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: | Керівник: |
| студент групи КМ-01 | *ст. викладач Бай Ю. П.* |
| *Дюбакін Р. С.* |  |

Київ — 2022

ЗМІСТ

[Постановка задачі 2](#_Toc100571354)

[Основні теоретичні відомості зі стандарту шифрування DES 3](#_Toc100571355)

[Контрольний приклад 4](#_Toc100571356)

[Шифрування тексту 5](#_Toc100571357)

[Розшифрування тексту 5](#_Toc100571358)

[Відповіді на контрольні запитання 5](#_Toc100571359)

[Список літератури 6](#_Toc100571360)

[Додаток 1 7](#_Toc100571361)

[Додаток 2 8](#_Toc100571362)

***Мета роботи:*** опрацювати загальну послідовність алгоритму DES, розробити криптосистему на основі стандарту шифрування DES, дослідити особливості алгоритму: нелінійні блоки, лавиновий ефект, режими роботи.

# Постановка задачі

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

Контрольний приклад:

<https://courses.cs.washington.edu/courses/cse467/99au/admin/Slides/Week6Lecture1/sld001.htm>. Виконати приклад в деталях. Зробити скріншоти до результатів слайдів 7, 9, 10, 11, 12, 13, 14, 15, 17, 19, 20, 21, 22, 23.

АБО

<https://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm>

Виконати приклад в деталях (від «How DES Works in Detail» до результату), зробити скріншоти до всіх проміжних результатів.

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

3. За стандартом DES зашифрувати текст довжиною від 8 до 80 символів, користуючись 64-бітним ключем.

4. Дано зашифроване за стандартом DES повідомлення довжиною від 8 до 80 символів та відомий 64-бітний ключ. Розшифрувати задане повідомлення.

5. Яка ефективна довжина ключа шифру DES?

6. Як працюють нелінійні блоки *S*1 … *S*8? Яким буде результат проходження 6-бітового блоку 111000 через блок *S*8 ?

7. Що означає лавиновий ефект? Продемонструвати лавиновий ефект при зміні одного біту на вході після трьох раундів шифрування.

8. Які існують режими роботи DES? У чому полягає режим CBC?

# 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.

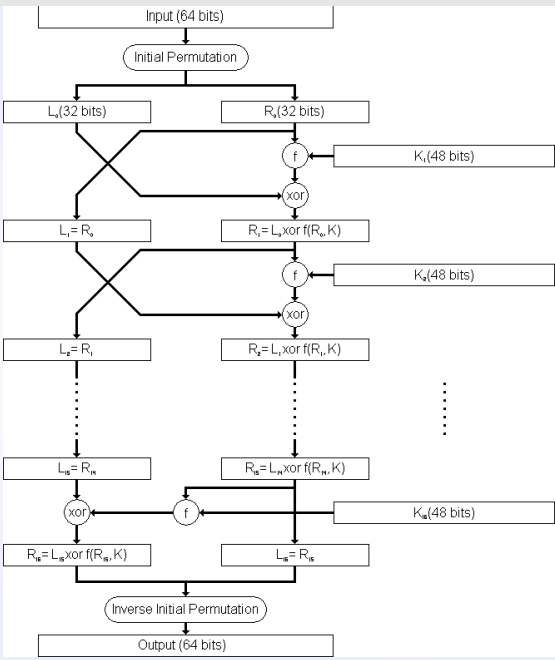
Зараз DES вважається ненадійним в оcновному через малу довжину ключа (56 біт) та розмір блоку (64 біти). У 1999 ключ DES було публічно дешифровано за 22 години 15 хвилин. Вважається, що алгоритм достатньо надійний для застосування у модифікації 3-DES, хоча існують розроблені теоретичні атаки. DES поступово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

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.

Структура DES

1. Використовується блоковий принцип шифрування, довжина блоку – 64 біт.
2. Довжина ключа – 56 біт.
3. Основа алгоритму – схема Фейстеля.
4. Кількість раундів – 16.

Малюнок 1 – Загальна структура DES

# Контрольний приклад

Plain text M = 0123456789ABCDEF, де М представлено у hex форматі. Перепишемо М у бінарний формат, отримаємо 64-бітний блок тексту:

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111,

де ліва частина L = 0000 0001 0010 0011 0100 0101 0110 0111,

права частина R = 1000 1001 1010 1011 1100 1101 1110 1111.

Візьмемо у якості hex ключа K = 133457799BBCDFF1 і перепишемо його в бінарному форматі:

К = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

**Крок 1. Створимо 16 підключів, кожен з яких має довжину 48 бітів.**

Зображення, що містить стіл

Автоматично згенерований описВихідний 64-бітний ключ K за таблицею PC-1 перетворимо на 56-бітний ключ з перестановками K+: (за таблицею першим бітом в ключі К+ буде 57 біт в К, другим в К+ буде 49 в К ключі, і так далі. )

Малюнок 2 – Таблиця PC-1



K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

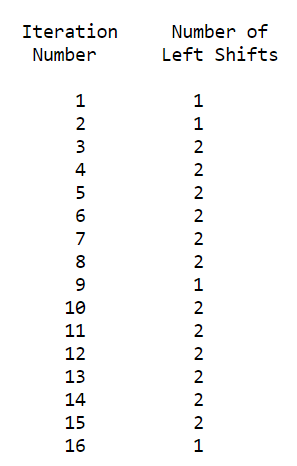


K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111



Далі розділимо ключ на ліву частину та праву частину , кожна з яких довжиною 28 біт.

Створимо далі 16 ключів, на основі зміщування на певну кількість бітів лівої частини та правої частини за таблицею:

**Малюнок 3 – Таблиця зміщень бітів вліво на кожній ітерації

C0 = 1111000011001100101010101111



C1 = 1110000110011001010101011111



D0 = 0101010101100110011110001111



D1 = 1010101011001100111100011110



C2 = 1100001100110010101010111111

D2 = 0101010110011001111000111101

C3 = 0000110011001010101011111111

D3 = 0101011001100111100011110101

C4 = 0011001100101010101111111100

D4 = 0101100110011110001111010101

C5 = 1100110010101010111111110000

D5 = 0110011001111000111101010101

C6 = 0011001010101011111111000011

D6 = 1001100111100011110101010101

C7 = 1100101010101111111100001100

D7 = 0110011110001111010101010110

C8 = 0010101010111111110000110011

D8 = 1001111000111101010101011001

C9 = 0101010101111111100001100110

D9 = 0011110001111010101010110011

C10 = 0101010111111110000110011001

D10 = 1111000111101010101011001100

C11 = 0101011111111000011001100101

D11 = 1100011110101010101100110011

C12 = 0101111111100001100110010101

D12 = 0001111010101010110011001111

C13 = 0111111110000110011001010101

D13 = 0111101010101011001100111100

C14 = 1111111000011001100101010101

D14 = 1110101010101100110011110001

C15 = 1111100001100110010101010111

D15 = 1010101010110011001111000111

C16 = 1111000011001100101010101111

D16 = 0101010101100110011110001111

*Зображення, що містить стіл

Автоматично згенерований опис*Далі об’єднуємо частини та та після перестановок за таблицею PC-2 отримуємо ключі , де 1 <= n <= 16:

Малюнок 4 – Таблиця перестановок PC-2

C1D1 = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110



K1 = 000110 110000 001011 101111 111111 000111 000001 110010



Для всіх 16 ключів маємо:

K2 = 011110 011010 111011 011001 110110 111100 100111 100101

K3 = 010101 011111 110010 001010 010000 101100 111110 011001

K4 = 011100 101010 110111 010110 110110 110011 010100 011101

K5 = 011111 001110 110000 000111 111010 110101 001110 101000

K6 = 011000 111010 010100 111110 010100 000111 101100 101111

K7 = 111011 001000 010010 110111 111101 100001 100010 111100

K8 = 111101 111000 101000 111010 110000 010011 101111 111011

K9 = 111000 001101 101111 101011 111011 011110 011110 000001

K10 = 101100 011111 001101 000111 101110 100100 011001 001111

K11 = 001000 010101 111111 010011 110111 101101 001110 000110

K12 = 011101 010111 000111 110101 100101 000110 011111 101001

K13 = 100101 111100 010111 010001 111110 101011 101001 000001

K14 = 010111 110100 001110 110111 111100 101110 011100 111010

K15 = 101111 111001 000110 001101 001111 010011 111100 001010

K16 = 110010 110011 110110 001011 000011 100001 011111 110101

**Крок 2. Шифруємо 64-бітний блок даних.**

Зображення, що містить стіл

Автоматично згенерований описРобимо первинну перестановку (initial permutation) тексту М за таблицею IP:

Малюнок 5 – Таблиця IP

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010

Ділимо IP на ліву і праву частини по 32 біти:

L0 = 1100 1100 0000 0000 1100 1100 1111 1111

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

Далі для всіх 16 ітерацій генеруємо ліву та праву частини за схемою:

**,**

**де + означає XOR операцію**

K1 = 000110 110000 001011 101111 111111 000111 000001 110010

L1 = R0 = 1111 0000 1010 1010 1111 0000 1010 1010

R1 = L0 + f(R0,K1).

**Робота функції**

Зображення, що містить стіл

Автоматично згенерований описСпочатку розширюємо від 32 до 48 бітів за таблицею Е:

Малюнок 6 – Таблиця Е розширення

Наприклад:

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

E(R0) = 011110 100001 010101 010101 011110 100001 010101 010101.

Далі ми виконуємо операцію XOR між ключем та **Е()**.

Наприклад для К1 та Е(R0):

K1 = 000110 110000 001011 101111 111111 000111 000001 110010



E(R0) = 011110 100001 010101 010101 011110 100001 010101 010101



K1+E(R0) = 011000 010001 011110 111010 100001 100110 010100 100111.



Значення  **+ Е()** складається з 8 блоків по 6 бітів:

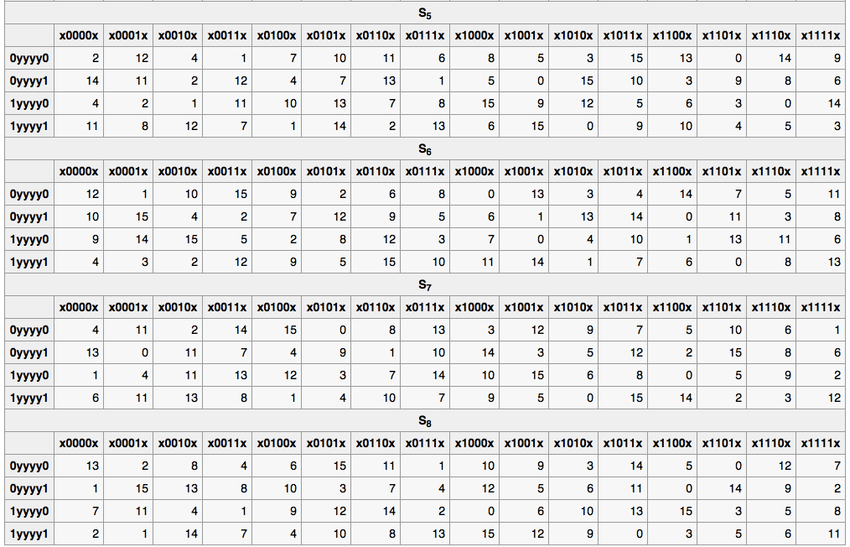
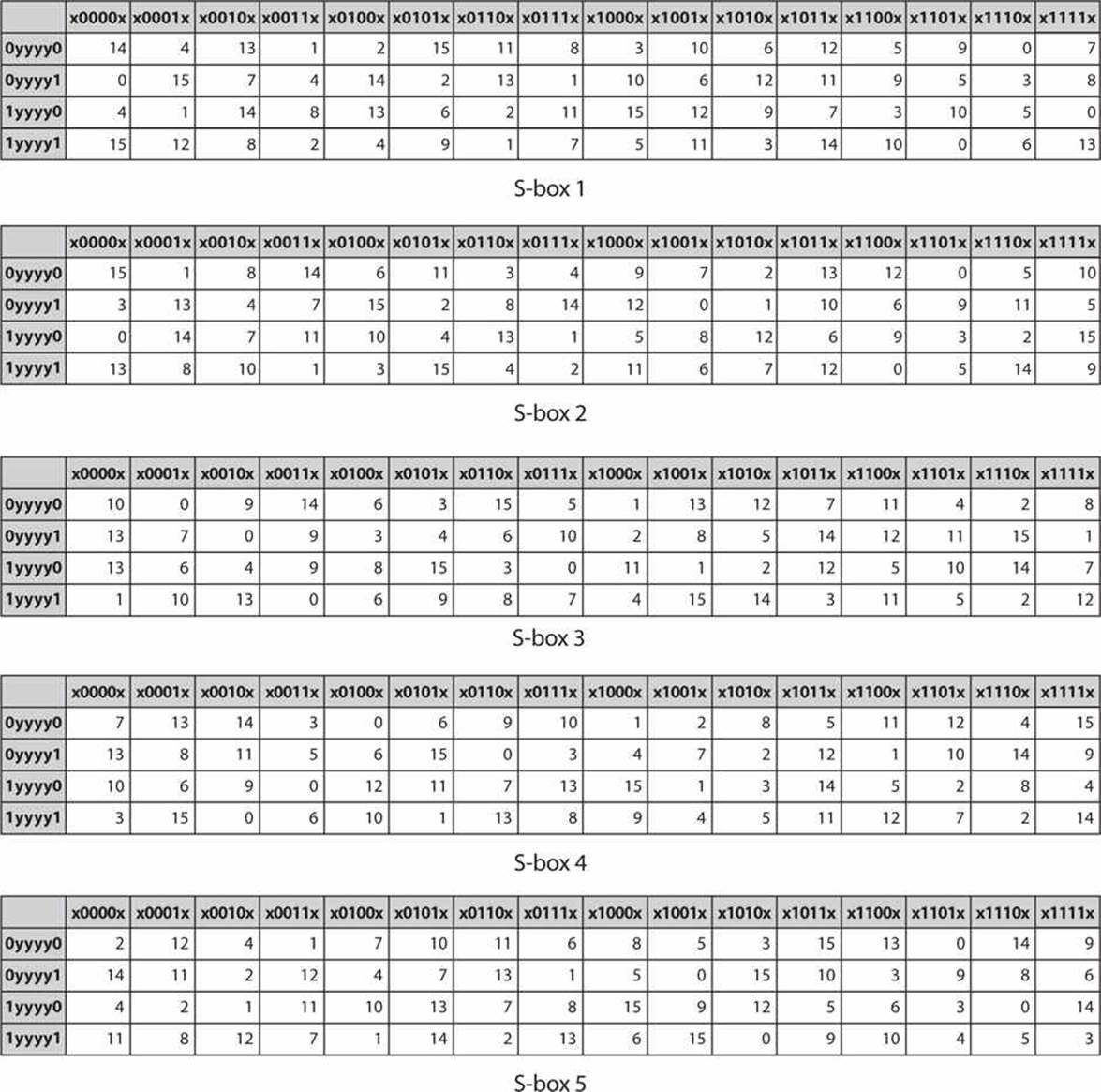
**+ Е() = ,**

Обчислемо значення

,

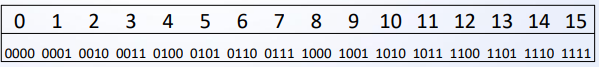
де – це результат роботи і-того S-box.

Малюнок 7 – Таблиці S-box



Приклад роботи S-box:



Зображення, що містить стіл

Автоматично згенерований описB1 = 0 1 1 0 0 0



S1(B1) = 5 = 0101

Так маємо результат для K1+E(R0):

K1+E(R0) = 011000 010001 011110 111010 100001 100110 010100 100111

= 0101 1100 1000 0010 1011 0101 1001 0111

Зображення, що містить текст

Автоматично згенерований описФінальним етапом функції f є перестановки за таблицею P:

Малюнок 8 – Таблиця перестановок P

= 0101 1100 1000 0010 1011 0101 1001 0111

f = 0010 0011 0100 1010 1010 1001 1011 1011

R1 = L0 + f(R0 , K1 ) =

= 1100 1100 0000 0000 1100 1100 1111 1111

+ 0010 0011 0100 1010 1010 1001 1011 1011

= 1110 1111 0100 1010 0110 0101 0100 0100

**Така схема повторюється 16 разів.**

В результаті останньої 16 ітерації маємо:

L16 = 0100 0011 0100 0010 0011 0010 0011 0100

R16 = 0000 1010 0100 1100 1101 1001 1001 0101

Змінюємо місцями блоки L16 та R16, отримуємо:

R16L16 = 00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100

Зображення, що містить стіл

Автоматично згенерований описВиконуємо останню перестановку за таблицею :

Малюнок 9 – Таблиця перестановок

= 10000101 11101000 00010011 01010100 00001111 00001010 10110100 00000101

У hex форматі маємо: 85E813540F0AB405.

Отже, маємо

plaintext M = 0123456789ABCDEF

та

ciphertext C = 85E813540F0AB405.

# Шифрування тексту

Зашифруємо текст

"Two wrongs don't make a right. " ,

використовуючи ключ *key* = '13 34 57 79 9B BC DF F1' (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:

CC 7F BE 00 AE 35 8E E9 B6 BF 48 89 B6 1D A1 08 04 AC 13 BD 95 86 3C F2 4D 14 15 41 16 A9 D9 4A (hex)

# Розшифрування тексту

Дано зашифроване за стандартом DES повідомлення:

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

і відомо 64-бітний ключ:

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

Розшифровуючи заданий криптотекст, одержимо:

01 23 45 67 89 AB CD EF (hex)

# Відповіді на контрольні запитання

1. Яка ефективна довжина ключа шифру DES?

Ключ має довжину 56 біт.

1. Як працюють нелінійні блоки *S*1 … *S*8? Яким буде результат проходження 6-бітового блоку 111000 через блок *S*8 ?

Для кожного із восьми блоків результати виразу  **+ Е()**  по шість бітів використовується свій відповідний нелінійний блок. Береться блок, де перший і останній біт дають значення рядку блоку, а біти, що стоять між крайніми, дають значення стовбця блоку. В перетині значення рядку та стовбця таблиці отримуємо значення результату проходження 6-бітового блоку. Така дія повторюється для всіх восьми блоків, так утворюється нове змінене значення.

1. Що означає лавиновий ефект? Продемонструвати лавиновий ефект при зміні одного біту на вході після трьох раундів шифрування.

Лавиновий ефект – значні зміни в результуючих даних за умови дуже маленької зміни даних на вході.

|  |  |  |  |
| --- | --- | --- | --- |
| *Raund* | Input block 1: 01 23 45 67 89 AB CD EF | Input block 2: 01 23 **3**5 67 89 AB CD EF | Δ (bits) |
| *IP* | L0: 11001100000000001100110011111111  R0: 11110000101010101111000010101010 | L0: 11001**0**0000000**1**001100110011111111  R0: 11110000101011101111000010101010 | 2 |
| 1 | L1: 11110000101010101111000010101010  R1: 11101111010010100110010101000100 | L1: 1111000010101**1**101111000010101010  R1: **0**1101**0**110**0**001**1**100110010101000100 | 4 |
| 2 | L2: 11101111010010100110010101000100  R2: 11001100000000010111011100001001 | L2: **0**1101**0**110**0**001**1**100110010101000100  R2: **00**001**0**00**11**00**111**10**0**11011**0**0**11**010**1**1 | 17 |
| 3 | L3: 11001100000000010111011100001001  R3: 10100010010111000000101111110100 | L3: **00**001**0**00**11**00**111**10**0**11011**0**0**11**010**1**1  R3: **0101110110**011**01**00**11**0**0**10**000**11**1**1**1**0 | 34 |

Отже, при зміні одного біта після трьох раундів ми маємо різницю в 34 біти, тобто, приблизно в половину бітів.

1. Які існують режими роботи DES? У чому полягає режим CBC?

ECB – Electronic Code-book (Електронна шифрувальна книга), CBC – Cipher Block Chaining (Зчеплення шифрованих блоків), CFB – Cipher FeedBack (Зворотний зв’язок за шифротекстом), OFB – Output FeedBack (Зворотний зв’язок за виходом).

*Опис режиму CBC:*

Вхідний блок даних для алгоритму шифрування обчислюється як XOR поточного 64-бітового блоку відкритого тексту та 64- бітового зашифрованого попереднього блоку.

# 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.
5. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації. – Вінниця: ВНТУ, 2011. – 198 с.

# Додаток 1

Текст програми, що реалізує стандарт шифрування DES

#-\*- coding: utf8 -\*-

#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\_\_':

#    key = "secret\_k"

#    text= "Hello wo"

    # text = "Two wrongs don't make a right.  " #The length of the text must be a multiple of 8

#   key\_hex =  'FE DC BA 98 76 54 32 10'

    key\_hex =  '13 34 57 79 9B BC DF F1'

    text\_hex = '01 23 35 67 89 AB CD EF'

    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, r)

    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 8 до 80 символів

0001001100110100010101110111100110011011101111001101111111110001

---ENC-Block: 11110111 00110011 11010111 01010110 00000000 11111110 11000100 11110110

L0: 1111 0111 0011 0011 1101 0111 0101 0110

R0:0000 0000 1111 1110 1100 0100 1111 0110

///ROUND 1///

Key1: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R1 expanded to 48bits: 0000 0000 0001 0111 1111 1101 0110 0000 1001 0111 1010 1100

R1 XOR with Key1: 0001 1011 0001 0101 0001 0010 1001 1100 1110 0111 1101 1110

R1 apply SBOXes: 0001 1011 1100 0010 0111 1000 0110 0111

R1 in IP table: 0111 0000 0101 1111 0100 1101 1010 0010

R1 XOR with L0: 1000 0111 0110 1100 1001 1010 1111 0100

L1: 0000 0000 1111 1110 1100 0100 1111 0110

R1: 1000 0111 0110 1100 1001 1010 1111 0100

///ROUND 2///

Key2: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R2 expanded to 48bits: 0100 0000 1110 1011 0101 1001 0100 1111 0101 0111 1010 1001

R2 XOR with Key2: 0011 1001 0100 0101 1000 0000 1001 0100 1001 1110 0100 1100

R2 apply SBOXes: 1000 0010 0111 0111 1100 0111 1110 1011

R2 in IP table: 1100 1101 1111 0111 0011 1100 0000 1101

R2 XOR with L1: 1100 1101 0000 1001 1111 1000 1111 1011

L2: 1000 0111 0110 1100 1001 1010 1111 0100

R2: 1100 1101 0000 1001 1111 1000 1111 1011

///ROUND 3///

Key3: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R3 expanded to 48bits: 1110 0101 1010 1000 0101 0011 1111 1111 0001 0111 1111 0111

R3 XOR with Key3: 1011 0000 0101 0100 1101 1001 1011 1101 1101 1000 0110 1110

R3 apply SBOXes: 0010 0100 1000 0001 1101 0011 0110 0010

R3 in IP table: 1010 0001 0011 0110 0010 0111 0001 0000

R3 XOR with L2: 0010 0110 0101 1010 1011 1101 1110 0100

L3: 1100 1101 0000 1001 1111 1000 1111 1011

R3: 0010 0110 0101 1010 1011 1101 1110 0100

///ROUND 4///

Key4: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R4 expanded to 48bits: 0001 0000 1100 0010 1111 0101 0101 1111 1011 1111 0000 1000

R4 XOR with Key4: 0110 0010 0110 1111 0010 0011 1000 0100 1000 1010 0001 0101

R4 apply SBOXes: 0101 1011 1110 1111 1011 1001 1100 0110

R4 in IP table: 1111 0001 0101 1011 1111 0001 1110 0111

R4 XOR with L3: 0011 1100 0101 0010 0000 1001 0001 1100

L4: 0010 0110 0101 1010 1011 1101 1110 0100

R4: 0011 1100 0101 0010 0000 1001 0001 1100

///ROUND 5///

Key5: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R5 expanded to 48bits: 0001 1111 1000 0010 1010 0100 0000 0101 0010 1000 1111 1000

R5 XOR with Key5: 0110 0011 0110 1110 1010 0011 1110 1110 0111 1011 0101 0000

R5 apply SBOXes: 0101 0110 1010 1111 0100 1100 1010 1010

R5 in IP table: 1101 1000 0100 0110 1001 0101 0101 1111

R5 XOR with L4: 1111 1110 0001 1100 0010 1000 1011 1011

L5: 0011 1100 0101 0010 0000 1001 0001 1100

R5: 1111 1110 0001 1100 0010 1000 1011 1011

///ROUND 6///

Key6: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R6 expanded to 48bits: 1111 1111 1100 0000 1111 1000 0001 0101 0001 0101 1111 0111

R6 XOR with Key6: 1001 1100 0110 0101 1100 0110 0100 0101 0110 1110 1101 1000

R6 apply SBOXes: 0010 1110 1110 0011 0101 0100 0010 0101

R6 in IP table: 1110 0000 0100 1101 0000 1111 0011 1100

R6 XOR with L5: 1101 1100 0001 1111 0000 0110 0010 0000

L6: 1111 1110 0001 1100 0010 1000 1011 1011

R6: 1101 1100 0001 1111 0000 0110 0010 0000

///ROUND 7///

Key7: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R7 expanded to 48bits: 0110 1111 1000 0000 1111 1110 1000 0000 1100 0001 0000 0001

R7 XOR with Key7: 1000 0011 0000 0100 0100 1001 0111 0110 1101 1001 1011 1101

R7 apply SBOXes: 0100 0101 0010 0110 1000 1111 1101 0110

R7 in IP table: 0001 0011 0111 0010 1111 0000 0011 1101

R7 XOR with L6: 1110 1101 0110 1110 1101 1000 1000 0110

L7: 1101 1100 0001 1111 0000 0110 0010 0000

R7: 1110 1101 0110 1110 1101 1000 1000 0110

///ROUND 8///

Key8: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R8 expanded to 48bits: 0111 0101 1010 1011 0101 1101 0110 1111 0001 0100 0000 1101

R8 XOR with Key8: 1000 0010 0010 0001 0110 0111 1010 1110 0010 1111 1111 0110

R8 apply SBOXes: 0100 1110 0000 0110 1110 1110 1100 1101

R8 in IP table: 0101 1001 0111 1100 1001 1000 1011 1001

R8 XOR with L7: 1000 0101 0110 0011 1001 1110 1001 1001

L8: 1110 1101 0110 1110 1101 1000 1000 0110

R8: 1000 0101 0110 0011 1001 1110 1001 1001

///ROUND 9///

Key9: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R9 expanded to 48bits: 1100 0000 1010 1011 0000 0111 1100 1111 1101 0100 1111 0011

R9 XOR with Key9: 0010 0000 0111 0000 1110 1100 0010 0010 0011 0011 0111 0010

R9 apply SBOXes: 0010 0111 0111 0111 0111 0011 0001 0110

R9 in IP table: 1110 0110 0110 0111 0111 0010 1011 0100

R9 XOR with L8: 0000 1011 0000 1001 1010 1010 0011 0010

L9: 1000 0101 0110 0011 1001 1110 1001 1001

R9: 0000 1011 0000 1001 1010 1010 0011 0010

///ROUND 10///

Key10: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R10 expanded to 48bits: 0000 0101 0110 1000 0101 0011 1101 0101 0100 0001 1010 0100

R10 XOR with Key10: 1011 0100 1001 1011 0001 0100 0110 1111 0000 0111 1110 1011

R10 apply SBOXes: 0001 1111 0011 1000 1001 0111 0110 1010

R10 in IP table: 0110 1101 0011 1010 0110 0100 0101 1110

R10 XOR with L9: 1110 1000 0101 1001 1111 1010 1100 0111

L10: 0000 1011 0000 1001 1010 1010 0011 0010

R10: 1110 1000 0101 1001 1111 1010 1100 0111

///ROUND 11///

Key11: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R11 expanded to 48bits: 1111 0101 0000 0010 1111 0011 1111 1111 0101 0110 0000 1111

R11 XOR with Key11: 1101 0100 0101 1101 0010 0000 0010 0001 1000 0101 1000 1001

R11 apply SBOXes: 0011 0100 0010 1010 0111 1110 0111 1010

R11 in IP table: 0011 1010 0111 0110 0000 0110 1101 1110

R11 XOR with L10: 0011 0001 0111 1111 1010 1100 1110 1100

L11: 1110 1000 0101 1001 1111 1010 1100 0111

R11: 0011 0001 0111 1111 1010 1100 1110 1100

///ROUND 12///

Key12: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R12 expanded to 48bits: 0001 1010 0010 1011 1111 1111 1101 0101 1001 0111 0101 1000

R12 XOR with Key12: 0110 1111 0101 1010 0000 1010 0100 0001 1111 0000 1011 0001

R12 apply SBOXes: 0101 0111 1000 0110 1000 1000 1011 1111

R12 in IP table: 0101 1011 0100 0010 1101 1101 0011 0011

R12 XOR with L11: 1011 0011 0001 1011 0010 0111 1111 0100

L12: 0011 0001 0111 1111 1010 1100 1110 1100

R12: 1011 0011 0001 1011 0010 0111 1111 0100

///ROUND 13///

Key13: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R13 expanded to 48bits: 0101 1010 0110 1000 1111 0110 1001 0000 1111 1111 1010 1001

R13 XOR with Key13: 1100 1101 1010 1101 0010 0111 0110 1010 0100 0101 1110 1000

R13 apply SBOXes: 1011 0000 0010 0110 0000 1111 1100 1001

R13 in IP table: 0001 1000 1111 0000 0011 1010 0000 1111

R13 XOR with L12: 0010 1001 1000 1111 1001 0110 1110 0011

L13: 1011 0011 0001 1011 0010 0111 1111 0100

R13: 0010 1001 1000 1111 1001 0110 1110 0011

///ROUND 14///

Key14: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R14 expanded to 48bits: 1001 0101 0011 1100 0101 1111 1100 1010 1101 0111 0000 0110

R14 XOR with Key14: 1100 1010 0111 1111 1110 1000 0011 1000 0011 0000 0011 1100

R14 apply SBOXes: 1100 0001 1100 1100 0110 1111 0100 0101

R14 in IP table: 0001 0000 1011 0101 1111 1001 1110 1000

R14 XOR with L13: 1010 0011 1010 1110 1101 1110 0001 1100

L14: 0010 1001 1000 1111 1001 0110 1110 0011

R14: 1010 0011 1010 1110 1101 1110 0001 1100

///ROUND 15///

Key15: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R15 expanded to 48bits: 0101 0000 0111 1101 0101 1101 0110 1111 1100 0000 1111 1001

R15 XOR with Key15: 1110 1111 1110 1100 1101 0000 0101 0010 1111 1111 1111 0011

R15 apply SBOXes: 0000 1111 1111 0001 0011 1010 1100 1100

R15 in IP table: 1111 1100 0011 1001 0100 0001 1011 0101

R15 XOR with L14: 1101 0101 1011 0110 1101 0111 0101 0110

L15: 1010 0011 1010 1110 1101 1110 0001 1100

R15: 1101 0101 1011 0110 1101 0111 0101 0110

///ROUND 16///

Key16: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R16 expanded to 48bits: 0110 1010 1011 1101 1010 1101 0110 1010 1110 1010 1010 1101

R16 XOR with Key16: 1010 0001 1000 0000 0010 0110 0110 0100 1111 1101 0101 1000

R16 apply SBOXes: 1101 1100 1010 0000 0011 0101 0000 0101

R16 in IP table: 0010 0000 1000 1000 1010 1001 1011 1110

R16 XOR with L15: 1000 0011 0010 0110 0111 0111 1010 0010

L16: 1101 0101 1011 0110 1101 0111 0101 0110

R16: 1000 0011 0010 0110 0111 0111 1010 0010

---Block final permutation: 11001100 01111111 10111110 00000000 10101110 00110101 10001110 11101001

---ENC-Block: 10111011 10000010 11111001 01010011 00000000 11111111 00110000 01110011

L0: 1011 1011 1000 0010 1111 1001 0101 0011

R0:0000 0000 1111 1111 0011 0000 0111 0011

///ROUND 1///

Key1: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R1 expanded to 48bits: 1000 0000 0001 0111 1111 1110 1001 1010 0000 0011 1010 0110

R1 XOR with Key1: 1001 1011 0001 0101 0001 0001 0110 0110 0111 0011 1101 0100

R1 apply SBOXes: 1000 1011 1100 0100 0011 1100 1010 0011

R1 in IP table: 0111 0000 1000 1011 0101 1101 1000 1001

R1 XOR with L0: 1100 1011 0000 1001 1010 0100 1101 1010

L1: 0000 0000 1111 1111 0011 0000 0111 0011

R1: 1100 1011 0000 1001 1010 0100 1101 1010

///ROUND 2///

Key2: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R2 expanded to 48bits: 0110 0101 0110 1000 0101 0011 1101 0000 1001 0110 1111 0101

R2 XOR with Key2: 0001 1100 1100 0110 1000 1010 0000 1011 0101 1111 0001 0000

R2 apply SBOXes: 0100 0011 0100 0110 1100 0001 1001 1010

R2 in IP table: 0100 1011 0100 0111 1111 0000 0000 0001

R2 XOR with L1: 0100 1011 1011 1000 1100 0000 0111 0010

L2: 1100 1011 0000 1001 1010 0100 1101 1010

R2: 0100 1011 1011 1000 1100 0000 0111 0010

///ROUND 3///

Key3: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R3 expanded to 48bits: 0010 0101 0111 1101 1111 0001 0110 0000 0000 0011 1010 0100

R3 XOR with Key3: 0111 0000 1000 0001 0111 1011 0010 0010 1100 1100 0011 1101

R3 apply SBOXes: 0000 0110 0000 0111 0111 1100 1010 0110

R3 in IP table: 1111 0000 0100 0110 0001 0100 1011 1001

R3 XOR with L2: 0011 1011 0100 1111 1011 0000 0110 0011

L3: 0100 1011 1011 1000 1100 0000 0111 0010

R3: 0011 1011 0100 1111 1011 0000 0110 0011

///ROUND 4///

Key4: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R4 expanded to 48bits: 1001 1111 0110 1010 0101 1111 1101 1010 0000 0011 0000 0110

R4 XOR with Key4: 1110 1101 1100 0111 1000 1001 0000 0001 0011 0110 0001 1011

R4 apply SBOXes: 0000 0101 1000 0110 0010 0001 0101 1110

R4 in IP table: 0000 1010 0101 0010 0111 0001 1011 0000

R4 XOR with L3: 0100 0001 1110 1010 1011 0001 1100 0010

L4: 0011 1011 0100 1111 1011 0000 0110 0011

R4: 0100 0001 1110 1010 1011 0001 1100 0010

///ROUND 5///

Key5: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R5 expanded to 48bits: 0010 0000 0011 1111 0101 0101 0101 1010 0011 1110 0000 0100

R5 XOR with Key5: 0101 1100 1101 0011 0101 0010 1011 0001 0110 1101 1010 1100

R5 apply SBOXes: 1011 1000 0110 0010 0111 0100 1000 1110

R5 in IP table: 0010 1000 1100 1111 0000 0010 1010 1111

R5 XOR with L4: 0001 0011 1000 0000 1011 0010 1100 1100

L5: 0100 0001 1110 1010 1011 0001 1100 0010

R5: 0001 0011 1000 0000 1011 0010 1100 1100

///ROUND 6///

Key6: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R6 expanded to 48bits: 0000 1010 0111 1100 0000 0001 0101 1010 0101 0110 0101 1000

R6 XOR with Key6: 0110 1001 1101 1001 0011 1111 0000 1010 0010 1101 0111 0111

R6 apply SBOXes: 1001 1011 0100 1110 1100 1110 0000 0000

R6 in IP table: 0101 0001 1110 1101 0101 0000 0100 1010

R6 XOR with L5: 0001 0000 0000 0111 1110 0001 1000 1000

L6: 0001 0011 1000 0000 1011 0010 1100 1100

R6: 0001 0000 0000 0111 1110 0001 1000 1000

///ROUND 7///

Key7: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R7 expanded to 48bits: 0000 1010 0000 0000 0000 1111 1111 0000 0011 1100 0101 0000

R7 XOR with Key7: 1110 0110 1000 0100 1011 1000 0000 0110 0010 0100 1110 1100

R7 apply SBOXes: 1010 1010 1101 0101 1110 1110 0011 1110

R7 in IP table: 1101 1111 1010 1111 0001 0111 1010 1000

R7 XOR with L6: 1100 1100 0010 1111 1010 0101 0110 0100

L7: 0001 0000 0000 0111 1110 0001 1000 1000

R7: 1100 1100 0010 1111 1010 0101 0110 0100

///ROUND 8///

Key8: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R8 expanded to 48bits: 0110 0101 1000 0001 0101 1111 1101 0000 1010 1011 0000 1001

R8 XOR with Key8: 1001 0010 0000 1011 0110 0101 0001 0001 1001 0000 1111 0010

R8 apply SBOXes: 1110 0000 1000 0000 0100 0000 0000 0110

R8 in IP table: 0000 0000 1000 0110 1000 0011 0010 0000

R8 XOR with L7: 0001 0000 1000 0001 0110 0010 1010 1000

L8: 1100 1100 0010 1111 1010 0101 0110 0100

R8: 0001 0000 1000 0001 0110 0010 1010 1000

///ROUND 9///

Key9: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R9 expanded to 48bits: 0000 1010 0001 0100 0000 0010 1011 0000 0101 0101 0101 0000

R9 XOR with Key9: 1110 1010 1100 1111 1110 1001 0101 1101 1011 0010 1101 0001

R9 apply SBOXes: 1010 1101 1100 1010 1010 1011 1001 1100

R9 in IP table: 0001 1011 1110 1001 0110 0011 1111 0001

R9 XOR with L8: 1101 0111 1100 0110 1100 0110 1001 0101

L9: 0001 0000 1000 0001 0110 0010 1010 1000

R9: 1101 0111 1100 0110 1100 0110 1001 0101

///ROUND 10///

Key10: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R10 expanded to 48bits: 1110 1010 1111 1110 0000 1101 0110 0000 1101 0100 1010 1011

R10 XOR with Key10: 0101 1011 0000 1101 0100 1010 1101 1010 1001 0010 1110 0100

R10 apply SBOXes: 1100 0101 1110 0110 0101 1001 1001 0100

R10 in IP table: 0011 0010 1100 0101 1111 0001 0011 0101

R10 XOR with L9: 0010 0010 0100 0100 1001 0011 1001 1101

L10: 1101 0111 1100 0110 1100 0110 1001 0101

R10: 0010 0010 0100 0100 1001 0011 1001 1101

///ROUND 11///

Key11: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R11 expanded to 48bits: 1001 0000 0100 0010 0000 1001 0100 1010 0111 1100 1111 1010

R11 XOR with Key11: 1011 0001 0001 1101 1101 1010 1001 0100 1010 1111 0111 1100

R11 apply SBOXes: 0010 1100 0011 1100 1100 0010 0011 0101

R11 in IP table: 0000 0111 0010 1100 0001 1110 0111 0100

R11 XOR with L10: 1101 0000 1110 1010 1101 1000 1110 0001

L11: 0010 0010 0100 0100 1001 0011 1001 1101

R11: 1101 0000 1110 1010 1101 1000 1110 0001

///ROUND 12///

Key12: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R12 expanded to 48bits: 1110 1010 0001 0111 0101 0101 0110 1111 0001 0111 0000 0011

R12 XOR with Key12: 1001 1111 0110 0110 1010 0000 1111 1011 0111 0000 1110 1010

R12 apply SBOXes: 0010 0110 0100 1010 1110 0111 0000 1100

R12 in IP table: 0100 1001 0110 0101 0010 0010 1111 1000

R12 XOR with L11: 0110 1011 0010 0001 1011 0001 0110 0101

L12: 1101 0000 1110 1010 1101 1000 1110 0001

R12: 0110 1011 0010 0001 1011 0001 0110 0101

///ROUND 13///

Key13: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R13 expanded to 48bits: 1011 0101 0110 1001 0000 0011 1101 1010 0010 1011 0000 1010

R13 XOR with Key13: 0010 0010 1010 1100 1101 0010 0010 0000 1001 0001 0100 1011

R13 apply SBOXes: 0010 0100 1111 0010 0111 0111 1011 0011

R13 in IP table: 0010 0110 0110 0111 0010 1111 1001 1101

R13 XOR with L12: 1111 0110 1000 1101 1111 0111 0111 1100

L13: 0110 1011 0010 0001 1011 0001 0110 0101

R13: 1111 0110 1000 1101 1111 0111 0111 1100

///ROUND 14///

Key14: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R14 expanded to 48bits: 0111 1010 1101 0100 0101 1011 1111 1010 1110 1011 1111 1001

R14 XOR with Key14: 0010 0101 1001 0111 1110 1100 0000 1000 0000 1100 1100 0011

R14 apply SBOXes: 1110 0110 0001 0111 1100 1100 0101 1111

R14 in IP table: 1101 1111 1101 0110 1001 1010 0011 1000

R14 XOR with L13: 1011 0100 1111 0111 0010 1011 0101 1101

L14: 1111 0110 1000 1101 1111 0111 0111 1100

R14: 1011 0100 1111 0111 0010 1011 0101 1101

///ROUND 15///

Key15: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R15 expanded to 48bits: 1101 1010 1001 0111 1010 1110 1001 0101 0110 1010 1111 1011

R15 XOR with Key15: 0110 0101 0000 0110 0010 0011 1010 1000 0101 0101 1111 0001

R15 apply SBOXes: 1001 1001 1011 1111 1101 0100 1100 1111

R15 in IP table: 1010 1101 1101 1110 0101 1001 0110 1111

R15 XOR with L14: 0101 1011 0101 0011 1010 1110 0001 0011

L15: 1011 0100 1111 0111 0010 1011 0101 1101

R15: 0101 1011 0101 0011 1010 1110 0001 0011

///ROUND 16///

Key16: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R16 expanded to 48bits: 1010 1111 0110 1010 1010 0111 1101 0101 1100 0000 1010 0110

R16 XOR with Key16: 0110 0100 0101 0111 0010 1100 1101 1011 1101 0111 0101 0011

R16 apply SBOXes: 1001 0100 0010 0111 0101 1000 1000 0101

R16 in IP table: 1011 0000 1100 0100 0001 1000 0011 0111

R16 XOR with L15: 0000 0100 0011 0011 0011 0011 0110 1010

L16: 0101 1011 0101 0011 1010 1110 0001 0011

R16: 0000 0100 0011 0011 0011 0011 0110 1010

---Block final permutation: 10110110 10111111 01001000 10001001 10110110 00011101 10100001 00001000

---ENC-Block: 01011110 00000000 00010010 01011110 00000000 11111111 00001010 00001000

L0: 0101 1110 0000 0000 0001 0010 0101 1110

R0:0000 0000 1111 1111 0000 1010 0000 1000

///ROUND 1///

Key1: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R1 expanded to 48bits: 0000 0000 0001 0111 1111 1110 1000 0101 0100 0000 0101 0000

R1 XOR with Key1: 0001 1011 0001 0101 0001 0001 0111 1001 0011 0000 0010 0010

R1 apply SBOXes: 0001 1011 1100 0100 1001 0001 0100 1011

R1 in IP table: 0110 1001 0001 1011 0111 1001 0000 0010

R1 XOR with L0: 0011 0111 0001 1011 0110 1011 0101 1100

L1: 0000 0000 1111 1111 0000 1010 0000 1000

R1: 0011 0111 0001 1011 0110 1011 0101 1100

///ROUND 2///

Key2: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R2 expanded to 48bits: 0001 1010 1110 1000 1111 0110 1011 0101 0110 1010 1111 1000

R2 XOR with Key2: 0110 0011 0100 0110 0010 1111 0110 1110 1010 0011 0001 1101

R2 apply SBOXes: 0101 1100 1011 1000 1001 1000 1000 1001

R2 in IP table: 0011 1101 0000 1000 1000 1001 0101 0111

R2 XOR with L1: 0011 1101 1111 0111 1000 0011 0101 1111

L2: 0011 0111 0001 1011 0110 1011 0101 1100

R2: 0011 1101 1111 0111 1000 0011 0101 1111

///ROUND 3///

Key3: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R3 expanded to 48bits: 1001 1111 1011 1111 1010 1111 1100 0000 0110 1010 1111 1110

R3 XOR with Key3: 1100 1010 0100 0011 0010 0101 1000 0010 1010 0101 0110 0111

R3 apply SBOXes: 1100 0111 1111 0000 0100 1000 0101 0111

R3 in IP table: 0101 0110 1001 0111 1100 1001 0011 0100

R3 XOR with L2: 0110 0001 1000 1100 1010 0010 0110 1000

L3: 0011 1101 1111 0111 1000 0011 0101 1111

R3: 0110 0001 1000 1100 1010 0010 0110 1000

///ROUND 4///

Key4: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R4 expanded to 48bits: 0011 0000 0011 1100 0101 1001 0101 0000 0100 0011 0101 0000

R4 XOR with Key4: 0100 0010 1001 0001 1000 1111 1000 1011 0111 0110 0100 1101

R4 apply SBOXes: 0011 0011 1110 0011 0010 0111 0010 0111

R4 in IP table: 1100 0000 0110 0011 0110 1111 1010 1110

R4 XOR with L3: 1111 1101 1001 0100 1110 1100 1111 0001

L4: 0110 0001 1000 1100 1010 0010 0110 1000

R4: 1111 1101 1001 0100 1110 1100 1111 0001

///ROUND 5///

Key5: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R5 expanded to 48bits: 1111 1111 1011 1100 1010 1001 0111 0101 1001 0111 1010 0011

R5 XOR with Key5: 1000 0011 0101 0000 1010 1110 1001 1110 1100 0100 0000 1011

R5 apply SBOXes: 0100 0111 0000 1101 0111 1100 0011 0011

R5 in IP table: 1111 0010 0000 0110 1101 1100 1101 1000

R5 XOR with L4: 1001 0011 1000 1010 0111 1110 1011 0000

L5: 1111 1101 1001 0100 1110 1100 1111 0001

R5: 1001 0011 1000 1010 0111 1110 1011 0000

///ROUND 6///

Key6: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R6 expanded to 48bits: 0100 1010 0111 1100 0101 0100 0011 1111 1101 0101 1010 0001

R6 XOR with Key6: 0010 1001 1101 1001 0110 1010 0110 1111 1010 1110 1000 1110

R6 apply SBOXes: 1111 1011 1101 1011 1001 1101 0101 0001

R6 in IP table: 1111 0111 1101 1001 1110 1011 0100 1010

R6 XOR with L5: 0000 1010 0100 1101 0000 0111 1011 1011

L6: 1001 0011 1000 1010 0111 1110 1011 0000

R6: 0000 1010 0100 1101 0000 0111 1011 1011

///ROUND 7///

Key7: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R7 expanded to 48bits: 1000 0101 0100 0010 0101 1010 1000 0000 1111 1101 1111 0110

R7 XOR with Key7: 0110 1001 1100 0110 1110 1101 0111 0110 1110 0101 0100 1010

R7 apply SBOXes: 1001 0101 1011 1101 1000 0011 0101 1111

R7 in IP table: 1000 1111 1011 0010 0111 1001 0111 0110

R7 XOR with L6: 0001 1100 0011 1000 0000 0111 1100 0110

L7: 0000 1010 0100 1101 0000 0111 1011 1011

R7: 0001 1100 0011 1000 0000 0111 1100 0110

///ROUND 8///

Key8: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R8 expanded to 48bits: 0000 1111 1000 0001 1111 0000 0000 0000 1111 1110 0000 1100

R8 XOR with Key8: 1111 1000 0000 1011 1100 1010 1100 0001 1100 0101 1111 0111

R8 apply SBOXes: 0000 1111 0111 0110 1111 0101 1100 0000

R8 in IP table: 0110 0101 0101 1101 0111 0000 1001 1101

R8 XOR with L7: 0110 1111 0001 0000 0111 0111 0010 0110

L8: 0001 1100 0011 1000 0000 0111 1100 0110

R8: 0110 1111 0001 0000 0111 0111 0010 0110

///ROUND 9///

Key9: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R9 expanded to 48bits: 0011 0101 1110 1000 1010 0000 0011 1010 1110 1001 0000 1100

R9 XOR with Key9: 1101 0101 0011 0011 0100 1011 1101 0111 0000 1110 1000 1101

R9 apply SBOXes: 0011 0000 0110 1111 0000 0111 0101 0111

R9 in IP table: 1000 0010 0111 0011 0011 1010 0110 1110

R9 XOR with L8: 1001 1110 0100 1011 0011 1101 1010 1000

L9: 0110 1111 0001 0000 0111 0111 0010 0110

R9: 1001 1110 0100 1011 0011 1101 1010 1000

///ROUND 10///

Key10: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R10 expanded to 48bits: 0100 1111 1100 0010 0101 0110 1001 1111 1011 1101 0101 0001

R10 XOR with Key10: 1111 1110 0011 0001 0001 0001 0010 0101 1111 1011 0001 1110

R10 apply SBOXes: 1101 1000 1001 0100 0100 1000 0111 0111

R10 in IP table: 0001 0110 1001 1110 1001 1101 0010 0010

R10 XOR with L9: 0111 1001 1000 1110 1110 1010 0000 0100

L10: 1001 1110 0100 1011 0011 1101 1010 1000

R10: 0111 1001 1000 1110 1110 1010 0000 0100

///ROUND 11///

Key11: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R11 expanded to 48bits: 0011 1111 0011 1100 0101 1101 0111 0101 0100 0000 0000 1000

R11 XOR with Key11: 0001 1110 0110 0011 1000 1110 1010 1011 1001 0011 1000 1110

R11 apply SBOXes: 0100 1011 0101 1010 1101 0110 1101 0001

R11 in IP table: 0110 0111 0111 1101 1100 1000 0100 1001

R11 XOR with L10: 1111 1001 0011 0110 1111 0101 1110 0001

L11: 0111 1001 1000 1110 1110 1010 0000 0100

R11: 1111 1001 0011 0110 1111 0101 1110 0001

///ROUND 12///

Key12: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R12 expanded to 48bits: 1111 1111 0010 1001 1010 1101 0111 1010 1011 1111 0000 0011

R12 XOR with Key12: 1000 1010 0101 1000 0101 1000 1110 1110 1101 1000 1110 1010

R12 apply SBOXes: 0001 1010 0001 1011 0100 1111 1011 1100

R12 in IP table: 1101 1110 0110 1100 0010 0100 0110 1011

R12 XOR with L11: 1010 0111 1110 0010 1100 1110 0110 1111

L12: 1111 1001 0011 0110 1111 0101 1110 0001

R12: 1010 0111 1110 0010 1100 1110 0110 1111

///ROUND 13///

Key13: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R13 expanded to 48bits: 1101 0000 1111 1111 0000 0101 0110 0101 1100 0011 0101 1111

R13 XOR with Key13: 0100 0111 0011 1010 1101 0100 1001 1111 0111 1001 0001 1110

R13 apply SBOXes: 1010 0110 1001 1000 0111 0111 1011 0111

R13 in IP table: 0110 0110 1010 0110 0010 1111 1111 1001

R13 XOR with L12: 1001 1111 1001 0000 1101 1010 0001 1000

L13: 1010 0111 1110 0010 1100 1110 0110 1111

R13: 1001 1111 1001 0000 1101 1010 0001 1000

///ROUND 14///

Key14: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R14 expanded to 48bits: 0100 1111 1111 1100 1010 0001 0110 1111 0100 0000 1111 0001

R14 XOR with Key14: 0001 0000 1011 1111 0001 0110 1001 1101 1010 0111 1100 1011

R14 apply SBOXes: 1101 0010 1110 0101 0111 0111 0110 0011

R14 in IP table: 1110 0000 1011 0111 1011 1101 1000 1110

R14 XOR with L13: 0100 0111 0101 0101 0111 0011 1110 0001

L14: 1001 1111 1001 0000 1101 1010 0001 1000

R14: 0100 0111 0101 0101 0111 0011 1110 0001

///ROUND 15///

Key15: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R15 expanded to 48bits: 1010 0000 1110 1010 1010 1010 1011 1010 0111 1111 0000 0010

R15 XOR with Key15: 0001 1111 0111 1011 0010 0111 1000 0111 0100 0000 0000 1000

R15 apply SBOXes: 0100 1100 0011 0110 1011 0100 0100 0110

R15 in IP table: 0010 0101 0101 1010 1001 0000 1011 1100

R15 XOR with L14: 1011 1010 1100 1010 0100 1010 1010 0100

L15: 0100 0111 0101 0101 0111 0011 1110 0001

R15: 1011 1010 1100 1010 0100 1010 1010 0100

///ROUND 16///

Key16: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R16 expanded to 48bits: 0101 1111 0101 0110 0101 0100 0010 0101 0101 0101 0000 1001

R16 XOR with Key16: 1001 0100 0110 1011 1101 1111 0010 1011 0100 0010 1111 1100

R16 apply SBOXes: 1000 1110 0111 1001 1010 0100 1001 0101

R16 in IP table: 1100 0111 1000 1001 0000 1000 1111 1101

R16 XOR with L15: 1000 0000 1101 1100 0111 1011 0001 1100

L16: 1011 1010 1100 1010 0100 1010 1010 0100

R16: 1000 0000 1101 1100 0111 1011 0001 1100

---Block final permutation: 00000100 10101100 00010011 10111101 10010101 10000110 00111100 11110010

---ENC-Block: 00011111 00010001 00110100 00000110 00000000 11111111 00101010 00100101

L0: 0001 1111 0001 0001 0011 0100 0000 0110

R0:0000 0000 1111 1111 0010 1010 0010 0101

///ROUND 1///

Key1: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R1 expanded to 48bits: 1000 0000 0001 0111 1111 1110 1001 0101 0100 0001 0000 1010

R1 XOR with Key1: 1001 1011 0001 0101 0001 0001 0110 1001 0011 0001 0111 1000

R1 apply SBOXes: 1000 1011 1100 0100 0000 0001 1011 1111

R1 in IP table: 0100 1010 1000 1011 0111 1101 0010 0001

R1 XOR with L0: 0101 0101 1001 1010 0100 1001 0010 0111

L1: 0000 0000 1111 1111 0010 1010 0010 0101

R1: 0101 0101 1001 1010 0100 1001 0010 0111

///ROUND 2///

Key2: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R2 expanded to 48bits: 1010 1010 1011 1100 1111 0100 0010 0101 0010 1001 0000 1110

R2 XOR with Key2: 1101 0011 0001 0010 0010 1101 1111 1110 1110 0000 1110 1011

R2 apply SBOXes: 1001 1011 0110 1101 0011 0011 0000 1010

R2 in IP table: 1110 1000 1010 1011 0111 0000 1100 0110

R2 XOR with L1: 1110 1000 0101 0100 0101 1010 1110 0011

L2: 0101 0101 1001 1010 0100 1001 0010 0111

R2: 1110 1000 0101 0100 0101 1010 1110 0011

///ROUND 3///

Key3: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R3 expanded to 48bits: 1111 0101 0000 0010 1010 1000 0010 1111 0101 0111 0000 0111

R3 XOR with Key3: 1010 0000 1111 1110 0010 0010 0110 1101 1001 1000 1001 1110

R3 apply SBOXes: 1101 1110 0101 0110 1001 0000 0100 0111

R3 in IP table: 0110 0101 1101 1011 1001 1000 0011 0010

R3 XOR with L2: 0011 0000 0100 0001 1101 0001 0001 0101

L3: 1110 1000 0101 0100 0101 1010 1110 0011

R3: 0011 0000 0100 0001 1101 0001 0001 0101

///ROUND 4///

Key4: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R4 expanded to 48bits: 1001 1010 0000 0010 0000 0011 1110 1010 0010 1000 1010 1010

R4 XOR with Key4: 1110 1000 1010 1111 1101 0101 0011 0001 0001 1101 1011 0111

R4 apply SBOXes: 1010 1011 1100 0010 1011 0110 1000 0000

R4 in IP table: 0110 0001 1110 1001 0100 0011 1000 1001

R4 XOR with L3: 1000 1001 1011 1101 0001 1001 0110 1010

L4: 0011 0000 0100 0001 1101 0001 0001 0101

R4: 1000 1001 1011 1101 0001 1001 0110 1010

///ROUND 5///

Key5: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R5 expanded to 48bits: 0100 0101 0011 1101 1111 1010 1000 1111 0010 1011 0101 0101

R5 XOR with Key5: 0011 1001 1101 0001 1111 1101 0110 0100 0111 1000 1111 1101

R5 apply SBOXes: 1000 1011 1001 0010 0011 0010 1011 0110

R5 in IP table: 0110 0110 1110 1010 0100 0101 1010 0001

R5 XOR with L4: 0101 0110 1010 1011 1001 0100 1011 0100

L5: 1000 1001 1011 1101 0001 1001 0110 1010

R5: 0101 0110 1010 1011 1001 0100 1011 0100

///ROUND 6///

Key6: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R6 expanded to 48bits: 0010 1010 1101 0101 0101 0111 1100 1010 1001 0101 1010 1000

R6 XOR with Key6: 0100 1001 0111 0000 0110 1001 1001 1010 1110 1110 1000 0111

R6 apply SBOXes: 1010 1010 1101 1010 1011 0011 0101 1000

R6 in IP table: 0110 1111 1111 1001 0010 0011 1100 0000

R6 XOR with L5: 1110 0110 0100 0100 0011 1010 1010 1010

L6: 0101 0110 1010 1011 1001 0100 1011 0100

R6: 1110 0110 0100 0100 0011 1010 1010 1010

///ROUND 7///

Key7: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R7 expanded to 48bits: 0111 0000 1100 0010 0000 1000 0001 1111 0101 0101 0101 0101

R7 XOR with Key7: 1001 1100 0100 0110 1011 1111 1110 1001 0100 1101 1110 1001

R7 apply SBOXes: 0010 1000 0100 1110 0011 0011 1111 0100

R7 in IP table: 0010 0010 0111 1001 0011 0110 1110 0001

R7 XOR with L6: 0111 0100 1101 0010 1010 0010 0101 0101

L7: 1110 0110 0100 0100 0011 1010 1010 1010

R7: 0111 0100 1101 0010 1010 0010 0101 0101

///ROUND 8///

Key8: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R8 expanded to 48bits: 1011 1010 1001 0110 1010 0101 0101 0000 0100 0010 1010 1010

R8 XOR with Key8: 0100 1101 0001 1100 1001 1111 1001 0001 0111 1001 0101 0001

R8 apply SBOXes: 0110 1100 0001 1001 0001 1110 1101 1100

R8 in IP table: 1011 1110 0011 1000 1000 0010 0111 1001

R8 XOR with L7: 0101 1000 0111 1100 1011 1000 1101 0011

L8: 0111 0100 1101 0010 1010 0010 0101 0101

R8: 0101 1000 0111 1100 1011 1000 1101 0011

///ROUND 9///

Key9: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R9 expanded to 48bits: 1010 1111 0000 0011 1111 1001 0101 1111 0001 0110 1010 0110

R9 XOR with Key9: 0100 1111 1101 1000 0001 0010 1011 0010 1111 0001 0010 0111

R9 apply SBOXes: 0110 1110 1101 0010 0111 1010 0010 0111

R9 in IP table: 0111 0100 0110 1111 1000 1111 1011 0000

R9 XOR with L8: 0000 0000 1011 1101 0010 1101 1110 0101

L9: 0101 1000 0111 1100 1011 1000 1101 0011

R9: 0000 0000 1011 1101 0010 1101 1110 0101

///ROUND 10///

Key10: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R10 expanded to 48bits: 1000 0000 0001 0101 1111 1010 1001 0101 1011 1111 0000 1010

R10 XOR with Key10: 0011 0001 1110 0110 1011 1101 0010 1111 1111 1001 0100 0101

R10 apply SBOXes: 1011 1010 0100 0010 0111 1101 1101 1101

R10 in IP table: 0111 1010 1101 1101 0010 1010 1010 1011

R10 XOR with L9: 0010 0010 1010 0001 1001 0010 0111 1000

L10: 0000 0000 1011 1101 0010 1101 1110 0101

R10: 0010 0010 1010 0001 1001 0010 0111 1000

///ROUND 11///

Key11: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R11 expanded to 48bits: 0001 0000 0101 0101 0000 0011 1100 1010 0100 0011 1111 0000

R11 XOR with Key11: 0011 0001 0000 1010 1101 0000 0001 0100 1001 0000 0111 0110

R11 apply SBOXes: 1011 1001 1001 0001 0010 0111 1101 1101

R11 in IP table: 1000 1110 1011 1000 0110 1011 1010 1011

R11 XOR with L10: 1000 1110 0000 0101 0100 0110 0100 1110

L11: 0010 0010 1010 0001 1001 0010 0111 1000

R11: 1000 1110 0000 0101 0100 0110 0100 1110

///ROUND 12///

Key12: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R12 expanded to 48bits: 0100 0101 1100 0000 0000 1010 1010 0000 1100 0010 0101 1101

R12 XOR with Key12: 0011 0000 1011 0001 1111 1111 0011 0100 1010 0101 1011 0100

R12 apply SBOXes: 1011 0010 1001 1110 1101 0010 0111 1010

R12 in IP table: 0110 1111 1111 0110 0001 0111 0100 0010

R12 XOR with L11: 0100 1101 0101 0111 1000 0101 0011 1010

L12: 1000 1110 0000 0101 0100 0110 0100 1110

R12: 0100 1101 0101 0111 1000 0101 0011 1010

///ROUND 13///

Key13: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R13 expanded to 48bits: 0010 0101 1010 1010 1010 1111 1100 0000 1010 1001 1111 0100

R13 XOR with Key13: 1011 0010 0110 1111 0111 1110 0011 1010 0001 0011 1011 0101

R13 apply SBOXes: 0010 1011 0010 0100 0110 0100 1101 1001

R13 in IP table: 0100 1010 0001 1100 0101 1010 1000 1101

R13 XOR with L12: 1100 0100 0001 1001 0001 1100 1100 0011

L13: 0100 1101 0101 0111 1000 0101 0011 1010

R13: 1100 0100 0001 1001 0001 1100 1100 0011

///ROUND 14///

Key14: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R14 expanded to 48bits: 1110 0000 1000 0000 1111 0010 1000 1111 1001 0110 0000 0111

R14 XOR with Key14: 1011 1111 1100 0011 0100 0101 0111 1101 0111 0001 0011 1101

R14 apply SBOXes: 0111 0010 0110 1011 0110 1110 0010 0110

R14 in IP table: 1101 0000 0110 0111 1000 0110 1110 1110

R14 XOR with L13: 1001 1101 0011 0000 0000 0011 1101 0100

L14: 1100 0100 0001 1001 0001 1100 1100 0011

R14: 1001 1101 0011 0000 0000 0011 1101 0100

///ROUND 15///

Key15: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R15 expanded to 48bits: 0100 1111 1010 1001 1010 0000 0000 0000 0111 1110 1010 1001

R15 XOR with Key15: 1111 0000 0011 1000 0010 1101 0011 1101 0100 0001 1010 0011

R15 apply SBOXes: 0101 1101 1101 1101 0001 0011 1110 0001

R15 in IP table: 1010 0100 0011 1001 1111 1101 0101 0011

R15 XOR with L14: 0110 0000 0010 0000 1110 0001 1001 0000

L15: 1001 1101 0011 0000 0000 0011 1101 0100

R15: 0110 0000 0010 0000 1110 0001 1001 0000

///ROUND 16///

Key16: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R16 expanded to 48bits: 0011 0000 0000 0001 0000 0001 0111 0000 0011 1100 1010 0000

R16 XOR with Key16: 1111 1011 0011 1100 1000 1010 0111 1110 0010 1011 0101 0101

R16 apply SBOXes: 0000 0110 0001 0110 0110 1110 1010 0110

R16 in IP table: 0101 0100 0110 0110 0001 0100 1011 1001

R16 XOR with L15: 1100 1001 0101 0110 0001 0111 0110 1101

L16: 0110 0000 0010 0000 1110 0001 1001 0000

R16: 1100 1001 0101 0110 0001 0111 0110 1101

---Block final permutation: 01001101 00010100 00010101 01000001 00010110 10101001 11011001 01001010

---DEC-Block: 10000011 00100110 01110111 10100010 11010101 10110110 11010111 01010110

L0: 1000 0011 0010 0110 0111 0111 1010 0010

R0:1101 0101 1011 0110 1101 0111 0101 0110

///ROUND 1///

Key1: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R1 expanded to 48bits: 0110 1010 1011 1101 1010 1101 0110 1010 1110 1010 1010 1101

R1 XOR with Key1: 1010 0001 1000 0000 0010 0110 0110 0100 1111 1101 0101 1000

R1 apply SBOXes: 1101 1100 1010 0000 0011 0101 0000 0101

R1 in IP table: 0010 0000 1000 1000 1010 1001 1011 1110

R1 XOR with L0: 1010 0011 1010 1110 1101 1110 0001 1100

L1: 1101 0101 1011 0110 1101 0111 0101 0110

R1: 1010 0011 1010 1110 1101 1110 0001 1100

///ROUND 2///

Key2: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R2 expanded to 48bits: 0101 0000 0111 1101 0101 1101 0110 1111 1100 0000 1111 1001

R2 XOR with Key2: 1110 1111 1110 1100 1101 0000 0101 0010 1111 1111 1111 0011

R2 apply SBOXes: 0000 1111 1111 0001 0011 1010 1100 1100

R2 in IP table: 1111 1100 0011 1001 0100 0001 1011 0101

R2 XOR with L1: 0010 1001 1000 1111 1001 0110 1110 0011

L2: 1010 0011 1010 1110 1101 1110 0001 1100

R2: 0010 1001 1000 1111 1001 0110 1110 0011

///ROUND 3///

Key3: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R3 expanded to 48bits: 1001 0101 0011 1100 0101 1111 1100 1010 1101 0111 0000 0110

R3 XOR with Key3: 1100 1010 0111 1111 1110 1000 0011 1000 0011 0000 0011 1100

R3 apply SBOXes: 1100 0001 1100 1100 0110 1111 0100 0101

R3 in IP table: 0001 0000 1011 0101 1111 1001 1110 1000

R3 XOR with L2: 1011 0011 0001 1011 0010 0111 1111 0100

L3: 0010 1001 1000 1111 1001 0110 1110 0011

R3: 1011 0011 0001 1011 0010 0111 1111 0100

///ROUND 4///

Key4: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R4 expanded to 48bits: 0101 1010 0110 1000 1111 0110 1001 0000 1111 1111 1010 1001

R4 XOR with Key4: 1100 1101 1010 1101 0010 0111 0110 1010 0100 0101 1110 1000

R4 apply SBOXes: 1011 0000 0010 0110 0000 1111 1100 1001

R4 in IP table: 0001 1000 1111 0000 0011 1010 0000 1111

R4 XOR with L3: 0011 0001 0111 1111 1010 1100 1110 1100

L4: 1011 0011 0001 1011 0010 0111 1111 0100

R4: 0011 0001 0111 1111 1010 1100 1110 1100

///ROUND 5///

Key5: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R5 expanded to 48bits: 0001 1010 0010 1011 1111 1111 1101 0101 1001 0111 0101 1000

R5 XOR with Key5: 0110 1111 0101 1010 0000 1010 0100 0001 1111 0000 1011 0001

R5 apply SBOXes: 0101 0111 1000 0110 1000 1000 1011 1111

R5 in IP table: 0101 1011 0100 0010 1101 1101 0011 0011

R5 XOR with L4: 1110 1000 0101 1001 1111 1010 1100 0111

L5: 0011 0001 0111 1111 1010 1100 1110 1100

R5: 1110 1000 0101 1001 1111 1010 1100 0111

///ROUND 6///

Key6: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R6 expanded to 48bits: 1111 0101 0000 0010 1111 0011 1111 1111 0101 0110 0000 1111

R6 XOR with Key6: 1101 0100 0101 1101 0010 0000 0010 0001 1000 0101 1000 1001

R6 apply SBOXes: 0011 0100 0010 1010 0111 1110 0111 1010

R6 in IP table: 0011 1010 0111 0110 0000 0110 1101 1110

R6 XOR with L5: 0000 1011 0000 1001 1010 1010 0011 0010

L6: 1110 1000 0101 1001 1111 1010 1100 0111

R6: 0000 1011 0000 1001 1010 1010 0011 0010

///ROUND 7///

Key7: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R7 expanded to 48bits: 0000 0101 0110 1000 0101 0011 1101 0101 0100 0001 1010 0100

R7 XOR with Key7: 1011 0100 1001 1011 0001 0100 0110 1111 0000 0111 1110 1011

R7 apply SBOXes: 0001 1111 0011 1000 1001 0111 0110 1010

R7 in IP table: 0110 1101 0011 1010 0110 0100 0101 1110

R7 XOR with L6: 1000 0101 0110 0011 1001 1110 1001 1001

L7: 0000 1011 0000 1001 1010 1010 0011 0010

R7: 1000 0101 0110 0011 1001 1110 1001 1001

///ROUND 8///

Key8: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R8 expanded to 48bits: 1100 0000 1010 1011 0000 0111 1100 1111 1101 0100 1111 0011

R8 XOR with Key8: 0010 0000 0111 0000 1110 1100 0010 0010 0011 0011 0111 0010

R8 apply SBOXes: 0010 0111 0111 0111 0111 0011 0001 0110

R8 in IP table: 1110 0110 0110 0111 0111 0010 1011 0100

R8 XOR with L7: 1110 1101 0110 1110 1101 1000 1000 0110

L8: 1000 0101 0110 0011 1001 1110 1001 1001

R8: 1110 1101 0110 1110 1101 1000 1000 0110

///ROUND 9///

Key9: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R9 expanded to 48bits: 0111 0101 1010 1011 0101 1101 0110 1111 0001 0100 0000 1101

R9 XOR with Key9: 1000 0010 0010 0001 0110 0111 1010 1110 0010 1111 1111 0110

R9 apply SBOXes: 0100 1110 0000 0110 1110 1110 1100 1101

R9 in IP table: 0101 1001 0111 1100 1001 1000 1011 1001

R9 XOR with L8: 1101 1100 0001 1111 0000 0110 0010 0000

L9: 1110 1101 0110 1110 1101 1000 1000 0110

R9: 1101 1100 0001 1111 0000 0110 0010 0000

///ROUND 10///

Key10: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R10 expanded to 48bits: 0110 1111 1000 0000 1111 1110 1000 0000 1100 0001 0000 0001

R10 XOR with Key10: 1000 0011 0000 0100 0100 1001 0111 0110 1101 1001 1011 1101

R10 apply SBOXes: 0100 0101 0010 0110 1000 1111 1101 0110

R10 in IP table: 0001 0011 0111 0010 1111 0000 0011 1101

R10 XOR with L9: 1111 1110 0001 1100 0010 1000 1011 1011

L10: 1101 1100 0001 1111 0000 0110 0010 0000

R10: 1111 1110 0001 1100 0010 1000 1011 1011

///ROUND 11///

Key11: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R11 expanded to 48bits: 1111 1111 1100 0000 1111 1000 0001 0101 0001 0101 1111 0111

R11 XOR with Key11: 1001 1100 0110 0101 1100 0110 0100 0101 0110 1110 1101 1000

R11 apply SBOXes: 0010 1110 1110 0011 0101 0100 0010 0101

R11 in IP table: 1110 0000 0100 1101 0000 1111 0011 1100

R11 XOR with L10: 0011 1100 0101 0010 0000 1001 0001 1100

L11: 1111 1110 0001 1100 0010 1000 1011 1011

R11: 0011 1100 0101 0010 0000 1001 0001 1100

///ROUND 12///

Key12: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R12 expanded to 48bits: 0001 1111 1000 0010 1010 0100 0000 0101 0010 1000 1111 1000

R12 XOR with Key12: 0110 0011 0110 1110 1010 0011 1110 1110 0111 1011 0101 0000

R12 apply SBOXes: 0101 0110 1010 1111 0100 1100 1010 1010

R12 in IP table: 1101 1000 0100 0110 1001 0101 0101 1111

R12 XOR with L11: 0010 0110 0101 1010 1011 1101 1110 0100

L12: 0011 1100 0101 0010 0000 1001 0001 1100

R12: 0010 0110 0101 1010 1011 1101 1110 0100

///ROUND 13///

Key13: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R13 expanded to 48bits: 0001 0000 1100 0010 1111 0101 0101 1111 1011 1111 0000 1000

R13 XOR with Key13: 0110 0010 0110 1111 0010 0011 1000 0100 1000 1010 0001 0101

R13 apply SBOXes: 0101 1011 1110 1111 1011 1001 1100 0110

R13 in IP table: 1111 0001 0101 1011 1111 0001 1110 0111

R13 XOR with L12: 1100 1101 0000 1001 1111 1000 1111 1011

L13: 0010 0110 0101 1010 1011 1101 1110 0100

R13: 1100 1101 0000 1001 1111 1000 1111 1011

///ROUND 14///

Key14: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R14 expanded to 48bits: 1110 0101 1010 1000 0101 0011 1111 1111 0001 0111 1111 0111

R14 XOR with Key14: 1011 0000 0101 0100 1101 1001 1011 1101 1101 1000 0110 1110

R14 apply SBOXes: 0010 0100 1000 0001 1101 0011 0110 0010

R14 in IP table: 1010 0001 0011 0110 0010 0111 0001 0000

R14 XOR with L13: 1000 0111 0110 1100 1001 1010 1111 0100

L14: 1100 1101 0000 1001 1111 1000 1111 1011

R14: 1000 0111 0110 1100 1001 1010 1111 0100

///ROUND 15///

Key15: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R15 expanded to 48bits: 0100 0000 1110 1011 0101 1001 0100 1111 0101 0111 1010 1001

R15 XOR with Key15: 0011 1001 0100 0101 1000 0000 1001 0100 1001 1110 0100 1100

R15 apply SBOXes: 1000 0010 0111 0111 1100 0111 1110 1011

R15 in IP table: 1100 1101 1111 0111 0011 1100 0000 1101

R15 XOR with L14: 0000 0000 1111 1110 1100 0100 1111 0110

L15: 1000 0111 0110 1100 1001 1010 1111 0100

R15: 0000 0000 1111 1110 1100 0100 1111 0110

///ROUND 16///

Key16: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R16 expanded to 48bits: 0000 0000 0001 0111 1111 1101 0110 0000 1001 0111 1010 1100

R16 XOR with Key16: 0001 1011 0001 0101 0001 0010 1001 1100 1110 0111 1101 1110

R16 apply SBOXes: 0001 1011 1100 0010 0111 1000 0110 0111

R16 in IP table: 0111 0000 0101 1111 0100 1101 1010 0010

R16 XOR with L15: 1111 0111 0011 0011 1101 0111 0101 0110

L16: 0000 0000 1111 1110 1100 0100 1111 0110

R16: 1111 0111 0011 0011 1101 0111 0101 0110

---Block final permutation: 01010100 01110111 01101111 00100000 01110111 01110010 01101111 01101110

---DEC-Block: 00000100 00110011 00110011 01101010 01011011 01010011 10101110 00010011

L0: 0000 0100 0011 0011 0011 0011 0110 1010

R0:0101 1011 0101 0011 1010 1110 0001 0011

///ROUND 1///

Key1: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R1 expanded to 48bits: 1010 1111 0110 1010 1010 0111 1101 0101 1100 0000 1010 0110

R1 XOR with Key1: 0110 0100 0101 0111 0010 1100 1101 1011 1101 0111 0101 0011

R1 apply SBOXes: 1001 0100 0010 0111 0101 1000 1000 0101

R1 in IP table: 1011 0000 1100 0100 0001 1000 0011 0111

R1 XOR with L0: 1011 0100 1111 0111 0010 1011 0101 1101

L1: 0101 1011 0101 0011 1010 1110 0001 0011

R1: 1011 0100 1111 0111 0010 1011 0101 1101

///ROUND 2///

Key2: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R2 expanded to 48bits: 1101 1010 1001 0111 1010 1110 1001 0101 0110 1010 1111 1011

R2 XOR with Key2: 0110 0101 0000 0110 0010 0011 1010 1000 0101 0101 1111 0001

R2 apply SBOXes: 1001 1001 1011 1111 1101 0100 1100 1111

R2 in IP table: 1010 1101 1101 1110 0101 1001 0110 1111

R2 XOR with L1: 1111 0110 1000 1101 1111 0111 0111 1100

L2: 1011 0100 1111 0111 0010 1011 0101 1101

R2: 1111 0110 1000 1101 1111 0111 0111 1100

///ROUND 3///

Key3: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R3 expanded to 48bits: 0111 1010 1101 0100 0101 1011 1111 1010 1110 1011 1111 1001

R3 XOR with Key3: 0010 0101 1001 0111 1110 1100 0000 1000 0000 1100 1100 0011

R3 apply SBOXes: 1110 0110 0001 0111 1100 1100 0101 1111

R3 in IP table: 1101 1111 1101 0110 1001 1010 0011 1000

R3 XOR with L2: 0110 1011 0010 0001 1011 0001 0110 0101

L3: 1111 0110 1000 1101 1111 0111 0111 1100

R3: 0110 1011 0010 0001 1011 0001 0110 0101

///ROUND 4///

Key4: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R4 expanded to 48bits: 1011 0101 0110 1001 0000 0011 1101 1010 0010 1011 0000 1010

R4 XOR with Key4: 0010 0010 1010 1100 1101 0010 0010 0000 1001 0001 0100 1011

R4 apply SBOXes: 0010 0100 1111 0010 0111 0111 1011 0011

R4 in IP table: 0010 0110 0110 0111 0010 1111 1001 1101

R4 XOR with L3: 1101 0000 1110 1010 1101 1000 1110 0001

L4: 0110 1011 0010 0001 1011 0001 0110 0101

R4: 1101 0000 1110 1010 1101 1000 1110 0001

///ROUND 5///

Key5: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R5 expanded to 48bits: 1110 1010 0001 0111 0101 0101 0110 1111 0001 0111 0000 0011

R5 XOR with Key5: 1001 1111 0110 0110 1010 0000 1111 1011 0111 0000 1110 1010

R5 apply SBOXes: 0010 0110 0100 1010 1110 0111 0000 1100

R5 in IP table: 0100 1001 0110 0101 0010 0010 1111 1000

R5 XOR with L4: 0010 0010 0100 0100 1001 0011 1001 1101

L5: 1101 0000 1110 1010 1101 1000 1110 0001

R5: 0010 0010 0100 0100 1001 0011 1001 1101

///ROUND 6///

Key6: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R6 expanded to 48bits: 1001 0000 0100 0010 0000 1001 0100 1010 0111 1100 1111 1010

R6 XOR with Key6: 1011 0001 0001 1101 1101 1010 1001 0100 1010 1111 0111 1100

R6 apply SBOXes: 0010 1100 0011 1100 1100 0010 0011 0101

R6 in IP table: 0000 0111 0010 1100 0001 1110 0111 0100

R6 XOR with L5: 1101 0111 1100 0110 1100 0110 1001 0101

L6: 0010 0010 0100 0100 1001 0011 1001 1101

R6: 1101 0111 1100 0110 1100 0110 1001 0101

///ROUND 7///

Key7: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R7 expanded to 48bits: 1110 1010 1111 1110 0000 1101 0110 0000 1101 0100 1010 1011

R7 XOR with Key7: 0101 1011 0000 1101 0100 1010 1101 1010 1001 0010 1110 0100

R7 apply SBOXes: 1100 0101 1110 0110 0101 1001 1001 0100

R7 in IP table: 0011 0010 1100 0101 1111 0001 0011 0101

R7 XOR with L6: 0001 0000 1000 0001 0110 0010 1010 1000

L7: 1101 0111 1100 0110 1100 0110 1001 0101

R7: 0001 0000 1000 0001 0110 0010 1010 1000

///ROUND 8///

Key8: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R8 expanded to 48bits: 0000 1010 0001 0100 0000 0010 1011 0000 0101 0101 0101 0000

R8 XOR with Key8: 1110 1010 1100 1111 1110 1001 0101 1101 1011 0010 1101 0001

R8 apply SBOXes: 1010 1101 1100 1010 1010 1011 1001 1100

R8 in IP table: 0001 1011 1110 1001 0110 0011 1111 0001

R8 XOR with L7: 1100 1100 0010 1111 1010 0101 0110 0100

L8: 0001 0000 1000 0001 0110 0010 1010 1000

R8: 1100 1100 0010 1111 1010 0101 0110 0100

///ROUND 9///

Key9: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R9 expanded to 48bits: 0110 0101 1000 0001 0101 1111 1101 0000 1010 1011 0000 1001

R9 XOR with Key9: 1001 0010 0000 1011 0110 0101 0001 0001 1001 0000 1111 0010

R9 apply SBOXes: 1110 0000 1000 0000 0100 0000 0000 0110

R9 in IP table: 0000 0000 1000 0110 1000 0011 0010 0000

R9 XOR with L8: 0001 0000 0000 0111 1110 0001 1000 1000

L9: 1100 1100 0010 1111 1010 0101 0110 0100

R9: 0001 0000 0000 0111 1110 0001 1000 1000

///ROUND 10///

Key10: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R10 expanded to 48bits: 0000 1010 0000 0000 0000 1111 1111 0000 0011 1100 0101 0000

R10 XOR with Key10: 1110 0110 1000 0100 1011 1000 0000 0110 0010 0100 1110 1100

R10 apply SBOXes: 1010 1010 1101 0101 1110 1110 0011 1110

R10 in IP table: 1101 1111 1010 1111 0001 0111 1010 1000

R10 XOR with L9: 0001 0011 1000 0000 1011 0010 1100 1100

L10: 0001 0000 0000 0111 1110 0001 1000 1000

R10: 0001 0011 1000 0000 1011 0010 1100 1100

///ROUND 11///

Key11: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R11 expanded to 48bits: 0000 1010 0111 1100 0000 0001 0101 1010 0101 0110 0101 1000

R11 XOR with Key11: 0110 1001 1101 1001 0011 1111 0000 1010 0010 1101 0111 0111

R11 apply SBOXes: 1001 1011 0100 1110 1100 1110 0000 0000

R11 in IP table: 0101 0001 1110 1101 0101 0000 0100 1010

R11 XOR with L10: 0100 0001 1110 1010 1011 0001 1100 0010

L11: 0001 0011 1000 0000 1011 0010 1100 1100

R11: 0100 0001 1110 1010 1011 0001 1100 0010

///ROUND 12///

Key12: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R12 expanded to 48bits: 0010 0000 0011 1111 0101 0101 0101 1010 0011 1110 0000 0100

R12 XOR with Key12: 0101 1100 1101 0011 0101 0010 1011 0001 0110 1101 1010 1100

R12 apply SBOXes: 1011 1000 0110 0010 0111 0100 1000 1110

R12 in IP table: 0010 1000 1100 1111 0000 0010 1010 1111

R12 XOR with L11: 0011 1011 0100 1111 1011 0000 0110 0011

L12: 0100 0001 1110 1010 1011 0001 1100 0010

R12: 0011 1011 0100 1111 1011 0000 0110 0011

///ROUND 13///

Key13: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R13 expanded to 48bits: 1001 1111 0110 1010 0101 1111 1101 1010 0000 0011 0000 0110

R13 XOR with Key13: 1110 1101 1100 0111 1000 1001 0000 0001 0011 0110 0001 1011

R13 apply SBOXes: 0000 0101 1000 0110 0010 0001 0101 1110

R13 in IP table: 0000 1010 0101 0010 0111 0001 1011 0000

R13 XOR with L12: 0100 1011 1011 1000 1100 0000 0111 0010

L13: 0011 1011 0100 1111 1011 0000 0110 0011

R13: 0100 1011 1011 1000 1100 0000 0111 0010

///ROUND 14///

Key14: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R14 expanded to 48bits: 0010 0101 0111 1101 1111 0001 0110 0000 0000 0011 1010 0100

R14 XOR with Key14: 0111 0000 1000 0001 0111 1011 0010 0010 1100 1100 0011 1101

R14 apply SBOXes: 0000 0110 0000 0111 0111 1100 1010 0110

R14 in IP table: 1111 0000 0100 0110 0001 0100 1011 1001

R14 XOR with L13: 1100 1011 0000 1001 1010 0100 1101 1010

L14: 0100 1011 1011 1000 1100 0000 0111 0010

R14: 1100 1011 0000 1001 1010 0100 1101 1010

///ROUND 15///

Key15: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

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

R15 XOR with Key15: 0001 1100 1100 0110 1000 1010 0000 1011 0101 1111 0001 0000

R15 apply SBOXes: 0100 0011 0100 0110 1100 0001 1001 1010

R15 in IP table: 0100 1011 0100 0111 1111 0000 0000 0001

R15 XOR with L14: 0000 0000 1111 1111 0011 0000 0111 0011

L15: 1100 1011 0000 1001 1010 0100 1101 1010

R15: 0000 0000 1111 1111 0011 0000 0111 0011

///ROUND 16///

Key16: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R16 expanded to 48bits: 1000 0000 0001 0111 1111 1110 1001 1010 0000 0011 1010 0110

R16 XOR with Key16: 1001 1011 0001 0101 0001 0001 0110 0110 0111 0011 1101 0100

R16 apply SBOXes: 1000 1011 1100 0100 0011 1100 1010 0011

R16 in IP table: 0111 0000 1000 1011 0101 1101 1000 1001

R16 XOR with L15: 1011 1011 1000 0010 1111 1001 0101 0011

L16: 0000 0000 1111 1111 0011 0000 0111 0011

R16: 1011 1011 1000 0010 1111 1001 0101 0011

---Block final permutation: 01100111 01110011 00100000 01100100 01101111 01101110 00100111 01110100

---DEC-Block: 10000000 11011100 01111011 00011100 10111010 11001010 01001010 10100100

L0: 1000 0000 1101 1100 0111 1011 0001 1100

R0:1011 1010 1100 1010 0100 1010 1010 0100

///ROUND 1///

Key1: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R1 expanded to 48bits: 0101 1111 0101 0110 0101 0100 0010 0101 0101 0101 0000 1001

R1 XOR with Key1: 1001 0100 0110 1011 1101 1111 0010 1011 0100 0010 1111 1100

R1 apply SBOXes: 1000 1110 0111 1001 1010 0100 1001 0101

R1 in IP table: 1100 0111 1000 1001 0000 1000 1111 1101

R1 XOR with L0: 0100 0111 0101 0101 0111 0011 1110 0001

L1: 1011 1010 1100 1010 0100 1010 1010 0100

R1: 0100 0111 0101 0101 0111 0011 1110 0001

///ROUND 2///

Key2: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R2 expanded to 48bits: 1010 0000 1110 1010 1010 1010 1011 1010 0111 1111 0000 0010

R2 XOR with Key2: 0001 1111 0111 1011 0010 0111 1000 0111 0100 0000 0000 1000

R2 apply SBOXes: 0100 1100 0011 0110 1011 0100 0100 0110

R2 in IP table: 0010 0101 0101 1010 1001 0000 1011 1100

R2 XOR with L1: 1001 1111 1001 0000 1101 1010 0001 1000

L2: 0100 0111 0101 0101 0111 0011 1110 0001

R2: 1001 1111 1001 0000 1101 1010 0001 1000

///ROUND 3///

Key3: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R3 expanded to 48bits: 0100 1111 1111 1100 1010 0001 0110 1111 0100 0000 1111 0001

R3 XOR with Key3: 0001 0000 1011 1111 0001 0110 1001 1101 1010 0111 1100 1011

R3 apply SBOXes: 1101 0010 1110 0101 0111 0111 0110 0011

R3 in IP table: 1110 0000 1011 0111 1011 1101 1000 1110

R3 XOR with L2: 1010 0111 1110 0010 1100 1110 0110 1111

L3: 1001 1111 1001 0000 1101 1010 0001 1000

R3: 1010 0111 1110 0010 1100 1110 0110 1111

///ROUND 4///

Key4: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R4 expanded to 48bits: 1101 0000 1111 1111 0000 0101 0110 0101 1100 0011 0101 1111

R4 XOR with Key4: 0100 0111 0011 1010 1101 0100 1001 1111 0111 1001 0001 1110

R4 apply SBOXes: 1010 0110 1001 1000 0111 0111 1011 0111

R4 in IP table: 0110 0110 1010 0110 0010 1111 1111 1001

R4 XOR with L3: 1111 1001 0011 0110 1111 0101 1110 0001

L4: 1010 0111 1110 0010 1100 1110 0110 1111

R4: 1111 1001 0011 0110 1111 0101 1110 0001

///ROUND 5///

Key5: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R5 expanded to 48bits: 1111 1111 0010 1001 1010 1101 0111 1010 1011 1111 0000 0011

R5 XOR with Key5: 1000 1010 0101 1000 0101 1000 1110 1110 1101 1000 1110 1010

R5 apply SBOXes: 0001 1010 0001 1011 0100 1111 1011 1100

R5 in IP table: 1101 1110 0110 1100 0010 0100 0110 1011

R5 XOR with L4: 0111 1001 1000 1110 1110 1010 0000 0100

L5: 1111 1001 0011 0110 1111 0101 1110 0001

R5: 0111 1001 1000 1110 1110 1010 0000 0100

///ROUND 6///

Key6: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R6 expanded to 48bits: 0011 1111 0011 1100 0101 1101 0111 0101 0100 0000 0000 1000

R6 XOR with Key6: 0001 1110 0110 0011 1000 1110 1010 1011 1001 0011 1000 1110

R6 apply SBOXes: 0100 1011 0101 1010 1101 0110 1101 0001

R6 in IP table: 0110 0111 0111 1101 1100 1000 0100 1001

R6 XOR with L5: 1001 1110 0100 1011 0011 1101 1010 1000

L6: 0111 1001 1000 1110 1110 1010 0000 0100

R6: 1001 1110 0100 1011 0011 1101 1010 1000

///ROUND 7///

Key7: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R7 expanded to 48bits: 0100 1111 1100 0010 0101 0110 1001 1111 1011 1101 0101 0001

R7 XOR with Key7: 1111 1110 0011 0001 0001 0001 0010 0101 1111 1011 0001 1110

R7 apply SBOXes: 1101 1000 1001 0100 0100 1000 0111 0111

R7 in IP table: 0001 0110 1001 1110 1001 1101 0010 0010

R7 XOR with L6: 0110 1111 0001 0000 0111 0111 0010 0110

L7: 1001 1110 0100 1011 0011 1101 1010 1000

R7: 0110 1111 0001 0000 0111 0111 0010 0110

///ROUND 8///

Key8: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R8 expanded to 48bits: 0011 0101 1110 1000 1010 0000 0011 1010 1110 1001 0000 1100

R8 XOR with Key8: 1101 0101 0011 0011 0100 1011 1101 0111 0000 1110 1000 1101

R8 apply SBOXes: 0011 0000 0110 1111 0000 0111 0101 0111

R8 in IP table: 1000 0010 0111 0011 0011 1010 0110 1110

R8 XOR with L7: 0001 1100 0011 1000 0000 0111 1100 0110

L8: 0110 1111 0001 0000 0111 0111 0010 0110

R8: 0001 1100 0011 1000 0000 0111 1100 0110

///ROUND 9///

Key9: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R9 expanded to 48bits: 0000 1111 1000 0001 1111 0000 0000 0000 1111 1110 0000 1100

R9 XOR with Key9: 1111 1000 0000 1011 1100 1010 1100 0001 1100 0101 1111 0111

R9 apply SBOXes: 0000 1111 0111 0110 1111 0101 1100 0000

R9 in IP table: 0110 0101 0101 1101 0111 0000 1001 1101

R9 XOR with L8: 0000 1010 0100 1101 0000 0111 1011 1011

L9: 0001 1100 0011 1000 0000 0111 1100 0110

R9: 0000 1010 0100 1101 0000 0111 1011 1011

///ROUND 10///

Key10: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R10 expanded to 48bits: 1000 0101 0100 0010 0101 1010 1000 0000 1111 1101 1111 0110

R10 XOR with Key10: 0110 1001 1100 0110 1110 1101 0111 0110 1110 0101 0100 1010

R10 apply SBOXes: 1001 0101 1011 1101 1000 0011 0101 1111

R10 in IP table: 1000 1111 1011 0010 0111 1001 0111 0110

R10 XOR with L9: 1001 0011 1000 1010 0111 1110 1011 0000

L10: 0000 1010 0100 1101 0000 0111 1011 1011

R10: 1001 0011 1000 1010 0111 1110 1011 0000

///ROUND 11///

Key11: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R11 expanded to 48bits: 0100 1010 0111 1100 0101 0100 0011 1111 1101 0101 1010 0001

R11 XOR with Key11: 0010 1001 1101 1001 0110 1010 0110 1111 1010 1110 1000 1110

R11 apply SBOXes: 1111 1011 1101 1011 1001 1101 0101 0001

R11 in IP table: 1111 0111 1101 1001 1110 1011 0100 1010

R11 XOR with L10: 1111 1101 1001 0100 1110 1100 1111 0001

L11: 1001 0011 1000 1010 0111 1110 1011 0000

R11: 1111 1101 1001 0100 1110 1100 1111 0001

///ROUND 12///

Key12: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R12 expanded to 48bits: 1111 1111 1011 1100 1010 1001 0111 0101 1001 0111 1010 0011

R12 XOR with Key12: 1000 0011 0101 0000 1010 1110 1001 1110 1100 0100 0000 1011

R12 apply SBOXes: 0100 0111 0000 1101 0111 1100 0011 0011

R12 in IP table: 1111 0010 0000 0110 1101 1100 1101 1000

R12 XOR with L11: 0110 0001 1000 1100 1010 0010 0110 1000

L12: 1111 1101 1001 0100 1110 1100 1111 0001

R12: 0110 0001 1000 1100 1010 0010 0110 1000

///ROUND 13///

Key13: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R13 expanded to 48bits: 0011 0000 0011 1100 0101 1001 0101 0000 0100 0011 0101 0000

R13 XOR with Key13: 0100 0010 1001 0001 1000 1111 1000 1011 0111 0110 0100 1101

R13 apply SBOXes: 0011 0011 1110 0011 0010 0111 0010 0111

R13 in IP table: 1100 0000 0110 0011 0110 1111 1010 1110

R13 XOR with L12: 0011 1101 1111 0111 1000 0011 0101 1111

L13: 0110 0001 1000 1100 1010 0010 0110 1000

R13: 0011 1101 1111 0111 1000 0011 0101 1111

///ROUND 14///

Key14: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R14 expanded to 48bits: 1001 1111 1011 1111 1010 1111 1100 0000 0110 1010 1111 1110

R14 XOR with Key14: 1100 1010 0100 0011 0010 0101 1000 0010 1010 0101 0110 0111

R14 apply SBOXes: 1100 0111 1111 0000 0100 1000 0101 0111

R14 in IP table: 0101 0110 1001 0111 1100 1001 0011 0100

R14 XOR with L13: 0011 0111 0001 1011 0110 1011 0101 1100

L14: 0011 1101 1111 0111 1000 0011 0101 1111

R14: 0011 0111 0001 1011 0110 1011 0101 1100

///ROUND 15///

Key15: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R15 expanded to 48bits: 0001 1010 1110 1000 1111 0110 1011 0101 0110 1010 1111 1000

R15 XOR with Key15: 0110 0011 0100 0110 0010 1111 0110 1110 1010 0011 0001 1101

R15 apply SBOXes: 0101 1100 1011 1000 1001 1000 1000 1001

R15 in IP table: 0011 1101 0000 1000 1000 1001 0101 0111

R15 XOR with L14: 0000 0000 1111 1111 0000 1010 0000 1000

L15: 0011 0111 0001 1011 0110 1011 0101 1100

R15: 0000 0000 1111 1111 0000 1010 0000 1000

///ROUND 16///

Key16: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R16 expanded to 48bits: 0000 0000 0001 0111 1111 1110 1000 0101 0100 0000 0101 0000

R16 XOR with Key16: 0001 1011 0001 0101 0001 0001 0111 1001 0011 0000 0010 0010

R16 apply SBOXes: 0001 1011 1100 0100 1001 0001 0100 1011

R16 in IP table: 0110 1001 0001 1011 0111 1001 0000 0010

R16 XOR with L15: 0101 1110 0000 0000 0001 0010 0101 1110

L16: 0000 0000 1111 1111 0000 1010 0000 1000

R16: 0101 1110 0000 0000 0001 0010 0101 1110

---Block final permutation: 00100000 01101101 01100001 01101011 01100101 00100000 01100001 00100000

---DEC-Block: 11001001 01010110 00010111 01101101 01100000 00100000 11100001 10010000

L0: 1100 1001 0101 0110 0001 0111 0110 1101

R0:0110 0000 0010 0000 1110 0001 1001 0000

///ROUND 1///

Key1: 1100 1011 0011 1101 1000 1011 0000 1110 0001 0111 1111 0101

R1 expanded to 48bits: 0011 0000 0000 0001 0000 0001 0111 0000 0011 1100 1010 0000

R1 XOR with Key1: 1111 1011 0011 1100 1000 1010 0111 1110 0010 1011 0101 0101

R1 apply SBOXes: 0000 0110 0001 0110 0110 1110 1010 0110

R1 in IP table: 0101 0100 0110 0110 0001 0100 1011 1001

R1 XOR with L0: 1001 1101 0011 0000 0000 0011 1101 0100

L1: 0110 0000 0010 0000 1110 0001 1001 0000

R1: 1001 1101 0011 0000 0000 0011 1101 0100

///ROUND 2///

Key2: 1011 1111 1001 0001 1000 1101 0011 1101 0011 1111 0000 1010

R2 expanded to 48bits: 0100 1111 1010 1001 1010 0000 0000 0000 0111 1110 1010 1001

R2 XOR with Key2: 1111 0000 0011 1000 0010 1101 0011 1101 0100 0001 1010 0011

R2 apply SBOXes: 0101 1101 1101 1101 0001 0011 1110 0001

R2 in IP table: 1010 0100 0011 1001 1111 1101 0101 0011

R2 XOR with L1: 1100 0100 0001 1001 0001 1100 1100 0011

L2: 1001 1101 0011 0000 0000 0011 1101 0100

R2: 1100 0100 0001 1001 0001 1100 1100 0011

///ROUND 3///

Key3: 0101 1111 0100 0011 1011 0111 1111 0010 1110 0111 0011 1010

R3 expanded to 48bits: 1110 0000 1000 0000 1111 0010 1000 1111 1001 0110 0000 0111

R3 XOR with Key3: 1011 1111 1100 0011 0100 0101 0111 1101 0111 0001 0011 1101

R3 apply SBOXes: 0111 0010 0110 1011 0110 1110 0010 0110

R3 in IP table: 1101 0000 0110 0111 1000 0110 1110 1110

R3 XOR with L2: 0100 1101 0101 0111 1000 0101 0011 1010

L3: 1100 0100 0001 1001 0001 1100 1100 0011

R3: 0100 1101 0101 0111 1000 0101 0011 1010

///ROUND 4///

Key4: 1001 0111 1100 0101 1101 0001 1111 1010 1011 1010 0100 0001

R4 expanded to 48bits: 0010 0101 1010 1010 1010 1111 1100 0000 1010 1001 1111 0100

R4 XOR with Key4: 1011 0010 0110 1111 0111 1110 0011 1010 0001 0011 1011 0101

R4 apply SBOXes: 0010 1011 0010 0100 0110 0100 1101 1001

R4 in IP table: 0100 1010 0001 1100 0101 1010 1000 1101

R4 XOR with L3: 1000 1110 0000 0101 0100 0110 0100 1110

L4: 0100 1101 0101 0111 1000 0101 0011 1010

R4: 1000 1110 0000 0101 0100 0110 0100 1110

///ROUND 5///

Key5: 0111 0101 0111 0001 1111 0101 1001 0100 0110 0111 1110 1001

R5 expanded to 48bits: 0100 0101 1100 0000 0000 1010 1010 0000 1100 0010 0101 1101

R5 XOR with Key5: 0011 0000 1011 0001 1111 1111 0011 0100 1010 0101 1011 0100

R5 apply SBOXes: 1011 0010 1001 1110 1101 0010 0111 1010

R5 in IP table: 0110 1111 1111 0110 0001 0111 0100 0010

R5 XOR with L4: 0010 0010 1010 0001 1001 0010 0111 1000

L5: 1000 1110 0000 0101 0100 0110 0100 1110

R5: 0010 0010 1010 0001 1001 0010 0111 1000

///ROUND 6///

Key6: 0010 0001 0101 1111 1101 0011 1101 1110 1101 0011 1000 0110

R6 expanded to 48bits: 0001 0000 0101 0101 0000 0011 1100 1010 0100 0011 1111 0000

R6 XOR with Key6: 0011 0001 0000 1010 1101 0000 0001 0100 1001 0000 0111 0110

R6 apply SBOXes: 1011 1001 1001 0001 0010 0111 1101 1101

R6 in IP table: 1000 1110 1011 1000 0110 1011 1010 1011

R6 XOR with L5: 0000 0000 1011 1101 0010 1101 1110 0101

L6: 0010 0010 1010 0001 1001 0010 0111 1000

R6: 0000 0000 1011 1101 0010 1101 1110 0101

///ROUND 7///

Key7: 1011 0001 1111 0011 0100 0111 1011 1010 0100 0110 0100 1111

R7 expanded to 48bits: 1000 0000 0001 0101 1111 1010 1001 0101 1011 1111 0000 1010

R7 XOR with Key7: 0011 0001 1110 0110 1011 1101 0010 1111 1111 1001 0100 0101

R7 apply SBOXes: 1011 1010 0100 0010 0111 1101 1101 1101

R7 in IP table: 0111 1010 1101 1101 0010 1010 1010 1011

R7 XOR with L6: 0101 1000 0111 1100 1011 1000 1101 0011

L7: 0000 0000 1011 1101 0010 1101 1110 0101

R7: 0101 1000 0111 1100 1011 1000 1101 0011

///ROUND 8///

Key8: 1110 0000 1101 1011 1110 1011 1110 1101 1110 0111 1000 0001

R8 expanded to 48bits: 1010 1111 0000 0011 1111 1001 0101 1111 0001 0110 1010 0110

R8 XOR with Key8: 0100 1111 1101 1000 0001 0010 1011 0010 1111 0001 0010 0111

R8 apply SBOXes: 0110 1110 1101 0010 0111 1010 0010 0111

R8 in IP table: 0111 0100 0110 1111 1000 1111 1011 0000

R8 XOR with L7: 0111 0100 1101 0010 1010 0010 0101 0101

L8: 0101 1000 0111 1100 1011 1000 1101 0011

R8: 0111 0100 1101 0010 1010 0010 0101 0101

///ROUND 9///

Key9: 1111 0111 1000 1010 0011 1010 1100 0001 0011 1011 1111 1011

R9 expanded to 48bits: 1011 1010 1001 0110 1010 0101 0101 0000 0100 0010 1010 1010

R9 XOR with Key9: 0100 1101 0001 1100 1001 1111 1001 0001 0111 1001 0101 0001

R9 apply SBOXes: 0110 1100 0001 1001 0001 1110 1101 1100

R9 in IP table: 1011 1110 0011 1000 1000 0010 0111 1001

R9 XOR with L8: 1110 0110 0100 0100 0011 1010 1010 1010

L9: 0111 0100 1101 0010 1010 0010 0101 0101

R9: 1110 0110 0100 0100 0011 1010 1010 1010

///ROUND 10///

Key10: 1110 1100 1000 0100 1011 0111 1111 0110 0001 1000 1011 1100

R10 expanded to 48bits: 0111 0000 1100 0010 0000 1000 0001 1111 0101 0101 0101 0101

R10 XOR with Key10: 1001 1100 0100 0110 1011 1111 1110 1001 0100 1101 1110 1001

R10 apply SBOXes: 0010 1000 0100 1110 0011 0011 1111 0100

R10 in IP table: 0010 0010 0111 1001 0011 0110 1110 0001

R10 XOR with L9: 0101 0110 1010 1011 1001 0100 1011 0100

L10: 1110 0110 0100 0100 0011 1010 1010 1010

R10: 0101 0110 1010 1011 1001 0100 1011 0100

///ROUND 11///

Key11: 0110 0011 1010 0101 0011 1110 0101 0000 0111 1011 0010 1111

R11 expanded to 48bits: 0010 1010 1101 0101 0101 0111 1100 1010 1001 0101 1010 1000

R11 XOR with Key11: 0100 1001 0111 0000 0110 1001 1001 1010 1110 1110 1000 0111

R11 apply SBOXes: 1010 1010 1101 1010 1011 0011 0101 1000

R11 in IP table: 0110 1111 1111 1001 0010 0011 1100 0000

R11 XOR with L10: 1000 1001 1011 1101 0001 1001 0110 1010

L11: 0101 0110 1010 1011 1001 0100 1011 0100

R11: 1000 1001 1011 1101 0001 1001 0110 1010

///ROUND 12///

Key12: 0111 1100 1110 1100 0000 0111 1110 1011 0101 0011 1010 1000

R12 expanded to 48bits: 0100 0101 0011 1101 1111 1010 1000 1111 0010 1011 0101 0101

R12 XOR with Key12: 0011 1001 1101 0001 1111 1101 0110 0100 0111 1000 1111 1101

R12 apply SBOXes: 1000 1011 1001 0010 0011 0010 1011 0110

R12 in IP table: 0110 0110 1110 1010 0100 0101 1010 0001

R12 XOR with L11: 0011 0000 0100 0001 1101 0001 0001 0101

L12: 1000 1001 1011 1101 0001 1001 0110 1010

R12: 0011 0000 0100 0001 1101 0001 0001 0101

///ROUND 13///

Key13: 0111 0010 1010 1101 1101 0110 1101 1011 0011 0101 0001 1101

R13 expanded to 48bits: 1001 1010 0000 0010 0000 0011 1110 1010 0010 1000 1010 1010

R13 XOR with Key13: 1110 1000 1010 1111 1101 0101 0011 0001 0001 1101 1011 0111

R13 apply SBOXes: 1010 1011 1100 0010 1011 0110 1000 0000

R13 in IP table: 0110 0001 1110 1001 0100 0011 1000 1001

R13 XOR with L12: 1110 1000 0101 0100 0101 1010 1110 0011

L13: 0011 0000 0100 0001 1101 0001 0001 0101

R13: 1110 1000 0101 0100 0101 1010 1110 0011

///ROUND 14///

Key14: 0101 0101 1111 1100 1000 1010 0100 0010 1100 1111 1001 1001

R14 expanded to 48bits: 1111 0101 0000 0010 1010 1000 0010 1111 0101 0111 0000 0111

R14 XOR with Key14: 1010 0000 1111 1110 0010 0010 0110 1101 1001 1000 1001 1110

R14 apply SBOXes: 1101 1110 0101 0110 1001 0000 0100 0111

R14 in IP table: 0110 0101 1101 1011 1001 1000 0011 0010

R14 XOR with L13: 0101 0101 1001 1010 0100 1001 0010 0111

L14: 1110 1000 0101 0100 0101 1010 1110 0011

R14: 0101 0101 1001 1010 0100 1001 0010 0111

///ROUND 15///

Key15: 0111 1001 1010 1110 1101 1001 1101 1011 1100 1001 1110 0101

R15 expanded to 48bits: 1010 1010 1011 1100 1111 0100 0010 0101 0010 1001 0000 1110

R15 XOR with Key15: 1101 0011 0001 0010 0010 1101 1111 1110 1110 0000 1110 1011

R15 apply SBOXes: 1001 1011 0110 1101 0011 0011 0000 1010

R15 in IP table: 1110 1000 1010 1011 0111 0000 1100 0110

R15 XOR with L14: 0000 0000 1111 1111 0010 1010 0010 0101

L15: 0101 0101 1001 1010 0100 1001 0010 0111

R15: 0000 0000 1111 1111 0010 1010 0010 0101

///ROUND 16///

Key16: 0001 1011 0000 0010 1110 1111 1111 1100 0111 0000 0111 0010

R16 expanded to 48bits: 1000 0000 0001 0111 1111 1110 1001 0101 0100 0001 0000 1010

R16 XOR with Key16: 1001 1011 0001 0101 0001 0001 0110 1001 0011 0001 0111 1000

R16 apply SBOXes: 1000 1011 1100 0100 0000 0001 1011 1111

R16 in IP table: 0100 1010 1000 1011 0111 1101 0010 0001

R16 XOR with L15: 0001 1111 0001 0001 0011 0100 0000 0110

L16: 0000 0000 1111 1111 0010 1010 0010 0101

R16: 0001 1111 0001 0001 0011 0100 0000 0110

---Block final permutation: 01110010 01101001 01100111 01101000 01110100 00101110 00100000 00100000

Ciphered: 'Ì\x7f¾\x00®5\x8eé¶¿H\x89¶\x1d¡\x08\x04¬\x13½\x95\x86<òM\x14\x15A\x16©ÙJ'

Ciphered (hex): CC 7F BE 00 AE 35 8E E9 B6 BF 48 89 B6 1D A1 08 04 AC 13 BD 95 86 3C F2 4D 14 15 41 16 A9 D9 4A

Deciphered: "Two wrongs don't make a right. "

Deciphered (hex): 54 77 6F 20 77 72 6F 6E 67 73 20 64 6F 6E 27 74 20 6D 61 6B 65 20 61 20 72 69 67 68 74 2E 20 20