (hex).

Зауважимо, що довжина відкритого тексту має бути кратною 64 бітам (8 байтам), довжина ключа має дорівнювати 64 бітам, з яких буде використано лише 56 бітів.

Одержуємо зашифрований текст:

«'í\xadÕwÁ\x84\x18ØiÃËQ?~J´d2¡ÔÐ\xa0R9\x1f7D_¸Õ;{'»

Примітка: початковий текст розбивався на 4 блоки по 64 біти (8 байт), кожен з блоків проходив 16 раундів, ці шматки збиралися до купи, далі зашифрований текст переведено в ASCII.

Розшифрування тексту

Дано зашифроване за стандартом DES повідомлення:

" ï©;ÞH\x98'Äáîùí\x9eSè{TïÙ\x0e:\x800ëqÅ¨\x93¶Ê·"

або

'20 EF A9 3B DE 48 98 27 C4 E1 EE F9 ED 9E 53 E8 7B 54 EF D9 0E 3A 80 30 EB 71 C5 A8 93 B6 CA B7' (hex)

і відомо 64-бітний ключ:

key = ‘6a 75 6d 70 73 75 69 74’ (hex).

Розшифровуючи заданий криптотекст, одержимо:

'jumpsuit, jumpsuit, cover me, yo'

або

6A 75 6D 70 73 75 69 74 2C 20 6A 75 6D 70 73 75 69 74 2C 20 63 6F 76 65 72 20 6D 65 2C 20 79 6F (hex)

Список літератури

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Диалектика, 2003. – 610 с.

3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.

4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: «Вильямс», 2001. – 672 с.

Додаток 1

Текст програми, що реалізує стандарт шифрування DES

```
#Initial permut matrix for the datas
PI = [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]

#Initial permut made on the key
CP_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]

#Permut applied on shifted key to get Ki+1
CP_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]

#Expand matrix to get a 48bits matrix of datas to apply the xor with Ki
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]

#SBOX
S_BOX = [

[[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],
],

[[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],
],
```

```
[[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],
],

[[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],
],

[[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],
],

[[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],
],

[[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],
],

[[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],
]
]

#Permut made after each SBox substitution for each round
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]

#Final permut for datas after the 16 rounds
PI_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]

#Matrix that determine the shift for each round of keys
SHIFT = [1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1]

def string_to_bit_array(text):#Convert a string into a list of bits
```

```
    array = list()
    for char in text:
        binval = binvalue(char, 8)#Get the char value on one byte
        array.extend([int(x) for x in list(binval)]) #Add the bits to the final list
    return array

def bit_array_to_string(array): #Recreate the string from the bit array
    res = ''.join([chr(int(y,2)) for y in [''.join([str(x) for x in _bytes]) for _bytes in
nsplit(array,8)]])
    return res

def binvalue(val, bitsize): #Return the binary value as a string of the given size
    binval = bin(val)[2:] if isinstance(val, int) else bin(ord(val))[2:]
    if len(binval) > bitsize:
        raise "binary value larger than the expected size"
    while len(binval) < bitsize:
        binval = "0"+binval #Add as many 0 as needed to get the wanted size
    return binval

def nsplit(s, n):#Split a list into sublists of size "n"
    return [s[k:k+n] for k in range(0, len(s), n)]

def string(li, sp=4):
  if sp:
  tmp = []
  for i in range(len(li)):
  tmp.append(li[i])
  if (i+1)%sp == 0 : tmp.append(" ")
  return ''.join(str(i) for i in tmp)
  else: return ''.join(str(i) for i in li)

ENCRYPT=1
DECRYPT=0

class DES():
    def __init__(self):
        self.password = None
        self.text = None
        self.keys = list()

    def run(self, key, text, action=ENCRYPT, padding=False):
        if len(key) < 8:
            raise "Key Should be 8 bytes long"
        elif len(key) > 8:
            key = key[:8] #If key size is above 8bytes, cut to be 8bytes long

        self.password = key
        self.text = text

        if padding and action == ENCRYPT:
            self.addPadding()

        elif len(self.text) % 8 != 0: #If not padding specified data size must be multiple
of 8 bytes
            raise "Data size should be multiple of 8"

        self.generatekeys() #Generate all the keys
```

```
        if action == DECRYPT:
            self.keys.reverse()

        text_blocks = nsplit(self.text, 8) #Split the text in blocks of 8 bytes so 64 bits

        action = "ENC" if action else "DEC"
        result = []
        for block in text_blocks: #Loop over all the blocks of data
            block = string_to_bit_array(block) #Convert the block in bit array
            block = self.permute(block, PI) #Apply the initial permutation
            left, right = nsplit(block, 32) #g(LEFT), d(RIGHT)
            tmp = None

            print(f"\n---{action}-Block:   {string(block,   8)}\nL0:   {string(left)}\nR0:
{string(right)}")

            for i in range(16): #Do the 16 rounds
                print(f"///ROUND {i+1}///")
                print(f"Key{i+1}: {string(self.keys[i])}")
                right_e = self.permute(right, E) #Expand d to match Ki size (48bits)
                print(f"R{i+1} expanded to 48bits: {string(right_e, 4)}")
                tmp = self.xor(self.keys[i], right_e)
                print(f"R{i+1} XOR with Key{i+1}: {string(tmp)}")

                tmp = self.substitute(tmp) #Method that will apply the SBOXes
                print(f"R{i+1} apply SBOXes: {string(tmp)}")
                tmp = self.permute(tmp, P)
                print(f"R{i+1} in IP table: {string(tmp)}")
                tmp = self.xor(left, tmp)
                print(f"R{i+1} XOR with L{i}: {string(tmp)}")
                left = right
                right = tmp
                print(f"L{i+1}: {string(left)}\nR{i+1}: {string(right)}")
            print(f"---Block final permutation: {string(self.permute(right + left, PI_1),
8)}")
            result += self.permute(right + left, PI_1) #Do the last permut and append the
result to result


        final_res = bit_array_to_string(result)
        if padding and action == DECRYPT:
            return self.removePadding(final_res) #Remove the padding if decrypt and padding
is true
        else:
            return final_res #Return the final string of data ciphered/deciphered

    def substitute(self, d_e): #Substitute bytes using SBOX
        subblocks = nsplit(d_e, 6) #Split bit array into sublist of 6 bits
        result = []

        for idx, block in enumerate(subblocks): #For all the sublists
            # [ABCDEF] -> (AF -> row, BCDE -> column)
            row = int(str(block[0]) + str(block[-1]), 2)
            column = int(''.join(str(x) for x in block[1:][:-1]), 2)
            val = S_BOX[idx][row][column]
            result += [int(x) for x in binvalue(val, 4)] # convert val to list of bits
```

```
        return result

    def permute(self, block, table):
        """ Transform block (represented as list of bits) using bit position table """
        return [block[x - 1] for x in table]

    def xor(self, t1, t2):#Apply a xor and return the resulting list
        return [x^y for x, y in zip(t1, t2)]

    def generatekeys(self):
        """ Generate all 16 bit shifted versions of key at once"""
        self.keys = []
        key = string_to_bit_array(self.password)
        key = self.permute(key, CP_1) #Apply the initial permut on the key
        left, right = nsplit(key, 28) #Split it in to (g->LEFT),(d->RIGHT)
        for i in range(16): #Apply the 16 rounds
            left, right = self.shift(left, right, SHIFT[i]) #Apply the shift associated with
the round (not always 1)
            tmp = left + right #Merge them
            self.keys.append(self.permute(tmp, CP_2)) #Apply the permut to get the Ki

    def shift(self, left, right, n):
        """ Shift a list of the given value cyclically to the LEFT
            ([0, 1, 1, 1] -> [1, 1, 1, 0]"""
        return left[n:] + left[:n], right[n:] + right[:n]

    def addPadding(self):#Add padding to the datas using PKCS5 spec.
        pad_len = 8 - (len(self.text) % 8)
        self.text += pad_len*chr(pad_len)

    def removePadding(self, data):#Remove the padding of the plain text (it assume there is
padding)
        pad_len = ord(data[-1])
        return data[:-pad_len]

    def encrypt(self, key, text, padding=False):
        return self.run(key, text, ENCRYPT, padding)

    def decrypt(self, key, text, padding=False):
        return self.run(key, text, DECRYPT, padding)



def hex_string_to_text(hex_string):
    return [chr(int(x, 16)) for x in hex_string.split()]

def text_to_hex_string(text):
    return ' '.join('{0:0>2}'.format(hex(ord(x))[2:].upper()) for x in text)



if __name__ == '__main__':
    text_hex = '07 0B 09 CF B5 6A 0E 6C 44 0D 77 F0 A9 58 B9 AD 6C BE A5 DB BF 5F 6D 45 2A
D5 CB 0D 7B 27 A3 2D'
    key_hex =  '76 73 65 6d 5f 62 61 6e'
    key = hex_string_to_text(key_hex)
```

```
    print(''.join(str(x) for x in string_to_bit_array(key)))       #Binary presentation of
KEY

    text = hex_string_to_text(text_hex)

    d = DES()
    r = d.encrypt(key, text)

    r2 = d.decrypt(key, text)
    print("Ciphered: {0!r}".format(r))
    print("Ciphered (hex): {0}".format(text_to_hex_string(r)))
    print("Deciphered: {0!r}".format(r2))
    print("Deciphered (hex): {0}".format(text_to_hex_string(r2)))
```

Додаток 2

Скріншоти шифрування та розшифрування тексту довжиною
від 20 до 80 символів

ШИФРУВАННЯ

```
---ENC-Block: 10101000 00010000 11011001 00011111 00011000 10110000 11101110 01101011
L0: 1010 1000 0001 0000 1101 1001 0001 1111
R0: 0001 1000 1011 0000 1110 1110 0110 1011
///ROUND 1///
Key1: 1110 0000 1011 1010 0110 1110 1010 1111 0001 1011 1000 0100
R1 expanded to 48bits: 1000 1111 0001 0101 1010 0001 0111 0101 1100 0011 0101 0110
R1 XOR with Key1: 0110 1111 1010 1111 1100 1111 1101 1010 1101 1000 1101 0010
R1 apply SBOXes: 0101 0011 1100 0011 0101 1111 1011 1001
R1 in IP table: 1111 1010 0110 0101 1110 1101 0000 1011
R1 XOR with L0: 0101 0010 0111 0101 0011 0100 0001 0100
L1: 0001 1000 1011 0000 1110 1110 0110 1011
R1: 0101 0010 0111 0101 0011 0100 0001 0100
///ROUND 2///
Key2: 1110 0000 1011 0110 1111 0110 0000 1111 0010 0010 1111 0010
R2 expanded to 48bits: 0010 1010 0100 0011 1010 1010 1001 1010 1000 0000 1010 1000
R2 XOR with Key2: 1100 1010 1111 0101 0101 1100 1001 0101 1010 0010 0101 1010
R2 apply SBOXes: 1100 0010 0101 0100 1100 0111 0100 0000
R2 in IP table: 0100 0101 1011 0101 1011 0000 0000 1000
R2 XOR with L1: 0101 1101 0000 0101 0101 1110 0110 0011
L2: 0101 0010 0111 0101 0011 0100 0001 0100
R2: 0101 1101 0000 0101 0101 1110 0110 0011
///ROUND 3///
Key3: 1111 0100 1101 0110 0101 0110 1111 0101 1110 1001 0100 0101
R3 expanded to 48bits: 1010 1111 1010 1000 0000 1010 1010 1111 1100 0011 0000 0110
R3 XOR with Key3: 0101 1011 0111 1110 0101 1100 0101 1010 0010 1010 0100 0011
R3 apply SBOXes: 1100 1100 1011 0100 1111 1110 0001 1111
R3 in IP table: 0011 1111 1010 1110 1001 1001 1011 1100
R3 XOR with L2: 0110 1101 1101 1011 1010 1101 1010 1000
L3: 0101 1101 0000 0101 0101 1110 0110 0011
R3: 0110 1101 1101 1011 1010 1101 1010 1000
///ROUND 4///
Key4: 0110 0110 1101 0011 0111 0010 0010 0010 1000 0110 1101 1110
R4 expanded to 48bits: 0011 0101 1011 1110 1111 0111 1101 0101 1011 1101 0101 0000
R4 XOR with Key4: 0101 0011 0110 1101 1000 0101 1111 0111 0011 1011 1000 1110
R4 apply SBOXes: 0110 0110 1100 1011 0101 1110 1110 0001
R4 in IP table: 1111 0000 0111 0101 1000 1111 0101 1001
R4 XOR with L3: 1010 1101 0111 0000 1101 0001 0011 1010
L4: 0110 1101 1101 1011 1010 1101 1010 1000
R4: 1010 1101 0111 0000 1101 0001 0011 1010
///ROUND 5///
Key5: 1010 1110 1101 0001 0111 0111 1101 1101 1011 0101 1000 0111
R5 expanded to 48bits: 0101 0101 1010 1011 1010 0001 0110 1010 0010 1001 1111 0101
R5 XOR with Key5: 1111 1011 0111 1010 1101 0110 1011 0111 1001 1100 0111 0010
R5 apply SBOXes: 0000 1100 1001 0101 0010 0110 1001 0110
R5 in IP table: 1000 0110 0010 1010 0001 0001 1011 1001
R5 XOR with L4: 1110 1011 1111 0001 1011 1100 0001 0001
L5: 1010 1101 0111 0000 1101 0001 0011 1010
R5: 1110 1011 1111 0001 1011 1100 0001 0001
///ROUND 6///
Key6: 1010 1111 0100 0011 0101 1011 0010 1110 0100 0110 1110 1001
R6 expanded to 48bits: 1111 0101 0111 1111 1010 0011 1101 1111 1000 0000 1010 0011
R6 XOR with Key6: 0101 1010 0011 1100 1111 1000 1111 0001 1100 0110 0100 1010
R6 apply SBOXes: 1100 1000 1111 0101 0000 0101 0010 1111
R6 in IP table: 1000 1100 1000 1011 1011 1101 0010 1100
R6 XOR with L5: 0010 0001 1111 1011 0110 1100 0001 0110
L6: 1110 1011 1111 0001 1011 1100 0001 0001
R6: 0010 0001 1111 1011 0110 1100 0001 0110
///ROUND 7///
Key7: 0010 1111 0101 0011 1011 1001 0101 1010 1111 1001 0100 0111
```

```
R7 expanded to 48bits: 0001 0000 0011 1111 1111 0110 1011 0101 1000 0000 1010 1100
R7 XOR with Key7: 0011 1111 0110 1100 0100 1111 1110 1111 0111 1001 1110 1011
R7 apply SBOXes: 0001 0110 0100 0011 0100 0111 1000 1010
R7 in IP table: 1100 1000 0110 0111 0010 0000 0001 1011
R7 XOR with L6: 0010 0011 1001 0110 1001 1100 0000 1010
L7: 0010 0001 1111 1011 0110 1100 0001 0110
R7: 0010 0011 1001 0110 1001 1100 0000 1010
///ROUND 8///
Key8: 1001 1111 0001 1001 1101 1001 1010 0110 1100 0101 1011 1000
R8 expanded to 48bits: 0001 0000 0111 1100 1010 1101 0100 1111 1000 0000 0101 0100
R8 XOR with Key8: 1000 1111 0110 0101 0111 0100 1110 1001 0100 0101 1110 1100
R8 apply SBOXes: 1100 0110 0101 0011 0011 0011 1100 1110
R8 in IP table: 1110 1100 1111 0011 1010 0000 1011 0001
R8 XOR with L7: 1100 1101 0000 1000 1100 1100 1010 0111
L8: 0010 0011 1001 0110 1001 1100 0000 1010
R8: 1100 1101 0000 1000 1100 1100 1010 0111
///ROUND 9///
Key9: 0001 1011 0100 1001 1101 1011 1000 0111 0111 1100 1101 1010
R9 expanded to 48bits: 1110 0101 1010 1000 0101 0001 0110 0101 1001 0101 0000 1111
R9 XOR with Key9: 1111 1110 1110 0001 1000 1010 1110 0010 1110 1001 1101 0101
R9 apply SBOXes: 1101 0001 1110 0110 0110 0011 1000 0110
R9 in IP table: 0000 0000 1110 0111 1111 0001 1010 0111
R9 XOR with L8: 0010 0011 0111 0001 0110 1101 1010 1101
L9: 1100 1101 0000 1000 1100 1100 1010 0111
R9: 0010 0011 0111 0001 0110 1101 1010 1101
///ROUND 10///
Key10: 0011 1101 0110 1001 1001 1101 0110 1101 1001 0011 0111 0001
R10 expanded to 48bits: 1001 0000 0110 1011 1010 0010 1011 0101 1011 1101 0101 1010
R10 XOR with Key10: 1010 1101 0000 0010 0011 1111 1101 1000 0010 1110 0010 1011
R10 apply SBOXes: 1001 1001 0110 1110 0101 0001 0000 1010
R10 in IP table: 0010 1000 1100 1111 0111 0000 0100 0110
R10 XOR with L9: 1110 0101 1100 0111 1011 1100 1110 0001
L10: 0010 0011 0111 0001 0110 1101 1010 1101
R10: 1110 0101 1100 0111 1011 1100 1110 0001
///ROUND 11///
Key11: 0001 0111 0010 1101 1000 1101 1001 0011 1100 1100 0110 1110
R11 expanded to 48bits: 1111 0000 1011 1110 0000 1111 1101 1111 1001 0111 0000 0011
R11 XOR with Key11: 1110 0111 1001 0011 1000 0010 0100 1100 0101 1011 0110 1101
R11 apply SBOXes: 1010 0000 0101 1101 0000 0100 1010 1000
R11 in IP table: 1000 1100 1000 0001 0001 0110 0100 1001
R11 XOR with L10: 1010 1111 1111 0000 0111 1011 1110 0100
L11: 1110 0101 1100 0111 1011 1100 1110 0001
R11: 1010 1111 1111 0000 0111 1011 1110 0100
///ROUND 12///
Key12: 0101 1011 0010 1100 1011 0101 0100 1100 1001 1111 1001 0100
R12 expanded to 48bits: 0101 0101 1111 1111 1010 0000 0011 1111 0111 1111 0000 1001
R12 XOR with Key12: 0000 1110 1101 0011 0001 0101 0111 0011 1110 0000 1001 1101
R12 apply SBOXes: 1111 0100 1111 0010 1110 0110 1011 1001
R12 in IP table: 0000 1111 1110 0101 1000 1111 1001 1111
R12 XOR with L11: 1110 1010 0010 0010 0011 0011 0111 1110
L12: 1010 1111 1111 0000 0111 1011 1110 0100
R12: 1110 1010 0010 0010 0011 0011 0111 1110
///ROUND 13///
Key13: 1101 1101 1010 1100 1010 1100 1001 1001 0110 0100 1111 1101
R13 expanded to 48bits: 0111 0101 0100 0001 0000 0100 0001 1010 0110 1011 1111 1101
R13 XOR with Key13: 1010 1000 1110 1101 1010 1000 1000 0011 0000 1111 0000 0000
R13 apply SBOXes: 0110 0100 1100 1100 0100 0111 1001 1101
R13 in IP table: 0000 1010 0010 0101 1011 1011 0111 1001
R13 XOR with L12: 1010 0101 1101 0101 1100 0000 1001 1101
L13: 1110 1010 0010 0010 0011 0011 0111 1110
R13: 1010 0101 1101 0101 1100 0000 1001 1101
///ROUND 14///
Key14: 1101 0010 1010 0110 1010 1110 0110 1011 1101 1010 1000 0001
R14 expanded to 48bits: 1101 0000 1011 1110 1010 1011 1110 0000 0001 0100 1111 1011
R14 XOR with Key14: 0000 0010 0001 1000 0000 0101 1000 1011 1100 1110 0111 1010
R14 apply SBOXes: 1110 1101 1101 1011 0010 1011 1110 0011
R14 in IP table: 1001 0100 1111 1011 1110 1111 1101 0001
R14 XOR with L13: 0111 1110 1101 1001 1101 1100 1010 1111
```

```
L14: 1010 0101 1101 0101 1100 0000 1001 1101
R14: 0111 1110 1101 1001 1101 1100 1010 1111
///ROUND 15///
Key15: 1111 1000 1001 1110 0010 0110 1001 0010 0110 0101 0011 1111
R15 expanded to 48bits: 1011 1111 1101 0110 1111 0011 1110 1111 1001 0101 0101 1110
R15 XOR with Key15: 0100 0111 0100 1000 1101 0101 0111 1101 1111 0000 0110 0001
R15 apply SBOXes: 1010 1100 1010 0010 0110 1000 1101 0010
R15 in IP table: 0001 0010 1101 1110 0000 0011 1001 0101
R15 XOR with L14: 1011 0111 0000 1011 1100 0011 0000 1000
L15: 0111 1110 1101 1001 1101 1100 1010 1111
R15: 1011 0111 0000 1011 1100 0011 0000 1000
///ROUND 16///
Key16: 1111 0001 1011 1110 0010 0010 1011 0101 0101 1101 0001 0111
R16 expanded to 48bits: 0101 1010 1110 1000 0101 0111 1110 0000 0110 1000 0101 0001
R16 XOR with Key16: 1010 1011 0101 0110 0111 0101 0101 0101 0011 0101 0100 0110
R16 apply SBOXes: 0110 0111 1100 0101 1111 0001 0101 0100
R16 in IP table: 1110 0011 0001 0101 1111 0011 1011 0000
R16 XOR with L15: 1001 1101 1100 1100 0010 1111 0001 1111
L16: 1011 0111 0000 1011 1100 0011 0000 1000
R16: 1001 1101 1100 1100 0010 1111 0001 1111
---Block final permutation: 11101101 10101101 11010101 01110111 11000001 10000100 00011000 11011000

---ENC-Block: 00101101 01101100 10000111 11010110 11011000 11011100 11110010 00000100
L0: 0010 1101 0110 1100 1000 0111 1101 0110
R0: 1101 1000 1101 1100 1111 0010 0000 0100
///ROUND 1///
Key1: 1110 0000 1011 1010 0110 1110 1010 1111 0001 1011 1000 0100
R1 expanded to 48bits: 0110 1111 0001 0110 1111 1001 0111 1010 0100 0000 0000 1001
R1 XOR with Key1: 1000 1111 1010 1100 1001 0111 1101 0101 0101 1011 1000 1101
R1 apply SBOXes: 1100 0011 0001 1100 0000 1101 1110 0111
R1 in IP table: 0101 0100 1001 0010 1111 1100 0110 1001
R1 XOR with L0: 0111 1001 1111 1110 0111 1011 1011 1111
L1: 1101 1000 1101 1100 1111 0010 0000 0100
R1: 0111 1001 1111 1110 0111 1011 1011 1111
///ROUND 2///
Key2: 1110 0000 1011 0110 1111 0110 0000 1111 0010 0010 1111 0010
R2 expanded to 48bits: 1011 1111 0011 1111 1111 1100 0011 1111 0111 1101 1111 1110
R2 XOR with Key2: 0101 1111 1000 1001 0000 1010 0011 0000 0101 1111 0000 1100
R2 apply SBOXes: 1011 1001 0100 0110 1011 0100 1001 1011
R2 in IP table: 0010 1011 1100 1011 0101 1010 1000 1011
R2 XOR with L1: 1111 0011 0001 0111 1010 1000 1000 1111
L2: 0111 1001 1111 1110 0111 1011 1011 1111
R2: 1111 0011 0001 0111 1010 1000 1000 1111
///ROUND 3///
Key3: 1111 0100 1101 0110 0101 0110 1111 0101 1110 1001 0100 0101
R3 expanded to 48bits: 1111 1010 0110 1000 1010 1111 1101 0101 0001 0100 0101 1111
R3 XOR with Key3: 0000 1110 1011 1110 1111 1001 0010 0000 1111 1101 0001 1010
R3 apply SBOXes: 1111 1111 0101 1100 0111 0101 0110 0000
R3 in IP table: 0110 0100 1001 1101 1111 0110 1101 1010
R3 XOR with L2: 0001 1101 0110 0011 1000 1101 0110 0101
L3: 1111 0011 0001 0111 1010 1000 1000 1111
R3: 0001 1101 0110 0011 1000 1101 0110 0101
///ROUND 4///
Key4: 0110 0110 1101 0011 0111 0010 0010 0010 1000 0110 1101 1110
R4 expanded to 48bits: 1000 1111 1010 1011 0000 0111 1100 0101 1010 1011 0000 1010
R4 XOR with Key4: 1110 1001 0111 1000 0111 0101 1110 0111 0010 1101 1101 0100
R4 apply SBOXes: 1010 1010 0001 0101 1010 0000 1111 0011
R4 in IP table: 1100 0111 1001 1010 0001 1110 1000 0001
R4 XOR with L3: 0011 0100 1000 1101 1011 0110 0000 1110
L4: 0001 1101 0110 0011 1000 1101 0110 0101
R4: 0011 0100 1000 1101 1011 0110 0000 1110
///ROUND 5///
Key5: 1010 1110 1101 0001 0111 0111 1101 1101 1011 0101 1000 0111
R5 expanded to 48bits: 0001 1010 1001 0100 0101 1011 1101 1010 1100 0000 0101 1100
R5 XOR with Key5: 1011 0100 0100 0101 0010 1100 0000 0111 0111 0101 1101 1011
R5 apply SBOXes: 0001 1000 1100 0111 1110 0111 1100 1110
R5 in IP table: 1000 1001 0111 1111 0011 0001 1010 1011
R5 XOR with L4: 1001 0100 0001 1100 1011 1100 1100 1110
```

```
L5: 0011 0100 1000 1101 1011 0110 0000 1110
R5: 1001 0100 0001 1100 1011 1100 1100 1110
///ROUND 6///
Key6: 1010 1111 0100 0011 0101 1011 0010 1110 0100 0110 1110 1001
R6 expanded to 48bits: 0100 1010 1000 0000 1111 1001 0101 1111 1001 0110 0101 1101
R6 XOR with Key6: 1110 0101 1100 0011 1010 0010 0111 0001 1101 0000 1011 0100
R6 apply SBOXes: 1010 0101 0101 0110 1110 0011 1011 1010
R6 in IP table: 0000 1111 1110 0111 0111 0110 1001 0001
R6 XOR with L5: 0011 1011 0110 1010 1100 0000 1001 1111
L6: 1001 0100 0001 1100 1011 1100 1100 1110
R6: 0011 1011 0110 1010 1100 0000 1001 1111
///ROUND 7///
Key7: 0010 1111 0101 0011 1011 1001 0101 1010 1111 1001 0100 0111
R7 expanded to 48bits: 1001 1111 0110 1011 0101 0101 0110 0000 0001 0100 1111 1110
R7 XOR with Key7: 1011 0000 0011 1000 1110 1100 0011 1010 1110 1101 1011 1001
R7 apply SBOXes: 0010 1101 1010 0111 0110 0011 1000 0011
R7 in IP table: 1000 0000 0110 1110 0111 1011 1001 0101
R7 XOR with L6: 0001 0100 0111 0010 1100 0111 0101 1011
L7: 0011 1011 0110 1010 1100 0000 1001 1111
R7: 0001 0100 0111 0010 1100 0111 0101 1011
///ROUND 8///
Key8: 1001 1111 0001 1001 1101 1001 1010 0110 1100 0101 1011 1000
R8 expanded to 48bits: 1000 1010 1000 0011 1010 0101 0110 0000 1110 1010 1111 0110
R8 XOR with Key8: 0001 0101 1001 1010 0111 1100 1100 0110 0010 1111 0100 1110
R8 apply SBOXes: 0111 0110 0110 1000 0110 1110 0011 0001
R8 in IP table: 0101 0010 0010 0101 1000 1110 1101 1110
R8 XOR with L7: 0110 1001 0100 1111 0100 1110 0100 0001
L8: 0001 0100 0111 0010 1100 0111 0101 1011
R8: 0110 1001 0100 1111 0100 1110 0100 0001
///ROUND 9///
Key9: 0001 1011 0100 1001 1101 1011 1000 0111 0111 1100 1101 1010
R9 expanded to 48bits: 1011 0101 0010 1010 0101 1110 1010 0101 1100 0010 0000 0010
R9 XOR with Key9: 1010 1110 0110 0011 1000 0101 0010 0010 1011 1110 1101 1000
R9 apply SBOXes: 1001 1011 0101 1011 0111 0101 0010 0101
R9 in IP table: 1110 0100 1100 1101 0110 1100 1110 1010
R9 XOR with L8: 1111 0000 1011 1111 1010 1011 1011 0001
L9: 0110 1001 0100 1111 0100 1110 0100 0001
R9: 1111 0000 1011 1111 1010 1011 1011 0001
///ROUND 10///
Key10: 0011 1101 0110 1001 1001 1101 0110 1101 1001 0011 0111 0001
R10 expanded to 48bits: 1111 1010 0001 0101 1111 1111 1101 0101 0111 1101 1010 0011
R10 XOR with Key10: 1100 0111 0111 1100 0110 0010 1011 1000 1110 1110 1101 0010
R10 apply SBOXes: 0101 1100 0100 0110 1000 1000 0010 1001
R10 in IP table: 0001 1001 0100 1001 1001 1100 0001 0010
R10 XOR with L9: 0111 0000 0000 0110 1101 0010 0101 0011
L10: 1111 0000 1011 1111 1010 1011 1011 0001
R10: 0111 0000 0000 0110 1101 0010 0101 0011
///ROUND 11///
Key11: 0001 0111 0010 1101 1000 1101 1001 0011 1100 1100 0110 1110
R11 expanded to 48bits: 1011 1010 0000 0000 0000 1101 0110 1010 0100 0010 1010 0110
R11 XOR with Key11: 1010 1101 0010 1101 1000 0000 1111 1001 1000 1110 1100 1000
R11 apply SBOXes: 1001 0111 1100 0111 1110 1110 0010 0110
R11 in IP table: 1101 0001 1110 0111 0101 0101 1011 1010
R11 XOR with L10: 0010 0001 0101 1000 1111 1110 0000 1011
L11: 0111 0000 0000 0110 1101 0010 0101 0011
R11: 0010 0001 0101 1000 1111 1110 0000 1011
///ROUND 12///
Key12: 0101 1011 0010 1100 1011 0101 0100 1100 1001 1111 1001 0100
R12 expanded to 48bits: 1001 0000 0010 1010 1111 0001 0111 1111 1100 0000 0101 0110
R12 XOR with Key12: 1100 1011 0000 0110 0100 0100 0011 0011 0101 1111 1100 0010
R12 apply SBOXes: 1100 0101 1100 1110 1011 0001 1100 0010
R12 in IP table: 0010 0001 1101 0011 1111 0001 1101 0001
R12 XOR with L11: 0101 0001 1101 0101 0010 0011 1000 0010
L12: 0010 0001 0101 1000 1111 1110 0000 1011
R12: 0101 0001 1101 0101 0010 0011 1000 0010
///ROUND 13///
Key13: 1101 1101 1010 1100 1010 1100 1001 1001 0110 0100 1111 1101
R13 expanded to 48bits: 0010 1010 0011 1110 1010 1010 1001 0000 0111 1100 0000 0100
```

```
R13 XOR with Key13: 1111 0111 1001 0010 0000 0110 0000 1001 0001 1000 1111 1001
R13 apply SBOXes: 0110 0000 0110 0011 1100 0110 1011 0011
R13 in IP table: 1000 0011 0110 0111 1000 1110 0000 1101
R13 XOR with L12: 1010 0010 0011 1111 0111 0000 0000 0110
L13: 0101 0001 1101 0101 0010 0011 1000 0010
R13: 1010 0010 0011 1111 0111 0000 0000 0110
///ROUND 14///
Key14: 1101 0010 1010 0110 1010 1110 0110 1011 1101 1010 1000 0001
R14 expanded to 48bits: 0101 0000 0100 0001 1111 1110 1011 1010 0000 0000 0000 1101
R14 XOR with Key14: 1000 0010 1110 0111 0101 0000 1101 0001 1101 1010 1000 1100
R14 apply SBOXes: 0100 0001 1111 0001 1100 0011 0011 1011
R14 in IP table: 1000 1111 0010 0111 1110 1101 0000 0100
R14 XOR with L13: 1101 1110 1111 0010 1100 1110 1000 0110
L14: 1010 0010 0011 1111 0111 0000 0000 0110
R14: 1101 1110 1111 0010 1100 1110 1000 0110
///ROUND 15///
Key15: 1111 1000 1001 1110 0010 0110 1001 0010 0110 0101 0011 1111
R15 expanded to 48bits: 0110 1111 1101 0111 1010 0101 0110 0101 1101 0100 0000 1101
R15 XOR with Key15: 1001 0111 0100 1001 1000 0011 1111 0111 1011 0001 0011 0010
R15 apply SBOXes: 1000 1100 1001 1000 0101 0000 0010 0110
R15 in IP table: 0010 0100 1000 1110 0000 0101 0111 0000
R15 XOR with L14: 1000 0110 1011 0001 0111 0101 0111 0110
L15: 1101 1110 1111 0010 1100 1110 1000 0110
R15: 1000 0110 1011 0001 0111 0101 0111 0110
///ROUND 16///
Key16: 1111 0001 1011 1110 0010 0010 1011 0101 0101 1101 0001 0111
R16 expanded to 48bits: 0100 0000 1101 0101 1010 0010 1011 1010 1010 1011 1010 1101
R16 XOR with Key16: 1011 0001 0110 1011 1000 0000 0000 1111 1111 0110 1011 1010
R16 apply SBOXes: 0010 1101 0000 0111 1011 1101 1010 0011
R16 in IP table: 1011 0001 0100 1010 0111 1110 1001 1001
R16 XOR with L15: 0110 1111 1011 1000 1011 0000 0001 1111
L16: 1000 0110 1011 0001 0111 0101 0111 0110
R16: 0110 1111 1011 1000 1011 0000 0001 1111
---Block final permutation: 01101001 11000011 11001011 01010001 00111111 01111110 01001010 10110100

---ENC-Block: 11101001 00111010 11110111 11111100 00011110 01010111 01111011 00111010
L0: 1110 1001 0011 1010 1111 0111 1111 1100
R0: 0001 1110 0101 0111 0111 1011 0011 1010
///ROUND 1///
Key1: 1110 0000 1011 1010 0110 1110 1010 1111 0001 1011 1000 0100
R1 expanded to 48bits: 0000 1111 1100 0010 1010 1110 1011 1111 0110 1001 1111 0100
R1 XOR with Key1: 1110 1111 0111 1000 1100 0000 0001 0000 0111 0010 0111 0000
R1 apply SBOXes: 0000 1100 1010 0111 0100 0010 0100 0000
R1 in IP table: 1000 0000 0111 1100 0001 0001 0001 0100
R1 XOR with L0: 0110 1001 0100 0110 1110 0110 1110 1000
L1: 0001 1110 0101 0111 0111 1011 0011 1010
R1: 0110 1001 0100 0110 1110 0110 1110 1000
///ROUND 2///
Key2: 1110 0000 1011 0110 1111 0110 0000 1111 0010 0010 1111 0010
R2 expanded to 48bits: 0011 0101 0010 1010 0000 1101 0111 0000 1101 0111 0101 0000
R2 XOR with Key2: 1101 0101 1001 1100 1111 1011 0111 1111 1111 0101 1010 0010
R2 apply SBOXes: 0011 0110 1111 0111 0110 1101 0111 1011
R2 in IP table: 1101 1110 0101 0111 0011 1111 1001 1110
R2 XOR with L1: 1100 0000 0000 0000 0100 0100 1010 0100
L2: 0110 1001 0100 0110 1110 0110 1110 1000
R2: 1100 0000 0000 0000 0100 0100 1010 0100
///ROUND 3///
Key3: 1111 0100 1101 0110 0101 0110 1111 0101 1110 1001 0100 0101
R3 expanded to 48bits: 0110 0000 0000 0000 0000 0000 0010 0000 1001 0101 0000 1001
R3 XOR with Key3: 1001 0100 1101 0110 0101 0110 1101 0101 0111 1100 0100 1100
R3 apply SBOXes: 1000 1000 1100 0101 0000 1110 1001 1011
R3 in IP table: 1001 1010 1010 1011 0001 1001 0000 1001
R3 XOR with L2: 1111 0011 1110 1101 1111 1111 1110 0001
L3: 1100 0000 0000 0000 0100 0100 1010 0100
R3: 1111 0011 1110 1101 1111 1111 1110 0001
///ROUND 4///
Key4: 0110 0110 1101 0011 0111 0010 0010 0010 1000 0110 1101 1110
R4 expanded to 48bits: 1111 1010 0111 1111 0101 1011 1111 1111 1111 1111 0000 0011
```

```
R4 XOR with Key4: 1001 1100 1010 1100 0010 1001 1101 1101 0111 1001 1101 1101
R4 apply SBOXes: 0010 1011 1011 1010 1001 1110 1000 1001
R4 in IP table: 0111 1101 0110 1000 0100 1011 0100 1101
R4 XOR with L3: 1011 1101 0110 1000 0000 1111 1110 1001
L4: 1111 0011 1110 1101 1111 1111 1110 0001
R4: 1011 1101 0110 1000 0000 1111 1110 1001
///ROUND 5///
Key5: 1010 1110 1101 0001 0111 0111 1101 1101 1011 0101 1000 0111
R5 expanded to 48bits: 1101 1111 1010 1011 0101 0000 0000 0101 1111 1111 0101 0011
R5 XOR with Key5: 0111 0001 0111 1010 0010 0111 1101 1000 0100 1010 1101 0100
R5 apply SBOXes: 0000 1010 1000 0110 0101 1010 0100 0011
R5 in IP table: 0111 0000 0111 1110 0001 1001 0000 0000
R5 XOR with L4: 1000 0011 1001 0011 1110 0110 1110 0001
L5: 1011 1101 0110 1000 0000 1111 1110 1001
R5: 1000 0011 1001 0011 1110 0110 1110 0001
///ROUND 6///
Key6: 1010 1111 0100 0011 0101 1011 0010 1110 0100 0110 1110 1001
R6 expanded to 48bits: 1100 0000 0111 1100 1010 0111 1111 0000 1101 0111 0000 0011
R6 XOR with Key6: 0110 1111 0011 1111 1111 1100 1101 1110 1001 0001 1110 1010
R6 apply SBOXes: 0101 0110 1100 1000 1001 1001 0111 1100
R6 in IP table: 0111 1011 0001 0001 1010 0101 0111 0010
R6 XOR with L5: 1100 0110 0111 1001 1010 1010 1001 1011
L6: 1000 0011 1001 0011 1110 0110 1110 0001
R6: 1100 0110 0111 1001 1010 1010 1001 1011
///ROUND 7///
Key7: 0010 1111 0101 0011 1011 1001 0101 1010 1111 1001 0100 0111
R7 expanded to 48bits: 1110 0000 1100 0011 1111 0011 1101 0101 0101 0100 1111 0111
R7 XOR with Key7: 1100 1111 1001 0000 0100 1010 1000 1111 1010 1101 1011 0000
R7 apply SBOXes: 1011 0000 1101 0110 1000 1101 1000 0000
R7 in IP table: 0001 0101 1100 0001 0011 0011 0000 1011
R7 XOR with L6: 1001 0110 0101 0010 1101 0101 1110 1010
L7: 1100 0110 0111 1001 1010 1010 1001 1011
R7: 1001 0110 0101 0010 1101 0101 1110 1010
///ROUND 8///
Key8: 1001 1111 0001 1001 1101 1001 1010 0110 1100 0101 1011 1000
R8 expanded to 48bits: 0100 1010 1100 0010 1010 0101 0110 1010 1011 1111 0101 0101
R8 XOR with Key8: 1101 0101 1101 1011 0111 1100 1100 1100 0111 1010 1110 1101
R8 apply SBOXes: 0011 1011 1000 1000 1111 0010 0100 1000
R8 in IP table: 0110 1001 0011 1100 0100 0011 1100 0010
R8 XOR with L7: 1010 1111 0100 0101 1110 1001 0101 1001
L8: 1001 0110 0101 0010 1101 0101 1110 1010
R8: 1010 1111 0100 0101 1110 1001 0101 1001
///ROUND 9///
Key9: 0001 1011 0100 1001 1101 1011 1000 0111 0111 1100 1101 1010
R9 expanded to 48bits: 1101 0101 1110 1010 0000 1011 1111 0101 0010 1010 1111 0011
R9 XOR with Key9: 1100 1110 1010 0011 1101 0000 0111 0010 0101 0110 0010 1001
R9 apply SBOXes: 1011 0100 1010 0001 1110 0010 0101 0100
R9 in IP table: 1000 0011 1011 0100 0000 0011 1011 0110
R9 XOR with L8: 0001 0101 1110 0110 1101 0110 0101 1100
L9: 1010 1111 0100 0101 1110 1001 0101 1001
R9: 0001 0101 1110 0110 1101 0110 0101 1100
///ROUND 10///
Key10: 0011 1101 0110 1001 1001 1101 0110 1101 1001 0011 0111 0001
R10 expanded to 48bits: 0000 1010 1011 1111 0000 1101 0110 1010 1100 0010 1111 1000
R10 XOR with Key10: 0011 0111 1101 0110 1001 0000 0000 0111 0101 0001 1000 1001
R10 apply SBOXes: 1101 1110 0100 0001 1110 0001 1110 1010
R10 in IP table: 1100 1001 1001 1111 1010 0100 1001 0011
R10 XOR with L9: 0110 0110 1101 1010 0100 1101 1100 1010
L10: 0001 0101 1110 0110 1101 0110 0101 1100
R10: 0110 0110 1101 1010 0100 1101 1100 1010
///ROUND 11///
Key11: 0001 0111 0010 1101 1000 1101 1001 0011 1100 1100 0110 1110
R11 expanded to 48bits: 0011 0000 1101 0110 1111 0100 0010 0101 1011 1110 0101 0100
R11 XOR with Key11: 0010 0111 1111 1011 0111 1001 1011 0110 0111 0010 0011 1010
R11 apply SBOXes: 1110 1001 1000 1100 0010 1100 1111 0011
R11 in IP table: 0001 0010 1001 1010 1101 1111 1100 1001
R11 XOR with L10: 0000 0111 0111 1100 0000 1001 1001 0101
L11: 0110 0110 1101 1010 0100 1101 1100 1010
```

```
R11: 0000 0111 0111 1100 0000 1001 1001 0101
///ROUND 12///
Key12: 0101 1011 0010 1100 1011 0101 0100 1100 1001 1111 1001 0100
R12 expanded to 48bits: 1000 0000 1110 1011 1111 1000 0000 0101 0011 1100 1010 1010
R12 XOR with Key12: 1101 1011 1100 0111 0100 1101 0100 1001 1010 0011 0011 1110
R12 apply SBOXes: 0111 0010 1111 0000 0101 0111 1000 1000
R12 in IP table: 0110 1100 0010 0101 1010 0011 0000 1111
R12 XOR with L11: 0000 1010 1111 1111 1110 1110 1100 0101
L12: 0000 0111 0111 1100 0000 1001 1001 0101
R12: 0000 1010 1111 1111 1110 1110 1100 0101
///ROUND 13///
Key13: 1101 1101 1010 1100 1010 1100 1001 1001 0110 0100 1111 1101
R13 expanded to 48bits: 1000 0101 0101 0111 1111 1111 1111 0101 1101 0110 0000 1010
R13 XOR with Key13: 0101 1000 1111 1011 0101 0011 0110 1100 1011 0010 1111 0111
R13 apply SBOXes: 1100 1110 1000 0111 1001 1100 1001 0000
R13 in IP table: 1111 0011 1100 1000 1001 0001 0001 1001
R13 XOR with L12: 1111 0100 1011 0100 1001 1000 1000 1100
L13: 0000 1010 1111 1111 1110 1110 1100 0101
R13: 1111 0100 1011 0100 1001 1000 1000 1100
///ROUND 14///
Key14: 1101 0010 1010 0110 1010 1110 0110 1011 1101 1010 1000 0001
R14 expanded to 48bits: 0111 1010 1001 0101 1010 1001 0100 1111 0001 0100 0101 1001
R14 XOR with Key14: 1010 1000 0011 0011 0000 0111 0010 0100 1100 1110 1101 1000
R14 apply SBOXes: 0110 1101 1111 0101 0100 0110 0010 0101
R14 in IP table: 1000 0100 0010 1101 1101 1111 0011 1100
R14 XOR with L13: 1000 1110 1101 0010 0011 0001 1111 1001
L14: 1111 0100 1011 0100 1001 1000 1000 1100
R14: 1000 1110 1101 0010 0011 0001 1111 1001
///ROUND 15///
Key15: 1111 1000 1001 1110 0010 0110 1001 0010 0110 0101 0011 1111
R15 expanded to 48bits: 1100 0101 1101 0110 1010 0100 0001 1010 0011 1111 1111 0011
R15 XOR with Key15: 0011 1101 0100 1000 1000 0010 1000 1000 0101 1010 1100 1100
R15 apply SBOXes: 0001 0010 0110 1101 0010 0100 0100 1011
R15 in IP table: 1100 1000 0001 0011 0001 1000 1100 1110
R15 XOR with L14: 0011 1100 1010 0111 1000 0000 0100 0010
L15: 1000 1110 1101 0010 0011 0001 1111 1001
R15: 0011 1100 1010 0111 1000 0000 0100 0010
///ROUND 16///
Key16: 1111 0001 1011 1110 0010 0010 1011 0101 0101 1101 0001 0111
R16 expanded to 48bits: 0001 1111 1001 0101 0000 1111 1100 0000 0000 0010 0000 0100
R16 XOR with Key16: 1110 1110 0010 1011 0010 1101 0111 0101 0101 1111 0001 0011
R16 apply SBOXes: 0000 1110 0011 1101 1000 1101 1001 0101
R16 in IP table: 1101 0111 0000 1000 0011 1000 0111 1101
R16 XOR with L15: 0101 1001 1101 1010 0000 1001 1000 0100
L16: 0011 1100 1010 0111 1000 0000 0100 0010
R16: 0101 1001 1101 1010 0000 1001 1000 0100
---Block final permutation: 01100100 00110010 10100001 11010100 11010000 10100000 01010010 00111001

---ENC-Block: 00010110 00010010 10101010 11111110 01000110 11110001 10011101 01110101
L0: 0001 0110 0001 0010 1010 1010 1111 1110
R0: 0100 0110 1111 0001 1001 1101 0111 0101
///ROUND 1///
Key1: 1110 0000 1011 1010 0110 1110 1010 1111 0001 1011 1000 0100
R1 expanded to 48bits: 1010 0000 1101 0111 1010 0011 1100 1111 1010 1011 1010 1010
R1 XOR with Key1: 0100 0000 0110 1101 1100 1101 0110 0000 1011 0000 0010 1110
R1 apply SBOXes: 0011 1110 0011 0000 1101 1100 0100 0010
R1 in IP table: 0111 0101 0001 1110 0000 0010 0001 1110
R1 XOR with L0: 0110 0011 0000 1100 1010 1000 1110 0000
L1: 0100 0110 1111 0001 1001 1101 0111 0101
R1: 0110 0011 0000 1100 1010 1000 1110 0000
///ROUND 2///
Key2: 1110 0000 1011 0110 1111 0110 0000 1111 0010 0010 1111 0010
R2 expanded to 48bits: 0011 0000 0110 1000 0101 1001 0101 0101 0001 0111 0000 0000
R2 XOR with Key2: 1101 0000 1101 1110 1010 1111 0101 1010 0011 0101 1111 0010
R2 apply SBOXes: 1001 1000 1010 1000 1111 0011 1100 0110
R2 in IP table: 0010 0001 1011 1110 0010 0001 1110 0111
R2 XOR with L1: 0110 0111 0100 1111 1011 1100 1001 0010
L2: 0110 0011 0000 1100 1010 1000 1110 0000
```

```
R2: 0110 0111 0100 1111 1011 1100 1001 0010
///ROUND 3///
Key3: 1111 0100 1101 0110 0101 0110 1111 0101 1110 1001 0100 0101
R3 expanded to 48bits: 0011 0000 1110 1010 0101 1111 1101 1111 1001 0100 1010 0100
R3 XOR with Key3: 1100 0100 0011 1100 0000 1001 0010 1010 0111 1101 1110 0001
R3 apply SBOXes: 0101 1101 1011 0110 1010 1100 1111 0010
R3 in IP table: 0001 0111 0101 1010 1101 0101 1001 1111
R3 XOR with L2: 0111 0100 0101 0110 0111 1101 0111 1111
L3: 0110 0111 0100 1111 1011 1100 1001 0010
R3: 0111 0100 0101 0110 0111 1101 0111 1111
///ROUND 4///
Key4: 0110 0110 1101 0011 0111 0010 0010 0010 1000 0110 1101 1110
R4 expanded to 48bits: 1011 1010 1000 0010 1010 1100 0011 1111 1010 1011 1111 1110
R4 XOR with Key4: 1101 1100 0101 0001 1101 1110 0001 1101 0010 1101 0010 0000
R4 apply SBOXes: 1110 0100 1001 1111 1100 1101 0110 0111
R4 in IP table: 1001 0101 1101 0110 1011 1111 0111 1000
R4 XOR with L3: 1111 0010 1001 1001 0000 0011 1110 1010
L4: 0111 0100 0101 0110 0111 1101 0111 1111
R4: 1111 0010 1001 1001 0000 0011 1110 1010
///ROUND 5///
Key5: 1010 1110 1101 0001 0111 0111 1101 1101 1011 0101 1000 0111
R5 expanded to 48bits: 0111 1010 0101 0100 1111 0010 1000 0000 0111 1111 0101 0101
R5 XOR with Key5: 1101 0100 1000 0101 1000 0101 0101 1101 1100 1010 1101 0010
R5 apply SBOXes: 0011 0110 0111 1011 1010 0101 0100 1001
R5 in IP table: 1100 1101 0101 0001 0010 1010 1101 1110
R5 XOR with L4: 1011 1001 0000 0111 0101 0111 1010 0001
L5: 1111 0010 1001 1001 0000 0011 1110 1010
R5: 1011 1001 0000 0111 0101 0111 1010 0001
///ROUND 6///
Key6: 1010 1111 0100 0011 0101 1011 0010 1110 0100 0110 1110 1001
R6 expanded to 48bits: 1101 1111 0010 1000 0000 1110 1010 1010 1111 1101 0000 0011
R6 XOR with Key6: 0111 0000 0110 1011 0101 0101 1000 0100 1011 1011 1110 1010
R6 apply SBOXes: 0000 1110 1000 0010 1011 1100 0111 1100
R6 in IP table: 0111 1011 0101 1000 0000 0101 1011 1000
R6 XOR with L5: 1000 1001 1100 0001 0000 0110 0101 0010
L6: 1011 1001 0000 0111 0101 0111 1010 0001
R6: 1000 1001 1100 0001 0000 0110 0101 0010
///ROUND 7///
Key7: 0010 1111 0101 0011 1011 1001 0101 1010 1111 1001 0100 0111
R7 expanded to 48bits: 0100 0101 0011 1110 0000 0010 1000 0000 1100 0010 1010 0101
R7 XOR with Key7: 0110 1010 0110 1101 1011 1011 1101 1010 0011 1011 1110 0010
R7 apply SBOXes: 1001 1011 1100 0111 0101 0011 0111 1011
R7 in IP table: 1110 1010 1111 1111 0111 1101 0000 0010
R7 XOR with L6: 0101 0011 1111 1000 0010 1010 1010 0011
L7: 1000 1001 1100 0001 0000 0110 0101 0010
R7: 0101 0011 1111 1000 0010 1010 1010 0011
///ROUND 8///
Key8: 1001 1111 0001 1001 1101 1001 1010 0110 1100 0101 1011 1000
R8 expanded to 48bits: 1010 1010 0111 1111 1111 0000 0001 0101 0101 0101 0000 0110
R8 XOR with Key8: 0011 0101 0110 0110 0010 1001 1011 0011 1001 0000 1011 1110
R8 apply SBOXes: 1101 1101 1011 1010 0111 0110 1011 1000
R8 in IP table: 0010 1110 1110 1100 1100 0101 1101 1111
R8 XOR with L7: 1010 0111 0010 1101 1100 0011 1000 1101
L8: 0101 0011 1111 1000 0010 1010 1010 0011
R8: 1010 0111 0010 1101 1100 0011 1000 1101
///ROUND 9///
Key9: 0001 1011 0100 1001 1101 1011 1000 0111 0111 1100 1101 1010
R9 expanded to 48bits: 1101 0000 1110 1001 0101 1011 1110 0000 0111 1100 0101 1011
R9 XOR with Key9: 1100 1011 1010 0000 1000 0000 0110 0111 0000 0000 1000 0001
R9 apply SBOXes: 1100 0011 0000 0111 0011 0111 1011 0001
R9 in IP table: 1110 0010 1110 0000 1111 1100 1000 1001
R9 XOR with L8: 1011 0001 0001 1000 1101 0110 0010 1010
L9: 1010 0111 0010 1101 1100 0011 1000 1101
R9: 1011 0001 0001 1000 1101 0110 0010 1010
///ROUND 10///
Key10: 0011 1101 0110 1001 1001 1101 0110 1101 1001 0011 0111 0001
R10 expanded to 48bits: 0101 1010 0010 1000 1111 0001 0110 1010 1100 0001 0101 0101
R10 XOR with Key10: 0110 0111 0100 0001 0110 1100 0000 0111 0101 0010 0010 0100
```

```
R10 apply SBOXes: 1001 1100 0000 0111 1110 0001 1111 0100
R10 in IP table: 1000 0011 1101 1100 0011 0100 1011 0011
R10 XOR with L9: 0010 0100 1111 0001 1111 0111 0011 1110
L10: 1011 0001 0001 1000 1101 0110 0010 1010
R10: 0010 0100 1111 0001 1111 0111 0011 1110
///ROUND 11///
Key11: 0001 0111 0010 1101 1000 1101 1001 0011 1100 1100 0110 1110
R11 expanded to 48bits: 0001 0000 1001 0111 1010 0011 1111 1010 1110 1001 1111 1100
R11 XOR with Key11: 0000 0111 1011 1010 0010 1110 0110 1001 0010 0101 1001 0010
R11 apply SBOXes: 0000 0101 1000 1101 0000 1101 0111 1001
R11 in IP table: 1001 1010 0001 0000 0111 1101 0101 1000
R11 XOR with L10: 0010 1011 0000 1000 1010 1011 0111 0010
L11: 0010 0100 1111 0001 1111 0111 0011 1110
R11: 0010 1011 0000 1000 1010 1011 0111 0010
///ROUND 12///
Key12: 0101 1011 0010 1100 1011 0101 0100 1100 1001 1111 1001 0100
R12 expanded to 48bits: 0001 0101 0110 1000 0101 0001 0101 0101 0110 1011 1010 0100
R12 XOR with Key12: 0100 1110 0100 0100 1110 0100 0001 1001 1111 0100 0011 0000
R12 apply SBOXes: 0110 0111 1000 1001 0001 1000 0011 0000
R12 in IP table: 1111 0010 0000 0000 1100 0111 0101 0000
R12 XOR with L11: 1101 0110 1111 0001 0011 0000 0110 1110
L12: 0010 1011 0000 1000 1010 1011 0111 0010
R12: 1101 0110 1111 0001 0011 0000 0110 1110
///ROUND 13///
Key13: 1101 1101 1010 1100 1010 1100 1001 1001 0110 0100 1111 1101
R13 expanded to 48bits: 0110 1010 1101 0111 1010 0010 1001 1010 0000 0011 0101 1101
R13 XOR with Key13: 1011 0111 0111 1011 0000 1110 0000 0011 0110 0111 1010 0000
R13 apply SBOXes: 0001 1100 0011 1010 0010 1010 0001 0111
R13 in IP table: 0001 0110 0110 1010 0000 1000 1111 0110
R13 XOR with L12: 0011 1101 0110 0010 1010 0011 1000 0100
L13: 1101 0110 1111 0001 0011 0000 0110 1110
R13: 0011 1101 0110 0010 1010 0011 1000 0100
///ROUND 14///
Key14: 1101 0010 1010 0110 1010 1110 0110 1011 1101 1010 1000 0001
R14 expanded to 48bits: 0001 1111 1010 1011 0000 0101 0101 0000 0111 1100 0000 1000
R14 XOR with Key14: 1100 1101 0000 1101 1010 1011 0011 1011 1010 0110 1000 1001
R14 apply SBOXes: 1011 1001 1100 0001 0110 1101 1010 1010
R14 in IP table: 1001 1000 1000 1111 0110 0111 1000 1011
R14 XOR with L13: 0100 1110 0111 1110 0101 0111 1110 0101
L14: 0011 1101 0110 0010 1010 0011 1000 0100
R14: 0100 1110 0111 1110 0101 0111 1110 0101
///ROUND 15///
Key15: 1111 1000 1001 1110 0010 0110 1001 0010 0110 0101 0011 1111
R15 expanded to 48bits: 1010 0101 1100 0011 1111 1100 0010 1010 1111 1111 0000 1010
R15 XOR with Key15: 0101 1101 0101 1101 1101 1010 1011 1000 1001 1010 0011 0101
R15 apply SBOXes: 1011 0001 0011 1100 1000 0111 1100 1001
R15 in IP table: 0000 1101 1011 0000 0111 1010 0100 1111
R15 XOR with L14: 0011 0000 1101 0010 1101 1001 1100 1011
L15: 0100 1110 0111 1110 0101 0111 1110 0101
R15: 0011 0000 1101 0010 1101 1001 1100 1011
///ROUND 16///
Key16: 1111 0001 1011 1110 0010 0010 1011 0101 0101 1101 0001 0111
R16 expanded to 48bits: 1001 1010 0001 0110 1010 0101 0110 1111 0011 1110 0101 0110
R16 XOR with Key16: 0110 1011 1010 1000 1000 0111 1101 1010 0110 0011 0100 0001
R16 apply SBOXes: 1001 0011 0110 0101 0101 0101 0001 0001
R16 in IP table: 1110 0010 1000 0101 0111 1000 0000 1110
R16 XOR with L15: 1010 1100 1111 1011 0010 1111 1110 1011
L16: 0011 0000 1101 0010 1101 1001 1100 1011
R16: 1010 1100 1111 1011 0010 1111 1110 1011
---Block final permutation: 00011111 00110111 01000100 01011111 10111000 11010101 00111011 01111011
```

РОЗШИФРУВАННЯ

```
---DEC-Block: 00110010 01011000 10010010 10001110 01010110 10001111 01111110 10011010
L0: 0011 0010 0101 1000 1001 0010 1000 1110
R0: 0101 0110 1000 1111 0111 1110 1001 1010
///ROUND 1///
Key1: 1111 0001 1011 1110 0010 1110 0101 0100 0000 0010 0111 1101
R1 expanded to 48bits: 0010 1010 1101 0100 0101 1110 1011 1111 1101 0100 1111 0100
R1 XOR with Key1: 1101 1011 0110 1010 0111 0000 1110 1011 1101 0110 1000 1001
R1 apply SBOXes: 0111 0110 0110 1111 0011 1000 1010 1010
R1 in IP table: 1111 1000 0100 0011 1001 0110 1101 0111
R1 XOR with L0: 1100 1010 0001 1011 0000 0100 0101 1001
L1: 0101 0110 1000 1111 0111 1110 1001 1010
R1: 1100 1010 0001 1011 0000 0100 0101 1001
///ROUND 2///
Key2: 1111 1001 1011 1110 1010 0110 0001 1001 1010 1001 0100 0000
R2 expanded to 48bits: 1110 0101 0100 0000 1111 0110 1000 0000 1000 0010 1111 0011
R2 XOR with Key2: 0001 1100 1111 1110 0101 0000 1001 1001 0010 1011 1011 0011
R2 apply SBOXes: 0100 1110 1011 0001 1011 1101 1110 1100
R2 in IP table: 1111 1101 0001 1000 1010 0101 1011 1101
R2 XOR with L1: 1010 1011 1001 0111 1101 1011 0010 0111
L2: 1100 1010 0001 1011 0000 0100 0101 1001
R2: 1010 1011 1001 0111 1101 1011 0010 0111
///ROUND 3///
Key3: 1101 0011 1010 1110 1010 1111 0000 0111 0100 0111 0111 0000
R3 expanded to 48bits: 1101 0101 0111 1100 1010 1111 1110 1111 0110 1001 0000 1111
R3 XOR with Key3: 0000 0110 1101 0010 0000 0000 1110 1000 0010 1110 0111 1111
R3 apply SBOXes: 0000 0100 0110 0111 0011 0001 1110 1011
R3 in IP table: 1010 1000 0101 0011 0011 1100 1001 0101
R3 XOR with L2: 0110 0010 0100 1000 0011 1000 1100 1100
L3: 1010 1011 1001 0111 1101 1011 0010 0111
R3: 0110 0010 0100 1000 0011 1000 1100 1100
///ROUND 4///
Key4: 1101 1101 1010 1101 1010 1101 1001 1110 1001 1000 0001 0011
R4 expanded to 48bits: 0011 0000 0100 0010 0101 0000 0001 1111 0001 0110 0101 1000
R4 XOR with Key4: 1110 1101 1110 1111 1111 1101 1000 0001 1000 1110 0100 1011
R4 apply SBOXes: 0000 1010 1100 0010 0100 1110 1110 0011
R4 in IP table: 0101 0000 0111 1111 0000 1101 0000 1001
R4 XOR with L3: 1111 1011 1110 1000 1101 0110 0010 1110
L4: 0110 0010 0100 1000 0011 1000 1100 1100
R4: 1111 1011 1110 1000 1101 0110 0010 1110
///ROUND 5///
Key5: 0101 1011 0110 1101 1011 1101 0010 0000 0000 1110 1110 1011
R5 expanded to 48bits: 0111 1111 0111 1111 0101 0001 0110 1010 1100 0001 0101 1101
R5 XOR with Key5: 0010 0100 0001 0010 1110 1100 0100 1010 1100 1111 1011 0110
R5 apply SBOXes: 1110 0011 0100 0111 0101 1100 0010 1101
R5 in IP table: 1111 1000 1100 0101 1101 1110 0010 1000
R5 XOR with L4: 1001 1010 1000 1101 1110 0110 1110 0100
L5: 1111 1011 1110 1000 1101 0110 0010 1110
R5: 1001 1010 1000 1101 1110 0110 1110 0100
///ROUND 6///
Key6: 0001 1111 0110 1101 1100 1101 1110 0100 1111 0000 1010 0100
```

R6 expanded to 48bits: 0100 1111 0101 0100 0101 1011 1111 0000 1101 0111 0000 1001
R6 XOR with Key6: 0101 0000 0011 1001 1001 0110 0001 0100 0010 0111 1010 1101
R6 apply SBOXes: 0110 1101 1001 0101 0010 0001 0001 1000
R6 in IP table: 1000 1110 0000 1000 1111 0011 1001 0000
R6 XOR with L5: 0111 0101 1110 0000 0010 0101 1011 1110
L6: 1001 1010 1000 1101 1110 0110 1110 0100
R6: 0111 0101 1110 0000 0010 0101 1011 1110
///ROUND 7///
Key7: 0011 1111 0111 1001 1101 1101 0000 1000 0011 0000 0100 1110
R7 expanded to 48bits: 0011 1010 1011 1111 0000 0000 0001 0000 1011 1101 1111 1100
R7 XOR with Key7: 0000 0101 1100 0110 1101 1101 0001 1000 1000 1101 1011 0010
R7 apply SBOXes: 0000 0101 1011 1110 0001 1001 1000 0110
R7 in IP table: 0011 0100 0100 0010 0111 0001 0111 0101
R7 XOR with L6: 1010 1110 1100 1111 1001 0111 1001 0001
L7: 0111 0101 1110 0000 0010 0101 1011 1110
R7: 1010 1110 1100 1111 1001 0111 1001 0001
///ROUND 8///
Key8: 0001 1111 0101 1011 1101 1011 0111 0101 0100 0101 0000 1000
R8 expanded to 48bits: 1101 0101 1101 0110 0101 1111 1100 1010 1111 1100 1010 0011
R8 XOR with Key8: 1100 1010 1000 1101 1000 0100 1011 1111 1011 1001 1010 1011
R8 apply SBOXes: 1100 1010 1100 1110 1101 0000 1101 1010
R8 in IP table: 0110 1011 1101 1111 1001 0001 0100 0001
R8 XOR with L7: 0001 1110 0011 1111 1011 0100 1111 1111
L8: 1010 1110 1100 1111 1001 0111 1001 0001
R8: 0001 1110 0011 1111 1011 0100 1111 1111
///ROUND 9///
Key9: 1011 1111 0101 1001 1101 1011 1000 0000 1000 0011 0110 1111
R9 expanded to 48bits: 1000 1111 1100 0001 1111 1111 1101 1010 1001 0111 1111 1110
R9 XOR with Key9: 0011 0000 1001 1000 0010 0100 0101 1010 0001 0100 1001 0001
R9 apply SBOXes: 1011 1111 1101 1001 1111 0100 1100 1100
R9 in IP table: 1110 1101 1001 1101 0100 0011 1111 1011
R9 XOR with L8: 0100 0011 0101 0010 1101 0100 0110 1010
L9: 0001 1110 0011 1111 1011 0100 1111 1111
R9: 0100 0011 0101 0010 1101 0100 0110 1010
///ROUND 10///
Key10: 0010 1111 1101 0011 1111 1011 1110 0111 0001 0000 1100 0000
R10 expanded to 48bits: 0010 0000 0110 1010 1010 0101 0110 1010 1000 0011 0101 0100
R10 XOR with Key10: 0000 1111 1011 1001 0101 1110 1000 1101 1001 0011 1001 0100
R10 apply SBOXes: 1111 0101 1101 1111 1000 0000 1101 0011
R10 in IP table: 1000 0111 1101 0011 1101 1011 0101 0011
R10 XOR with L9: 1001 1001 1110 1100 0110 1111 1010 1100
L10: 0100 0011 0101 0010 1101 0100 0110 1010
R10: 1001 1001 1110 1100 0110 1111 1010 1100
///ROUND 11///
Key11: 1110 1111 1101 0011 0101 1011 0000 0101 0110 0000 0001 1111
R11 expanded to 48bits: 0100 1111 0011 1111 0101 1000 0011 0101 1111 1101 0101 1001
R11 XOR with Key11: 1010 0000 1110 1100 0000 0011 0011 0000 1001 1101 0100 0110
R11 apply SBOXes: 1101 0100 1011 1000 1011 0111 0000 0100
R11 in IP table: 0010 0101 1010 0000 1010 0001 1111 1110
R11 XOR with L10: 0110 0110 1111 0010 0111 0101 1001 0100
L11: 1001 1001 1110 1100 0110 1111 1010 1100
R11: 0110 0110 1111 0010 0111 0101 1001 0100

```
///ROUND 12///
Key12: 1110 1110 1101 0111 0111 0111 0110 1000 0100 1001 1001 0010
R12 expanded to 48bits: 0011 0000 1101 0111 1010 0100 0011 1010 1011 1100 1010 1000
R12 XOR with Key12: 1101 1110 0000 0000 1101 0011 0101 0010 1111 0101 0011 1010
R12 apply SBOXes: 1110 0000 0111 0111 0011 1010 1001 0011
R12 in IP table: 1011 0110 1110 0011 1001 1010 1000 0101
R12 XOR with L11: 0010 1111 0000 1111 1111 0101 0010 1001
L12: 0110 0110 1111 0010 0111 0101 1001 0100
R12: 0010 1111 0000 1111 1111 0101 0010 1001
///ROUND 13///
Key13: 1110 0110 1111 0111 0111 0010 0011 1011 0010 1100 0010 0100
R13 expanded to 48bits: 1001 0101 1110 1000 0101 1111 1111 1010 1010 1001 0101 0010
R13 XOR with Key13: 0111 0011 0001 1111 0010 1101 1100 0001 1000 0101 0111 0110
R13 apply SBOXes: 0000 1011 1110 1101 1111 1110 0101 1101
R13 in IP table: 1111 1011 0011 1101 0101 1001 1110 1100
R13 XOR with L12: 1001 1101 1100 1111 0010 1100 0111 1000
L13: 0010 1111 0000 1111 1111 0101 0010 1001
R13: 1001 1101 1100 1111 0010 1100 0111 1000
///ROUND 14///
Key14: 1111 0100 1111 1110 0111 0110 0000 0000 1011 0111 0011 0001
R14 expanded to 48bits: 0100 1111 1011 1110 0101 1110 1001 0101 1000 0011 1111 0001
R14 XOR with Key14: 1011 1011 0100 0000 0010 1000 1001 0101 0011 0100 1100 0000
R14 apply SBOXes: 1011 1100 1010 1100 1100 0001 0011 1101
R14 in IP table: 0000 1011 1000 1100 0011 1111 0111 0110
R14 XOR with L13: 0010 0100 1000 0011 1100 1010 0101 1111
L14: 1001 1101 1100 1111 0010 1100 0111 1000
R14: 0010 0100 1000 0011 1100 1010 0101 1111
///ROUND 15///
Key15: 1110 0000 1011 1110 1111 0110 1001 0011 1001 1000 1100 1000
R15 expanded to 48bits: 1001 0000 1001 0100 0000 0111 1110 0101 0100 0010 1111 1110
R15 XOR with Key15: 0111 0000 0010 1010 1111 0001 0111 0110 1101 1010 0011 0110
R15 apply SBOXes: 0000 0001 1001 1001 1000 1111 1100 1101
R15 in IP table: 1001 1101 0011 0000 0110 1001 0110 1001
R15 XOR with L14: 0000 0000 1111 1111 0100 0101 0001 0001
L15: 0010 0100 1000 0011 1100 1010 0101 1111
R15: 0000 0000 1111 1111 0100 0101 0001 0001
///ROUND 16///
Key16: 1111 0000 1011 1110 1110 1110 1110 0000 1100 0100 0001 0100
R16 expanded to 48bits: 1000 0000 0001 0111 1111 1110 1010 0000 1010 1000 1010 0010
R16 XOR with Key16: 0111 0000 1010 1001 0001 0000 0100 0000 0110 1100 1011 0110
R16 apply SBOXes: 0000 1011 0100 0001 1000 1111 1111 1101
R16 in IP table: 1101 1011 0011 1001 0110 1100 0010 1001
R16 XOR with L15: 1111 1111 1011 1010 1010 0110 0111 0110
L16: 0000 0000 1111 1111 0100 0101 0001 0001
R16: 1111 1111 1011 1010 1010 0110 0111 0110
---Block final permutation: 01101010 01110101 01101101 01110000 01110011 01110101 01101001 01110100

---DEC-Block: 11011111 01101000 00110101 01011010 10111111 10011110 10111100 01100100
L0: 1101 1111 0110 1000 0011 0101 0101 1010
R0: 1011 1111 1001 1110 1011 1100 0110 0100
///ROUND 1///
Key1: 1111 0001 1011 1110 0010 1110 0101 0100 0000 0010 0111 1101
```

R1 expanded to 48bits: 0101 1111 1111 1100 1111 1101 0101 1111 1000 0011 0000 1001
R1 XOR with Key1: 1010 1110 0100 0010 1101 0011 0000 1011 1000 0001 0111 0100
R1 apply SBOXes: 1001 0111 0100 0111 1100 0001 1011 1010
R1 in IP table: 1100 1011 1100 0111 0111 0100 0001 0011
R1 XOR with L0: 0001 0100 1010 1111 0100 0001 0100 1001
L1: 1011 1111 1001 1110 1011 1100 0110 0100
R1: 0001 0100 1010 1111 0100 0001 0100 1001
///ROUND 2///
Key2: 1111 1001 1011 1110 1010 0110 0001 1001 1010 1001 0100 0000
R2 expanded to 48bits: 1000 1010 1001 0101 0101 1110 1010 0000 0010 1010 0101 0010
R2 XOR with Key2: 0111 0011 0010 1011 1111 1000 1011 1001 1000 0011 0001 0010
R2 apply SBOXes: 0000 1000 0111 0101 1000 1110 1000 1001
R2 in IP table: 1001 1101 0010 1001 0001 1000 0000 1101
R2 XOR with L1: 0010 0010 1011 0111 1010 0100 0110 1001
L2: 0001 0100 1010 1111 0100 0001 0100 1001
R2: 0010 0010 1011 0111 1010 0100 0110 1001
///ROUND 3///
Key3: 1101 0011 1010 1110 1010 1111 0000 0111 0100 0111 0111 0000
R3 expanded to 48bits: 1001 0000 0101 0101 1010 1111 1101 0000 1000 0011 0101 0010
R3 XOR with Key3: 0100 0011 1111 1011 0000 0000 1101 0111 1100 0100 0010 0010
R3 apply SBOXes: 0011 1001 0011 0111 0000 1011 0011 1011
R3 in IP table: 1001 1110 0110 1010 0111 1110 0000 0110
R3 XOR with L2: 1000 1010 1100 0101 0011 1111 0100 1111
L3: 0010 0010 1011 0111 1010 0100 0110 1001
R3: 1000 1010 1100 0101 0011 1111 0100 1111
///ROUND 4///
Key4: 1101 1101 1010 1101 1010 1101 1001 1110 1001 1000 0001 0011
R4 expanded to 48bits: 1100 0101 0101 0110 0000 1010 1001 1111 1110 1010 0101 1111
R4 XOR with Key4: 0001 1000 1111 1011 1010 0111 0000 0001 0111 0010 0100 1100
R4 apply SBOXes: 0001 1110 0000 0110 0010 1110 0100 1011
R4 in IP table: 0101 1000 0111 1010 0001 1000 1001 1010
R4 XOR with L3: 0111 1010 1100 1101 1011 1100 1111 0011
L4: 1000 1010 1100 0101 0011 1111 0100 1111
R4: 0111 1010 1100 1101 1011 1100 1111 0011
///ROUND 5///
Key5: 0101 1011 0110 1101 1011 1101 0010 0000 0000 1110 1110 1011
R5 expanded to 48bits: 1011 1111 0101 0110 0101 1011 1101 1111 1001 0111 1010 0110
R5 XOR with Key5: 1110 0100 0011 1011 1110 0110 1111 1111 1001 1001 0100 1101
R5 apply SBOXes: 1010 1101 0111 0000 0011 0110 1101 0111
R5 in IP table: 0010 0110 1011 1011 0100 1010 1011 1101
R5 XOR with L4: 1010 1100 0111 1110 0111 0101 1111 0010
L5: 0111 1010 1100 1101 1011 1100 1111 0011
R5: 1010 1100 0111 1110 0111 0101 1111 0010
///ROUND 6///
Key6: 0001 1111 0110 1101 1100 1101 1110 0100 1111 0000 1010 0100
R6 expanded to 48bits: 0101 0101 1000 0011 1111 1100 0011 1010 1011 1111 1010 0101
R6 XOR with Key6: 0100 1010 1110 1110 0011 0001 1101 1110 0100 1111 0000 0001
R6 apply SBOXes: 1010 0001 0101 1001 1001 1111 1001 0001
R6 in IP table: 1011 0111 1010 0001 0110 1010 0100 1001
R6 XOR with L5: 1100 1101 0110 1100 1101 0110 1011 1010
L6: 1010 1100 0111 1110 0111 0101 1111 0010
R6: 1100 1101 0110 1100 1101 0110 1011 1010

```
///ROUND 7///
Key7: 0011 1111 0111 1001 1101 1101 0000 1000 0011 0000 0100 1110
R7 expanded to 48bits: 0110 0101 1010 1011 0101 1001 0110 1010 1101 0101 1111 0101
R7 XOR with Key7: 0101 1010 1101 0010 1000 0100 0110 0010 1110 0101 1011 1011
R7 apply SBOXes: 1100 0100 0011 1110 1101 0011 0111 0101
R7 in IP table: 0010 0111 1111 0100 1011 1100 0111 0100
R7 XOR with L6: 1000 1011 1000 1010 1100 1001 1000 0110
L7: 1100 1101 0110 1100 1101 0110 1011 1010
R7: 1000 1011 1000 1010 1100 1001 1000 0110
///ROUND 8///
Key8: 0001 1111 0101 1011 1101 1011 0111 0101 0100 0101 0000 1000
R8 expanded to 48bits: 0100 0101 0111 1100 0101 0101 0110 0101 0011 1100 0000 1101
R8 XOR with Key8: 0101 1010 0010 0111 1000 1110 0001 0000 0111 1001 0000 0101
R8 apply SBOXes: 1100 1110 1000 1010 0100 0010 1011 1101
R8 in IP table: 0100 1010 1110 1100 1000 1101 0111 0001
R8 XOR with L7: 1000 0111 1000 0000 0101 1011 1100 1011
L8: 1000 1011 1000 1010 1100 1001 1000 0110
R8: 1000 0111 1000 0000 0101 1011 1100 1011
///ROUND 9///
Key9: 1011 1111 0101 1001 1101 1011 1000 0000 1000 0011 0110 1111
R9 expanded to 48bits: 1100 0000 1111 1100 0000 0000 0010 1111 0111 1110 0101 0111
R9 XOR with Key9: 0111 1111 1010 0101 1101 1011 1010 1111 1111 1101 0011 1000
R9 apply SBOXes: 1000 0011 1110 1010 1110 1101 0110 1111
R9 in IP table: 0101 1001 1101 0111 0110 1101 1110 1100
R9 XOR with L8: 1101 0010 0101 1101 1010 0100 0110 1010
L9: 1000 0111 1000 0000 0101 1011 1100 1011
R9: 1101 0010 0101 1101 1010 0100 0110 1010
///ROUND 10///
Key10: 0010 1111 1101 0011 1111 1011 1110 0111 0001 0000 1100 0000
R10 expanded to 48bits: 0110 1010 0100 0010 1111 1011 1101 0000 1000 0011 0101 0101
R10 XOR with Key10: 0100 0101 1001 0001 0000 0000 0011 0111 1001 0011 1001 0101
R10 apply SBOXes: 1010 0110 1001 0111 1101 0110 1101 0110
R10 in IP table: 1110 0111 1111 0110 0001 0011 0011 1001
R10 XOR with L9: 0110 0000 0111 0110 0100 1000 1111 0010
L10: 1101 0010 0101 1101 1010 0100 0110 1010
R10: 0110 0000 0111 0110 0100 1000 1111 0010
///ROUND 11///
Key11: 1110 1111 1101 0011 0101 1011 0000 0101 0110 0000 0001 1111
R11 expanded to 48bits: 0011 0000 0000 0011 1010 1100 0010 0101 0001 0111 1010 0100
R11 XOR with Key11: 1101 1111 1101 0000 1111 0111 0010 0000 0111 0111 1011 1011
R11 apply SBOXes: 1110 1110 0111 1011 0111 0010 0001 0101
R11 in IP table: 1110 0110 1110 1101 1000 1010 1111 0100
R11 XOR with L10: 0011 0100 1011 0000 0010 1110 1001 1110
L11: 0110 0000 0111 0110 0100 1000 1111 0010
R11: 0011 0100 1011 0000 0010 1110 1001 1110
///ROUND 12///
Key12: 1110 1110 1101 0111 0111 0111 0110 1000 0100 1001 1001 0010
R12 expanded to 48bits: 0001 1010 1001 0101 1010 0000 0001 0101 1101 0100 1111 1100
R12 XOR with Key12: 1111 0100 0100 0010 1101 0111 0111 1101 1001 1101 0110 1110
R12 apply SBOXes: 0110 1000 0100 1100 0110 0000 0000 0010
R12 in IP table: 0000 0000 0000 1111 1001 0010 1100 0000
R12 XOR with L11: 0110 0000 0111 1001 1101 1010 0011 0010
```

L12: 0011 0100 1011 0000 0010 1110 1001 1110
R12: 0110 0000 0111 1001 1101 1010 0011 0010
///ROUND 13///
Key13: 1110 0110 1111 0111 0111 0010 0011 1011 0010 1100 0010 0100
R13 expanded to 48bits: 0011 0000 0000 0011 1111 0011 1110 1111 0100 0001 1010 0100
R13 XOR with Key13: 1101 0110 1111 0100 1000 0001 1101 0100 0110 1101 1000 0000
R13 apply SBOXes: 0011 0010 1101 1101 0000 1111 1000 1101
R13 in IP table: 1101 1100 0010 0001 0011 1011 0110 1011
R13 XOR with L12: 1110 1000 1001 0001 0001 0101 1111 0101
L13: 0110 0000 0111 1001 1101 1010 0011 0010
R13: 1110 1000 1001 0001 0001 0101 1111 0101
///ROUND 14///
Key14: 1111 0100 1111 1110 0111 0110 0000 0000 1011 0111 0011 0001
R14 expanded to 48bits: 1111 0101 0001 0100 1010 0010 1000 1010 1011 1111 1010 1011
R14 XOR with Key14: 0000 0001 1110 1010 1101 0100 1000 1010 0000 1000 1001 1010
R14 apply SBOXes: 1110 1010 1001 1000 0010 1001 0100 0000
R14 in IP table: 0101 0100 1001 1000 1010 0011 1100 0000
R14 XOR with L13: 0011 0100 1110 0001 0111 1001 1111 0010
L14: 1110 1000 1001 0001 0001 0101 1111 0101
R14: 0011 0100 1110 0001 0111 1001 1111 0010
///ROUND 15///
Key15: 1110 0000 1011 1110 1111 0110 1001 0011 1001 1000 1100 1000
R15 expanded to 48bits: 0001 1010 1001 0111 0000 0010 1011 1111 0011 1111 1010 0100
R15 XOR with Key15: 1111 1010 0010 1001 1111 0100 0010 1100 1010 0111 0110 1100
R15 apply SBOXes: 0000 1110 0000 0011 0111 0010 1000 1110
R15 in IP table: 1110 1000 0110 1110 0000 0000 1011 0001
R15 XOR with L14: 0000 0000 1111 1111 0001 0101 0100 0100
L15: 0011 0100 1110 0001 0111 1001 1111 0010
R15: 0000 0000 1111 1111 0001 0101 0100 0100
///ROUND 16///
Key16: 1111 0000 1011 1110 1110 1110 1110 0000 1100 0100 0001 0100
R16 expanded to 48bits: 0000 0000 0001 0111 1111 1110 1000 1010 1010 1010 0000 1000
R16 XOR with Key16: 1111 0000 1010 1001 0001 0000 0110 1010 0110 1110 0001 1100
R16 apply SBOXes: 0101 1011 0100 0001 0000 0101 0000 1100
R16 in IP table: 1100 1000 0000 1001 1110 0000 0010 1010
R16 XOR with L15: 1111 1100 1110 1000 1001 1001 1101 1000
L16: 0000 0000 1111 1111 0001 0101 0100 0100
R16: 1111 1100 1110 1000 1001 1001 1101 1000
---Block final permutation: 00101100 00100000 01101010 01110101 01101101 01110000 01110011 01110101

---DEC-Block: 00001111 10101011 00010110 00001101 01001100 10100101 00111101 00110101
L0: 0000 1111 1010 1011 0001 0110 0000 1101
R0: 0100 1100 1010 0101 0011 1101 0011 0101
///ROUND 1///
Key1: 1111 0001 1011 1110 0010 1110 0101 0100 0000 0010 0111 1101
R1 expanded to 48bits: 1010 0101 1001 0101 0000 1010 1001 1111 1010 1001 1010 1010
R1 XOR with Key1: 0101 0100 0010 1011 0010 0100 1100 1011 1010 1011 1101 0111
R1 apply SBOXes: 1100 0001 0011 1001 1001 1101 0111 1011
R1 in IP table: 1011 1111 1001 0010 1110 1100 0100 1100
R1 XOR with L0: 1011 0000 0011 1001 1111 1010 0100 0001
L1: 0100 1100 1010 0101 0011 1101 0011 0101
R1: 1011 0000 0011 1001 1111 1010 0100 0001

```
///ROUND 2///
Key2: 1111 1001 1011 1110 1010 0110 0001 1001 1010 1001 0100 0000
R2 expanded to 48bits: 1101 1010 0000 0001 1111 0011 1111 1111 0100 0010 0000 0011
R2 XOR with Key2: 0010 0011 1011 1111 0101 0101 1110 0110 1110 1011 0100 0011
R2 apply SBOXes: 0010 0101 0010 0010 1010 0011 1010 1111
R2 in IP table: 0000 1001 0110 0010 0110 1110 1011 0101
R2 XOR with L1: 0100 0101 1100 0111 0101 0011 1000 0000
L2: 1011 0000 0011 1001 1111 1010 0100 0001
R2: 0100 0101 1100 0111 0101 0011 1000 0000
///ROUND 3///
Key3: 1101 0011 1010 1110 1010 1111 0000 0111 0100 0111 0111 0000
R3 expanded to 48bits: 0010 0000 1011 1110 0000 1110 1010 1010 0111 1100 0000 0000
R3 XOR with Key3: 1111 0011 0001 0000 1010 0001 1010 1101 0011 1011 0111 0000
R3 apply SBOXes: 0101 1011 0000 0011 1110 0001 1010 0000
R3 in IP table: 1100 0001 0100 1100 1110 0100 1000 0011
R3 XOR with L2: 0111 0001 0111 0101 0001 1110 1100 0010
L3: 0100 0101 1100 0111 0101 0011 1000 0000
R3: 0111 0001 0111 0101 0001 1110 1100 0010
///ROUND 4///
Key4: 1101 1101 1010 1101 1010 1101 1001 1110 1001 1000 0001 0011
R4 expanded to 48bits: 0011 1010 0010 1011 1010 1010 1000 1111 1101 0110 0000 0100
R4 XOR with Key4: 1110 0111 1000 0110 0000 0111 0001 0001 0100 1110 0001 0111
R4 apply SBOXes: 1010 1001 1011 0101 0100 0011 0000 1011
R4 in IP table: 1000 1100 1010 1110 0111 1011 0000 0100
R4 XOR with L3: 1100 1001 0110 1001 0010 1000 1000 0100
L4: 0111 0001 0111 0101 0001 1110 1100 0010
R4: 1100 1001 0110 1001 0010 1000 1000 0100
///ROUND 5///
Key5: 0101 1011 0110 1101 1011 1101 0010 0000 0000 1110 1110 1011
R5 expanded to 48bits: 0110 0101 0010 1011 0101 0010 1001 0101 0001 0100 0000 1001
R5 XOR with Key5: 0011 1110 0100 0110 1110 1111 1011 0101 0001 1010 1110 0010
R5 apply SBOXes: 0001 0111 1011 1000 0010 0110 0100 1011
R5 in IP table: 0100 1100 0011 0010 0100 1001 1101 1110
R5 XOR with L4: 0011 1101 0100 0111 0101 0111 0001 1100
L5: 1100 1001 0110 1001 0010 1000 1000 0100
R5: 0011 1101 0100 0111 0101 0111 0001 1100
///ROUND 6///
Key6: 0001 1111 0110 1101 1100 1101 1110 0100 1111 0000 1010 0100
R6 expanded to 48bits: 0001 1111 1010 1010 0000 1110 1010 1010 1110 1000 1111 1000
R6 XOR with Key6: 0000 0000 1100 0111 1100 0011 0100 1110 0001 1000 0101 1100
R6 apply SBOXes: 1110 0011 0001 1000 0000 0100 0110 1100
R6 in IP table: 0100 1100 1001 0000 1100 0110 0110 1000
R6 XOR with L5: 1000 0101 1111 1001 1110 1110 1110 1100
L6: 0011 1101 0100 0111 0101 0111 0001 1100
R6: 1000 0101 1111 1001 1110 1110 1110 1100
///ROUND 7///
Key7: 0011 1111 0111 1001 1101 1101 0000 1000 0011 0000 0100 1110
R7 expanded to 48bits: 0100 0000 1011 1111 1111 0011 1111 0101 1101 0111 0101 1001
R7 XOR with Key7: 0111 1111 1100 0110 0010 1110 1111 1101 1110 0111 0001 0111
R7 apply SBOXes: 1000 0010 1011 1101 0011 1011 0110 1011
R7 in IP table: 1111 1100 1011 0010 0011 1101 1100 0100
R7 XOR with L6: 1100 0001 1111 0101 0110 1010 1101 1000
```

L7: 1000 0101 1111 1001 1110 1110 1110 1100
R7: 1100 0001 1111 0101 0110 1010 1101 1000
///ROUND 8///
Key8: 0001 1111 0101 1011 1101 1011 0111 0101 0100 0101 0000 1000
R8 expanded to 48bits: 0110 0000 0011 1111 1010 1010 1011 0101 0101 0110 1111 0001
R8 XOR with Key8: 0111 1111 0110 0100 0111 0001 1100 0000 0001 0011 1111 1001
R8 apply SBOXes: 1000 0110 0010 1001 1111 1010 1010 0011
R8 in IP table: 1111 0001 1010 0110 0000 1100 1101 0101
R8 XOR with L7: 0111 0100 0101 1111 1110 0010 0011 1001
L8: 1100 0001 1111 0101 0110 1010 1101 1000
R8: 0111 0100 0101 1111 1110 0010 0011 1001
///ROUND 9///
Key9: 1011 1111 0101 1001 1101 1011 1000 0000 1000 0011 0110 1111
R9 expanded to 48bits: 1011 1010 1000 0010 1111 1111 1111 0000 0100 0001 1111 0010
R9 XOR with Key9: 0000 0101 1101 1011 0010 0100 0111 0000 1100 0010 1001 1101
R9 apply SBOXes: 0000 1011 0011 1001 1110 0110 0000 1001
R9 in IP table: 1100 1101 0010 1100 0100 1000 1100 1100
R9 XOR with L8: 0000 1100 1101 1001 0010 0010 0001 0100
L9: 0111 0100 0101 1111 1110 0010 0011 1001
R9: 0000 1100 1101 1001 0010 0010 0001 0100
///ROUND 10///
Key10: 0010 1111 1101 0011 1111 1011 1110 0111 0001 0000 1100 0000
R10 expanded to 48bits: 0000 0101 1001 0110 1111 0010 1001 0000 0100 0000 1010 1000
R10 XOR with Key10: 0010 1010 0100 0101 0000 1001 0111 0111 0101 0000 0110 1000
R10 apply SBOXes: 1111 0111 1100 0110 1000 0001 1101 1001
R10 in IP table: 0100 1011 1101 0001 1111 1011 0001 0011
R10 XOR with L9: 0011 1111 1000 1110 0001 1001 0010 1010
L10: 0000 1100 1101 1001 0010 0010 0001 0100
R10: 0011 1111 1000 1110 0001 1001 0010 1010
///ROUND 11///
Key11: 1110 1111 1101 0011 0101 1011 0000 0101 0110 0000 0001 1111
R11 expanded to 48bits: 0001 1111 1111 1100 0101 1100 0000 1111 0010 1001 0101 0100
R11 XOR with Key11: 1111 0000 0010 1111 0000 0111 0000 1010 0100 1001 0100 1011
R11 apply SBOXes: 0101 0001 1110 0101 1100 1111 1101 0011
R11 in IP table: 1001 0011 0011 0111 1111 1001 0000 1111
R11 XOR with L10: 1001 1111 1110 1110 1101 1011 0001 1011
L11: 0011 1111 1000 1110 0001 1001 0010 1010
R11: 1001 1111 1110 1110 1101 1011 0001 1011
///ROUND 12///
Key12: 1110 1110 1101 0111 0111 0111 0110 1000 0100 1001 1001 0010
R12 expanded to 48bits: 1100 1111 1111 1111 0101 1101 0110 1111 0110 1000 1111 0111
R12 XOR with Key12: 0010 0001 0010 1000 0010 1010 0000 0111 0010 0001 0110 0101
R12 apply SBOXes: 0010 0111 1101 1011 1110 0000 1011 1110
R12 in IP table: 1100 1111 0100 0111 0100 0111 1111 0001
R12 XOR with L11: 1111 0000 1100 1001 0101 1110 1101 1011
L12: 1001 1111 1110 1110 1101 1011 0001 1011
R12: 1111 0000 1100 1001 0101 1110 1101 1011
///ROUND 13///
Key13: 1110 0110 1111 0111 0111 0010 0011 1011 0010 1100 0010 0100
R13 expanded to 48bits: 1111 1010 0001 0110 0101 0010 1010 1111 1101 0110 1111 0111
R13 XOR with Key13: 0001 1100 1110 0001 0010 0000 1001 0100 1111 1010 1101 0011
R13 apply SBOXes: 0100 0100 1001 1010 1100 0101 0100 0101

R13 in IP table: 0000 0101 0101 0100 1010 1001 0111 1000
R13 XOR with L12: 1001 1010 1011 1010 0111 0010 0110 0011
L13: 1111 0000 1100 1001 0101 1110 1101 1011
R13: 1001 1010 1011 1010 0111 0010 0110 0011
///ROUND 14///
Key14: 1111 0100 1111 1110 0111 0110 0000 0000 1011 0111 0011 0001
R14 expanded to 48bits: 1100 1111 0101 0101 1111 0100 0011 1010 0100 0011 0000 0111
R14 XOR with Key14: 0011 1011 1010 1011 1000 0010 0011 1010 1111 0100 0011 0110
R14 apply SBOXes: 1000 0011 0000 1101 0110 1010 0011 1101
R14 in IP table: 1101 1010 1010 0100 0101 1100 1110 0000
R14 XOR with L13: 0010 1010 0110 1101 0000 0010 0011 1011
L14: 1001 1010 1011 1010 0111 0010 0110 0011
R14: 0010 1010 0110 1101 0000 0010 0011 1011
///ROUND 15///
Key15: 1110 0000 1011 1110 1111 0110 1001 0011 1001 1000 1100 1000
R15 expanded to 48bits: 1001 0101 0100 0011 0101 1010 1000 0000 0100 0001 1111 0110
R15 XOR with Key15: 0111 0101 1111 1101 1010 1100 0001 0011 1101 1001 0011 1110
R15 apply SBOXes: 0011 0101 1100 0111 0100 1000 1011 1000
R15 in IP table: 1001 1010 0100 0101 0101 0111 0001 0011
R15 XOR with L14: 0000 0000 1111 1111 0010 0101 0111 0000
L15: 0010 1010 0110 1101 0000 0010 0011 1011
R15: 0000 0000 1111 1111 0010 0101 0111 0000
///ROUND 16///
Key16: 1111 0000 1011 1110 1110 1110 1110 0000 1100 0100 0001 0100
R16 expanded to 48bits: 0000 0000 0001 0111 1111 1110 1001 0000 1010 1011 1010 0000
R16 XOR with Key16: 1111 0000 1010 1001 0001 0000 0111 0000 0110 1111 1011 0100
R16 apply SBOXes: 0101 1011 0100 0001 1110 1111 0010 1010
R16 in IP table: 1101 1001 0010 1111 1110 0100 1000 1010
R16 XOR with L15: 1111 0011 0100 0010 1110 0110 1011 0001
L16: 0000 0000 1111 1111 0010 0101 0111 0000
R16: 1111 0011 0100 0010 1110 0110 1011 0001
---Block final permutation: 01101001 01110100 00101100 00100000 01100011 01101111 01110110 01100101

---DEC-Block: 01000111 10110010 10100100 10010111 11111101 10101011 01001001 11110001
L0: 0100 0111 1011 0010 1010 0100 1001 0111
R0: 1111 1101 1010 1011 0100 1001 1111 0001
///ROUND 1///
Key1: 1111 0001 1011 1110 0010 1110 0101 0100 0000 0010 0111 1101
R1 expanded to 48bits: 1111 1111 1011 1101 0101 0110 1010 0101 0011 1111 1010 0011
R1 XOR with Key1: 0000 1110 0000 0011 0111 1000 1111 0001 0011 1101 1101 1110
R1 apply SBOXes: 1111 0000 0110 0101 0000 0001 1111 0111
R1 in IP table: 1000 0010 1001 0011 1011 1110 0010 0111
R1 XOR with L0: 1100 0101 0010 0001 0001 1010 1011 0000
L1: 1111 1101 1010 1011 0100 1001 1111 0001
R1: 1100 0101 0010 0001 0001 1010 1011 0000
///ROUND 2///
Key2: 1111 1001 1011 1110 1010 0110 0001 1001 1010 1001 0100 0000
R2 expanded to 48bits: 0110 0000 1010 1001 0000 0010 1000 1111 0101 0101 1010 0001
R2 XOR with Key2: 1001 1001 0001 0111 1010 0100 1001 0110 1111 1100 1110 0001
R2 apply SBOXes: 1000 1100 1000 1001 1100 1010 0101 0010
R2 in IP table: 1001 0011 1011 1110 0000 0001 0101 0000
R2 XOR with L1: 0110 1110 0001 0101 0100 1000 1010 0001

L2: 1100 0101 0010 0001 0001 1010 1011 0000
R2: 0110 1110 0001 0101 0100 1000 1010 0001
///ROUND 3///
Key3: 1101 0011 1010 1110 1010 1111 0000 0111 0100 0111 0111 0000
R3 expanded to 48bits: 1011 0101 1100 0000 1010 1010 1010 0101 0001 0101 0000 0010
R3 XOR with Key3: 0110 0110 0110 1110 0000 0101 1010 0010 0101 0010 0111 0010
R3 apply SBOXes: 1001 1011 0101 1011 1010 0010 0100 0110
R3 in IP table: 1100 0101 1111 1011 0100 0000 1110 0010
R3 XOR with L2: 0000 0000 1101 1010 0101 1010 0101 0010
L3: 0110 1110 0001 0101 0100 1000 1010 0001
R3: 0000 0000 1101 1010 0101 1010 0101 0010
///ROUND 4///
Key4: 1101 1101 1010 1101 1010 1101 1001 1110 1001 1000 0001 0011
R4 expanded to 48bits: 0000 0000 0001 0110 1111 0100 0010 1111 0100 0010 1010 0100
R4 XOR with Key4: 1101 1101 1011 1011 0101 1001 1011 0001 1101 1010 1011 0111
R4 apply SBOXes: 1110 1001 1000 0001 0111 0011 0011 0000
R4 in IP table: 1010 0010 1010 1100 1110 0111 1000 0000
R4 XOR with L3: 1100 1100 1011 1001 1010 1111 0010 0001
L4: 0000 0000 1101 1010 0101 1010 0101 0010
R4: 1100 1100 1011 1001 1010 1111 0010 0001
///ROUND 5///
Key5: 0101 1011 0110 1101 1011 1101 0010 0000 0000 1110 1110 1011
R5 expanded to 48bits: 1110 0101 1001 0101 1111 0011 1101 0101 1110 1001 0000 0011
R5 XOR with Key5: 1011 1110 1111 1000 0100 1110 1111 0101 1110 0111 1110 1000
R5 apply SBOXes: 0111 0010 0001 1010 0101 1011 0110 1001
R5 in IP table: 0111 1100 0111 0100 1010 1110 0100 0010
R5 XOR with L4: 0111 1100 1010 1110 1111 0100 0001 0000
L5: 1100 1100 1011 1001 1010 1111 0010 0001
R5: 0111 1100 1010 1110 1111 0100 0001 0000
///ROUND 6///
Key6: 0001 1111 0110 1101 1100 1101 1110 0100 1111 0000 1010 0100
R6 expanded to 48bits: 0011 1111 1001 0101 0101 1101 0111 1010 1000 0000 1010 0000
R6 XOR with Key6: 0010 0000 1111 1000 1001 0000 1001 1110 0111 0000 0000 0100
R6 apply SBOXes: 0010 1110 0110 0001 0111 1100 0100 1000
R6 in IP table: 1111 1000 0001 1101 0000 0010 1001 1100
R6 XOR with L5: 0011 0100 1010 0100 1010 1101 1011 1101
L6: 0111 1100 1010 1110 1111 0100 0001 0000
R6: 0011 0100 1010 0100 1010 1101 1011 1101
///ROUND 7///
Key7: 0011 1111 0111 1001 1101 1101 0000 1000 0011 0000 0100 1110
R7 expanded to 48bits: 1001 1010 1001 0101 0000 1001 0101 0101 1011 1101 1111 1010
R7 XOR with Key7: 1010 0101 1110 1100 1101 0100 0101 1101 1000 1101 1011 0100
R7 apply SBOXes: 0100 1010 1111 1000 1010 1110 1000 1010
R7 in IP table: 0101 1101 0010 1011 1000 0001 1100 1101
R7 XOR with L6: 0010 0001 1000 0101 0111 0101 1101 1101
L7: 0011 0100 1010 0100 1010 1101 1011 1101
R7: 0010 0001 1000 0101 0111 0101 1101 1101
///ROUND 8///
Key8: 0001 1111 0101 1011 1101 1011 0111 0101 0100 0101 0000 1000
R8 expanded to 48bits: 1001 0000 0011 1100 0000 1010 1011 1010 1011 1110 1111 1010
R8 XOR with Key8: 1000 1111 0110 0111 1101 0001 1100 1111 1111 1011 1111 0010
R8 apply SBOXes: 1100 0110 0001 0100 1111 1101 0111 0110

R8 in IP table: 0111 0111 1001 0110 1011 0100 1011 1000
R8 XOR with L7: 0100 0011 0011 0010 0001 1001 0000 0101
L8: 0010 0001 1000 0101 0111 0101 1101 1101
R8: 0100 0011 0011 0010 0001 1001 0000 0101
///ROUND 9///
Key9: 1011 1111 0101 1001 1101 1011 1000 0000 1000 0011 0110 1111
R9 expanded to 48bits: 1010 0000 0110 1001 1010 0100 0000 1111 0010 1000 0000 1010
R9 XOR with Key9: 0001 1111 0011 0000 0111 1111 1000 1111 1010 1011 0110 0101
R9 apply SBOXes: 0100 0110 1101 1110 1000 1101 1010 1110
R9 in IP table: 0101 1101 0100 0011 1011 0101 0111 1001
R9 XOR with L8: 0111 1100 1100 0110 1100 0000 1010 0100
L9: 0100 0011 0011 0010 0001 1001 0000 0101
R9: 0111 1100 1100 0110 1100 0000 1010 0100
///ROUND 10///
Key10: 0010 1111 1101 0011 1111 1011 1110 0111 0001 0000 1100 0000
R10 expanded to 48bits: 0011 1111 1001 0110 0000 1101 0110 0000 0001 0101 0000 1000
R10 XOR with Key10: 0001 0000 0100 0101 1111 0110 1000 0111 0000 0101 1100 1000
R10 apply SBOXes: 1101 1000 1110 1110 1011 0111 1100 0110
R10 in IP table: 0010 0001 1111 1011 1011 0001 1110 1111
R10 XOR with L9: 0110 0010 1100 1001 1010 1000 1110 1010
L10: 0111 1100 1100 0110 1100 0000 1010 0100
R10: 0110 0010 1100 1001 1010 1000 1110 1010
///ROUND 11///
Key11: 1110 1111 1101 0011 0101 1011 0000 0101 0110 0000 0001 1111
R11 expanded to 48bits: 0011 0000 0101 0110 0101 0011 1101 0101 0001 0111 0101 0100
R11 XOR with Key11: 1101 1111 1000 0101 0000 1000 1101 0000 0111 0111 0100 1011
R11 apply SBOXes: 1110 1001 1100 0000 1100 0010 1000 0011
R11 in IP table: 0000 0001 1010 1111 1100 1011 0000 0001
R11 XOR with L10: 0111 1101 0110 1001 0000 1011 1010 0101
L11: 0110 0010 1100 1001 1010 1000 1110 1010
R11: 0111 1101 0110 1001 0000 1011 1010 0101
///ROUND 12///
Key12: 1110 1110 1101 0111 0111 0111 0110 1000 0100 1001 1001 0010
R12 expanded to 48bits: 1011 1111 1010 1011 0101 0010 1000 0101 0111 1101 0000 1010
R12 XOR with Key12: 0101 0001 0111 1100 0010 0101 1110 1101 0011 0100 1001 1000
R12 apply SBOXes: 0110 1010 1011 0000 0100 0001 1100 0101
R12 in IP table: 0100 0100 0001 1100 1010 1011 0010 0101
R12 XOR with L11: 0010 0110 1101 0101 0000 0011 1100 1111
L12: 0111 1101 0110 1001 0000 1011 1010 0101
R12: 0010 0110 1101 0101 0000 0011 1100 1111
///ROUND 13///
Key13: 1110 0110 1111 0111 0111 0010 0011 1011 0010 1100 0010 0100
R13 expanded to 48bits: 1001 0000 1101 0110 1010 1010 1000 0000 0111 1110 0101 1110
R13 XOR with Key13: 0111 0110 0010 0001 1101 1000 1011 1011 0101 0010 0111 1010
R13 apply SBOXes: 0011 1110 1001 1011 1000 0001 0100 0011
R13 in IP table: 1100 0101 0101 1010 0010 1011 0101 0010
R13 XOR with L12: 1011 1000 0011 0011 0010 0000 1111 0111
L13: 0010 0110 1101 0101 0000 0011 1100 1111
R13: 1011 1000 0011 0011 0010 0000 1111 0111
///ROUND 14///
Key14: 1111 0100 1111 1110 0111 0110 0000 0000 1011 0111 0011 0001
R14 expanded to 48bits: 1101 1111 0000 0001 1010 0110 1001 0000 0001 0111 1010 1111

R14 XOR with Key14: 0010 1011 1111 1111 1101 0000 1001 0000 1010 0000 1001 1110

R14 apply SBOXes: 1111 1001 1100 0001 0001 0010 1011 0111

R14 in IP table: 1010 0010 1010 1011 1100 1111 0010 0011

R14 XOR with L13: 1000 0100 0111 1110 1100 1100 1110 1100

L14: 1011 1000 0011 0011 0010 0000 1111 0111

R14: 1000 0100 0111 1110 1100 1100 1110 1100

///ROUND 15///

Key15: 1110 0000 1011 1110 1111 0110 1001 0011 1001 1000 1100 1000

R15 expanded to 48bits: 0100 0000 1000 0011 1111 1101 0110 0101 1001 0111 0101 1001

R15 XOR with Key15: 1010 0000 0011 1101 0000 1011 1111 0110 0000 1111 1001 0001

R15 apply SBOXes: 1101 1101 0010 1111 0101 1001 0010 1100

R15 in IP table: 1011 1000 1100 1100 1111 0100 0111 0110

R15 XOR with L14: 0000 0000 1111 1111 1101 0100 1000 0001

L15: 1000 0100 0111 1110 1100 1100 1110 1100

R15: 0000 0000 1111 1111 1101 0100 1000 0001

///ROUND 16///

Key16: 1111 0000 1011 1110 1110 1110 1110 0000 1100 0100 0001 0100

R16 expanded to 48bits: 1000 0000 0001 0111 1111 1111 1110 1010 1001 0100 0000 0010

R16 XOR with Key16: 0111 0000 1010 1001 0001 0001 0000 1010 0101 0000 0001 0110

R16 apply SBOXes: 0000 1011 0100 0100 1100 0010 0100 1110

R16 in IP table: 0100 1001 0011 1111 0101 0000 0010 0000

R16 XOR with L15: 1100 1101 0100 0001 1001 1100 1100 1100

L16: 0000 0000 1111 1111 1101 0100 1000 0001

R16: 1100 1101 0100 0001 1001 1100 1100 1100

---Block final permutation: 01110010 00100000 01101101 01100101 00101100 00100000 01111001 01101111