1Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

КАФЕДРА ИНФОРМАТИКИ

Лабораторная работа № 1

**Компьютерная реализация блочных шифров на примере DES и ГОСТ**

Выполнил студент гр. 553502

Стаина Д.С.

Проверил

Бондаренко А.С.

Минск, 2018

# 1. Введение

Целью данной лабораторной было изучить алгоритмы DES и ГОСТ 28147-89 и реализовать программные средства шифрования и дешифрования текстовых файлов при их помощи.

2. Блок-схемы алгоритмов

Схема алгоритма DES:



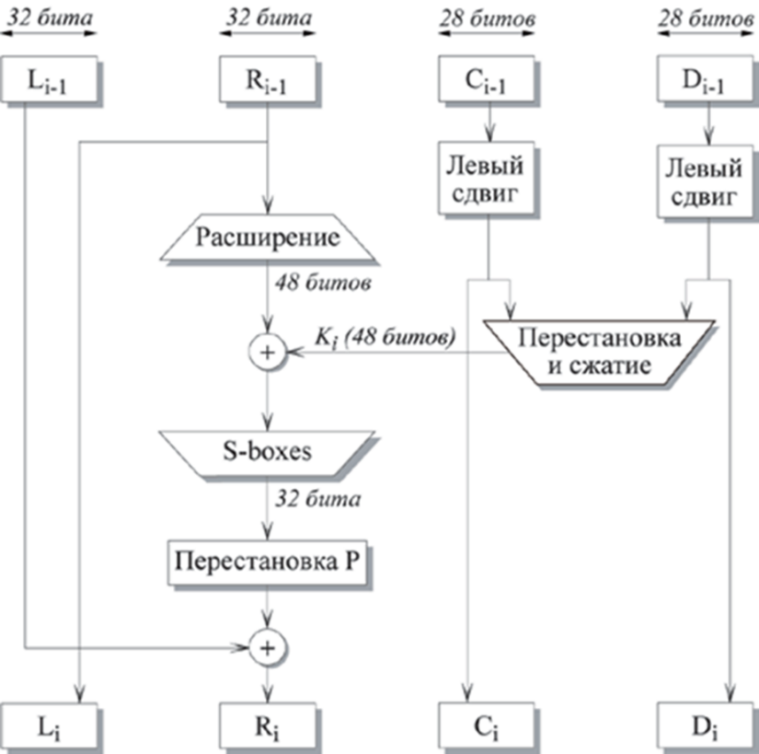
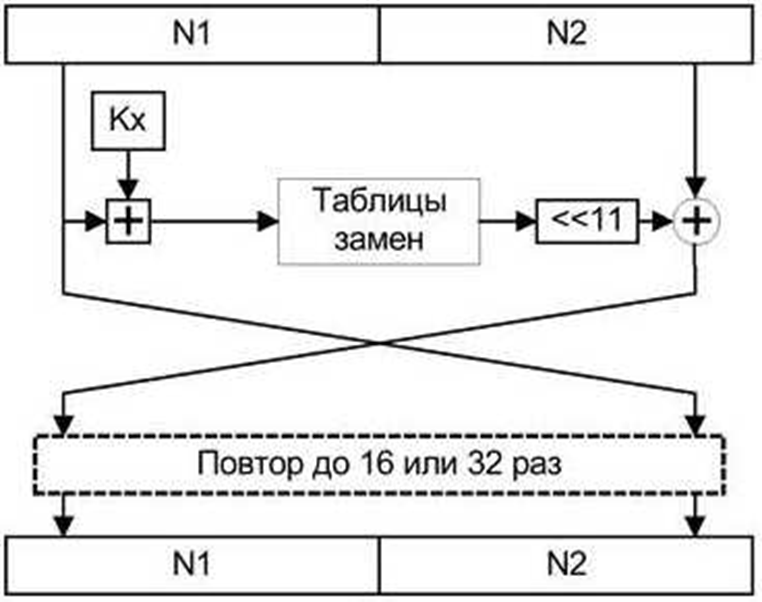
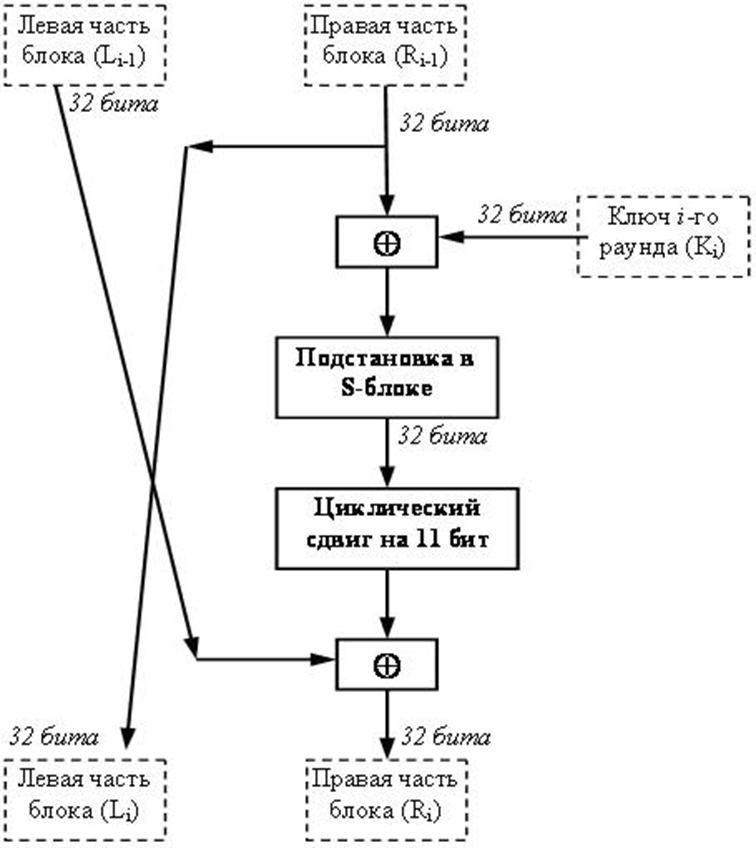


Схема алгоритма ГОСТ 28147-89:





**3. Теоретические сведения**

**Общая схема DES**

DES является классической сетью Фейстеля с двумя ветвями.

Данные шифруются 64-битными блоками, используя 56-битный ключ.

Алгоритм преобразует за несколько раундов 64-битный вход в 64-битный выход.

Процесс шифрования состоит из четырех этапов.

* Выполняется начальная перестановка (IP) 64-битного исходного текста (забеливание), во время которой биты переупорядочиваются в соответствии со стандартной таблицей.
* Этап состоит из 16 раундов одной и той же функции, которая использует операции сдвига и подстановки.
* Левая и правая половины выхода последней (16-й) итерации меняются местами.
* Выполняется перестановка IP-1 результата, полученного на третьем этапе.

Перестановка IP-1 инверсна начальной перестановке.



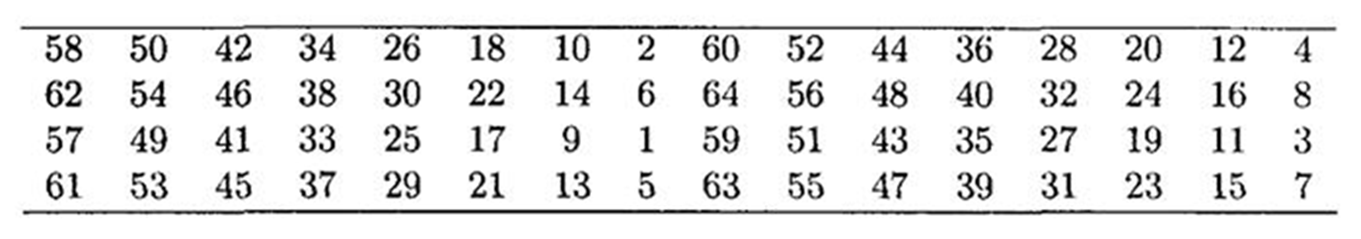
**Шифрование**

**Начальная перестановка**

Начальная перестановка и ее инверсия определяются стандартной таблицей.

Если М - это произвольные 64 бита, то

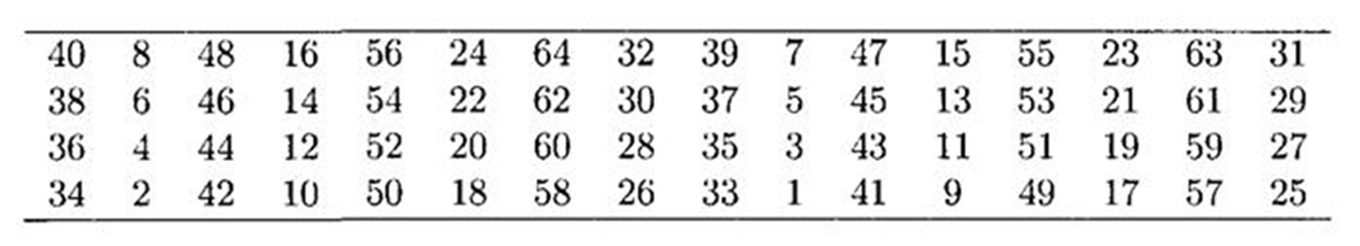
X = IP (M) - переставленные 64 бита.



Если применить обратную функцию перестановки

Y = IP-1 (X) = IP-1 (IP(M)),

то получится первоначальная последовательность бит.



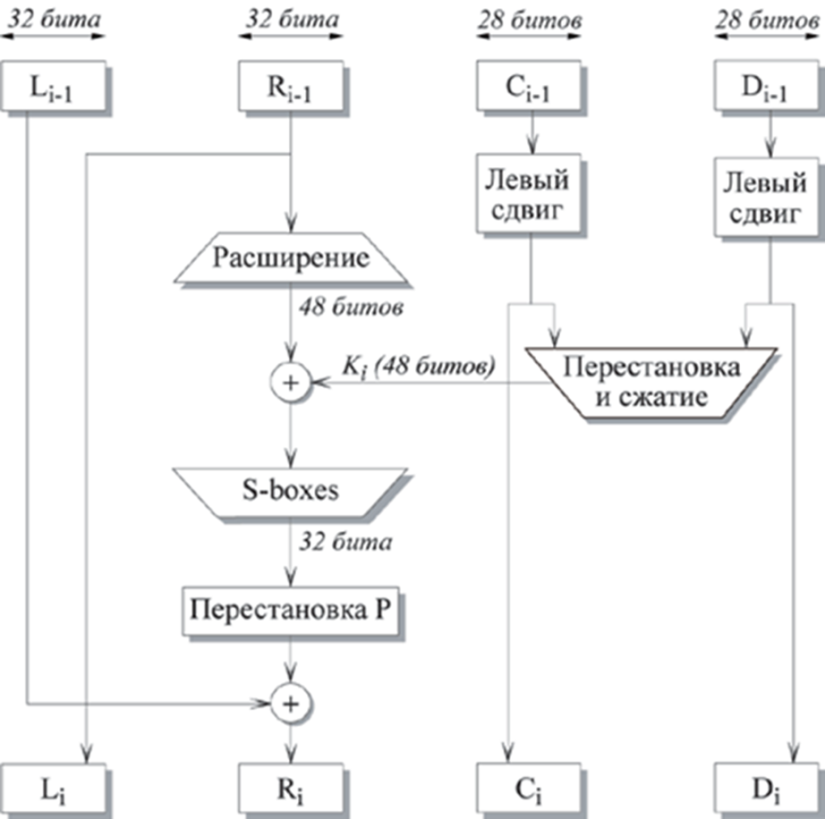
Начальная перестановка и соответствующая заключительная перестановка не влияют на криптостойкость DES (перестановка в первую очередь служит для облегчения побайтной загрузки данных открытого текста и шифротекста в микросхему DES).

Последовательность преобразований отдельного раунда

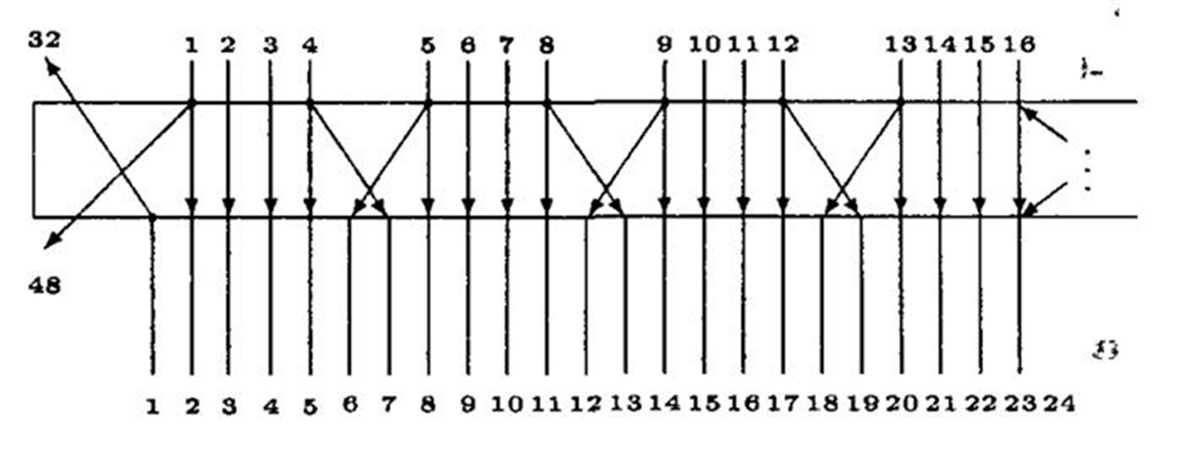
Каждую итерацию можно описать следующим образом:

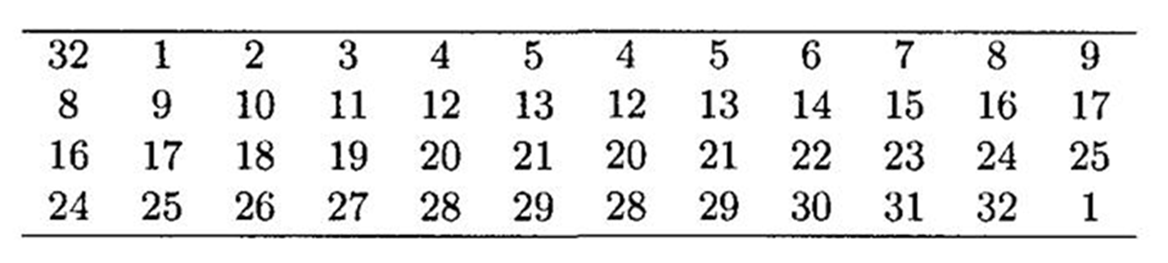
Li = Ri-1

Ri = Li-1⊕F(Ri-1, Ki)



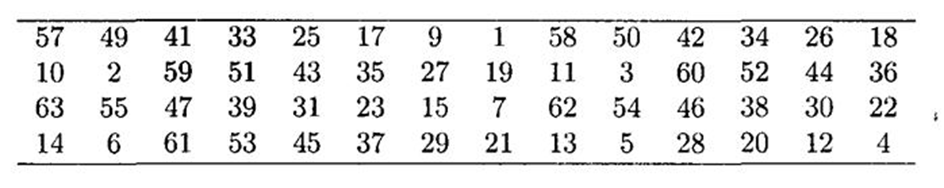
DES — схема перестановки с расширением





**Процедура преобразования ключа**

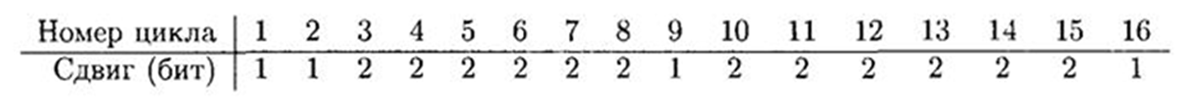
64-битовый ключ DES уменьшается до 56-битового ключа отбрасыванием каждого восьмого бита. Эти биты используются только для контроля четности, позволяя проверять правильность ключа.



После извлечения 56-битного ключа для каждого из 16 циклов генерируется новый 48-битный подключ.

Эти подключи, К2, определяются следующим образом:

* 56-битный ключ делится на две 28-битные половины.
* Половины циклически сдвигаются влево на один или два бита в зависимости от номера цикла.



**DES — подстановка при помощи S-блоков**

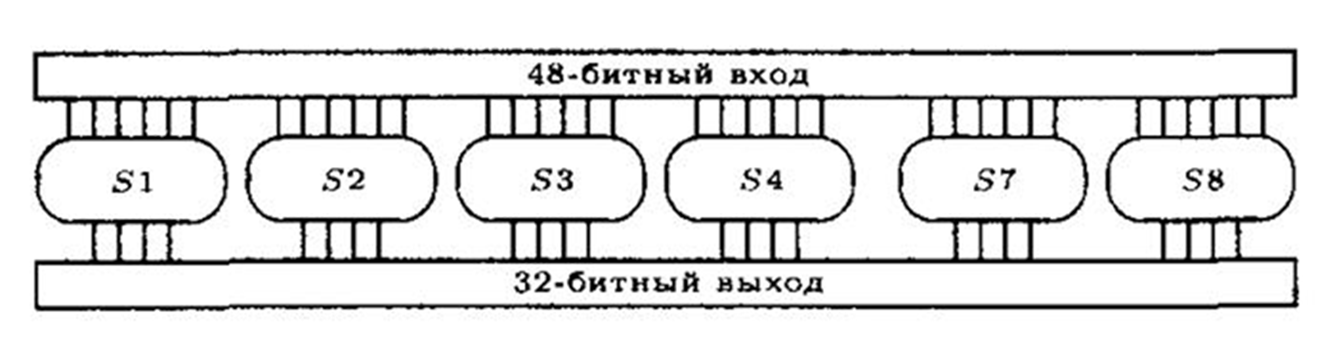
После объединения сжатого блока с расширенным блоком с помощью XOR над 48-битным результатом выполняется операция подстановки.

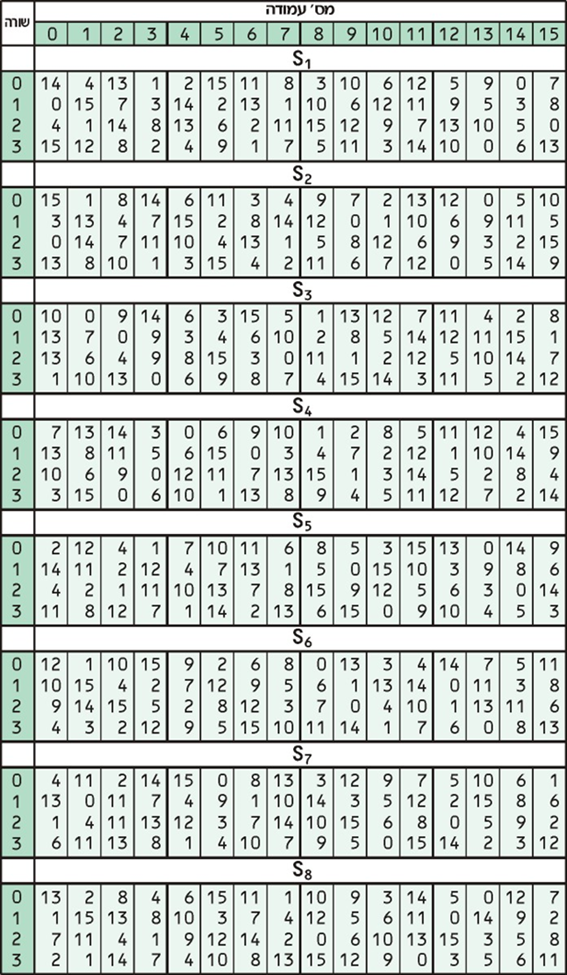
Подстановки производятся в восьми блоках подстановки, или S-блоках (от substitution).

У каждого S-блока есть 6-битный вход и 4-битный выход, всего используется восемь различных S-блоков.

48 битов делятся на восемь 6-битных подблоков.

Каждый отдельный подблок обрабатывается отдельным S-блоком: первый подблок - первым S-блоком, второй - вторым S-блоком и так далее.



Каждый S-блок представляет собой таблицу из четырех строк и шестнадцати столбцов. Каждый элемент в блоке является 4-битным числом. По шести входным битам S-блока определяется, под какими номерами столбцов и строк следует искать выходное значение.

Например, пусть на вход шестого S-блока (то есть биты функции XOR с 31 по 36) попадает 110011. Первый и последний биты, объединяясь, образуют 11, что соответствует строке три шестого S-блока. Средние четыре бита образуют 1001, что соответствует столбцу девять того же S-блока. Элемент шестого S-блока, находящийся на пересечении строки три и столбца девять, - это 14 (строки и столбцы нумеруются с нуля, а не с единицы). Вместо 110011 подставляется 1110.

**Дешифрование**

Процесс дешифрования аналогичен процессу шифрования.

На входе алгоритма используется зашифрованный текст, но ключи Ki используются в обратной последовательности.

K16 используется на первом раунде, K1 используется на последнем раунде.

Проблемой DES является малая длина ключа.

Также без ответа пока остается вопрос, возможен ли криптоанализ с использованием существующих характеристик алгоритма DES.

Основой алгоритма являются восемь таблиц подстановки, или S-boxes, которые применяются в каждой итерации.

Существует опасность, что эти S-boxes конструировались таким образом, что криптоанализ возможен для взломщика, который знает слабые места S-boxes.

В течение многих лет обсуждалось как стандартное, так и неожиданное поведение S-boxes, но все-таки никому не удалось обнаружить их фатально слабые места.

**Двойной DES**

Простейший способ увеличить длину ключа состоит в повторном применении DES с двумя разными ключами.

Используя незашифрованное сообщение P и два ключа K1 и K2, зашифрованное сообщение С можно получить следующим образом:

C = Ek2 [Ek1 [P]]

При дешифрования два ключа применяются в обратном порядке:

P = Dk1 [Dk2 [C]]

В этом случае длина ключа равна 56 \* 2 = 112 бит.

**Атака "встреча посередине"**

Для приведенного выше алгоритма двойного DES существует так называемая атака "встреча посередине".

Она основана на следующем свойстве алгоритма. Мы имеем

С = Ek2 [Ek1 [P]]

Тогда

X = Ek1 [P] = Dk2 [C].

Атака состоит в следующем.

* Требуется, чтобы атакующий знал хотя бы одну пару незашифрованный текст и соответствующий ему зашифрованный текст: (Р, С).
* Шифруется Р для всех возможных 256 значений K1.
* Результат запоминается в таблице, и затем таблица упорядочивается по значению Х.
* Дешифруется С, с применением всех возможных 256 значений K2.
* Для каждого выполненного дешифрования ищется равное ему значение в первой таблице.
* Если соответствующее значение найдено, то считается, что эти ключи могут быть правильными, и они проверяются для следующей известной пары незашифрованный текст, зашифрованный текст.

**Тройной DES с двумя ключами**

Очевидное противодействие атаке "встреча посередине" состоит в использовании третьей стадии шифрования с тремя различными ключами.

Это поднимает стоимость лобовой атаки до 2168, которая на сегодняшний день считается выше практических возможностей.

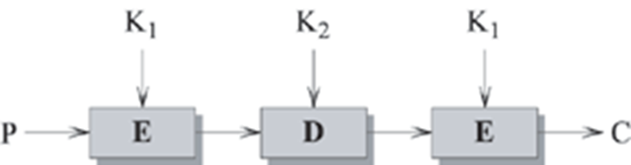
Но при этом длина ключа равна 56 \* 3 = 168 бит, что иногда бывает громоздко.

В качестве альтернативы предлагается метод тройного шифрования, использующий только два ключа.

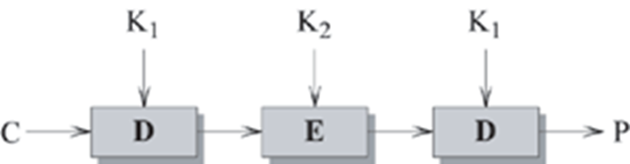
В этом случае выполняется последовательность зашифрование-расшифрование-зашифрование (EDE).

C = EK1 [DK2 [EK1 [P]]]

**Шифрование тройным DES**



**Дешифрование тройным DES**



Не имеет большого значения, что используется на второй стадии: шифрование или дешифрование.

В случае использования дешифрования существует только то преимущество, что можно тройной DES свести к обычному одиночному DES, используя K1 = K2:

C = EK1 [DK1 [EK1 [P]]] = EK1 [P]

Известных криптографических атак на тройной DES не существует.

Цена подбора ключа в тройном DES равна 2112.

## **Стандарт шифрования ГОСТ 28147-89**

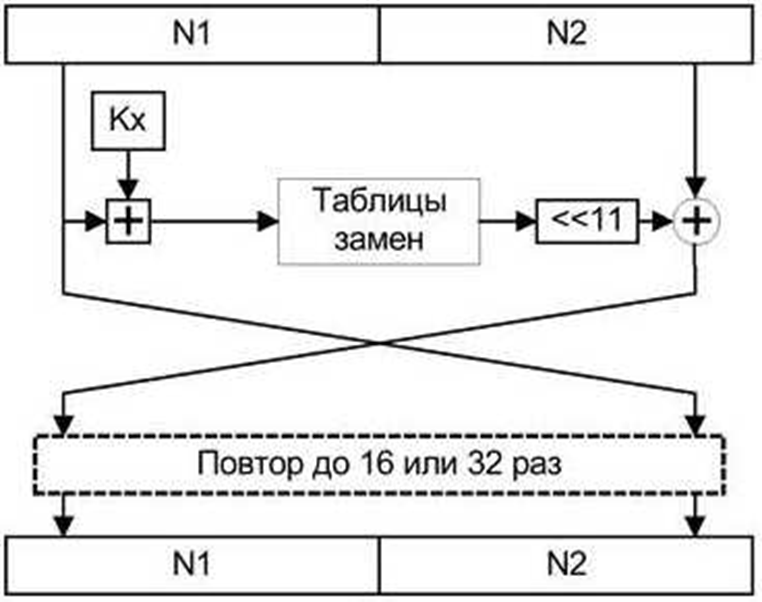
ГОСТ 28147-89 представляет собой симметричный 64-битовый блочный алгоритм с 256-битовым ключом.

Этот алгоритм криптографического преобразования данных предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации.

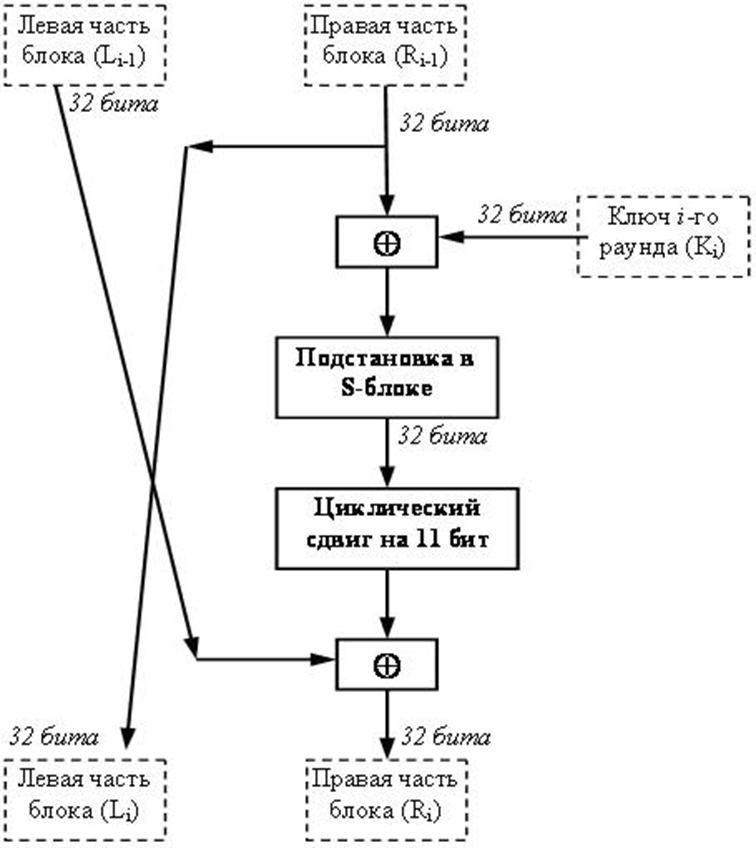
**Схема алгоритма ГОСТ 28147-89**

Данные, подлежащие зашифровке, разбивают на 64-разрядные блоки.

Эти блоки разбиваются на два субблока N1 и N2 по 32 бит



Структура одного раунда ГОСТ 28147-89



**Описание работы ГОСТ 28147-89**

Шифруемый блок данных разбивается на две части, которые затем обрабатываются как отдельные 32-битовые целые числа без знака.

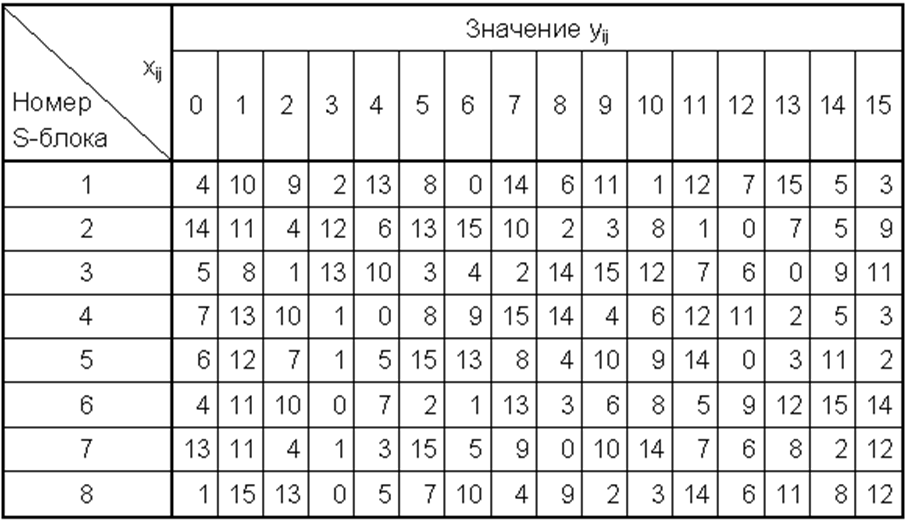
Сначала правая половина блока и подключ раунда складываются по модулю 232.

Затем производится поблочная подстановка.

32-битовое значение, полученное на предыдущем шаге (обозначим его S), интерпретируется как массив из восьми 4-битовых блоков кода: S=(S0,S1,S2,S3,S4,S5,S6,S7).

Далее значение каждого из восьми блоков заменяется на новое, которое выбирается по таблице замен

Таблица замен ГОСТ 28147-89



В каждой строке таблицы замен записаны числа от 0 до 15 в произвольном порядке без повторений.

Значения элементов таблицы замен взяты от 0 до 15, так как в четырех битах, которые подвергаются подстановке, может быть записано целое число без знака в диапазоне от 0 до 15.

Значение блока S1 (четыре младших бита 32-разрядного числа S) заменится на число, стоящее на позиции, номер которой равен значению заменяемого блока.

Например, в этом случае S1=0 заменится на 4, если S1=1, то оно заменится на 10 и т.д.

**Описание ГОСТ 28147-89**

После выполнения подстановки все 4-битовые блоки снова объединяются в единое 32-битное слово, которое затем циклически сдвигается на 11 битов влево.

Наконец, с помощью побитовой операции "сумма по модулю 2" результат объединяется с левой половиной, вследствие чего получается новая правая половина Ri.

Новая левая часть Li берется равной младшей части преобразуемого блока: Li= Ri-1.

Полученное значение преобразуемого блока рассматривается как результат выполнения одного раунда алгоритма шифрования.

**Процедуры шифрования и расшифрования**

ГОСТ 28147-89 является блочным шифром, поэтому преобразование данных осуществляется блоками в так называемых базовых циклах.

Базовые циклы заключаются в многократном выполнении для блока данных основного раунда, рассмотренного нами ранее, с использованием разных элементов ключа и отличаются друг от друга порядком использования ключевых элементов.

В каждом раунде используется один из восьми возможных 32-разрядных подключей.

Рассмотрим процесс создания подключей раундов.  
В ГОСТ эта процедура очень проста, особенно по сравнению с DES.  
256-битный ключ K разбивается на восемь 32-битных подключей, обозначаемых K0, K1, K2, K3, K4, K5, K6, K7.   
Алгоритм включает 32 раунда, поэтому каждый подключ при шифровании используется в четырех раундах в последовательности, представленной в таблице

Таблица Последовательность использования подключей при шифровании

Раунд 1 2 3 4 5 6 7 8

Подключ K0 K1 K2 K3 K4 K5 K6 K7

Раунд 9 10 11 12 13 14 15 16

Подключ K0 K1 K2 K3 K4 K5 K6 K7

Раунд 17 18 19 20 21 22 23 24

Подключ K0 K1 K2 K3 K4 K5 K6 K7

Раунд 25 26 27 28 29 30 31 32

Подключ K7 K6 K5 K4 K3 K2 K1 K0

Процесс расшифрования производится по тому же алгоритму, что и шифрование. Единственное отличие заключается в порядке использования подключей Ki. При расшифровании подключи должны быть использованы в обратном порядке, а именно, как указано в таблице

Таблица Последовательность использования подключей при расшифровании

Раунд 1 2 3 4 5 6 7 8

Подключ K0 K1 K2 K3 K4 K5 K6 K7

Раунд 9 10 11 12 13 14 15 16

Подключ K7 K6 K5 K4 K3 K2 K1 K0

Раунд 17 18 19 20 21 22 23 24

Подключ K7 K6 K5 K4 K3 K2 K1 K0

Раунд 25 26 27 28 29 30 31 32

Подключ K7 K6 K5 K4 K3 K2 K1 K0

**ГОСТ 28147-89 Режимы работы**

**Режим простой замены:** все блоки шифруются независимо друг от друга с разными подключами в разных раундах. Для одинаковых блоков сообщения М блоки шифртекста будут одинаковыми.

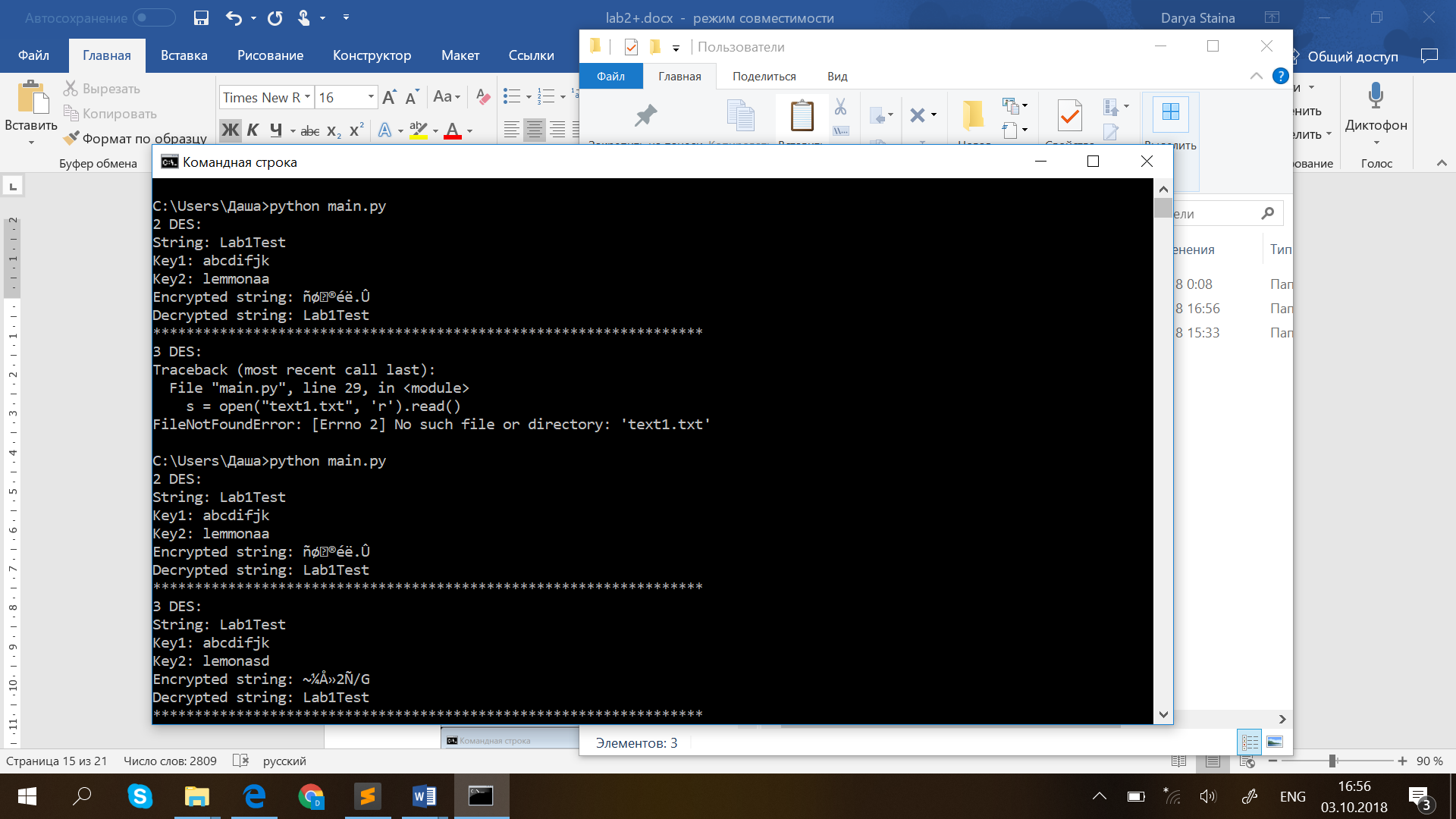
**Режим гаммирования:** В регистры N1 и N2 записывается 64-битовая синхропосылка (вектор инициализации) и шифруется с использованием СК. Результат подается на вход регистров и снова шифруется с использованием ключа. Получается «одноразовый блокнот».

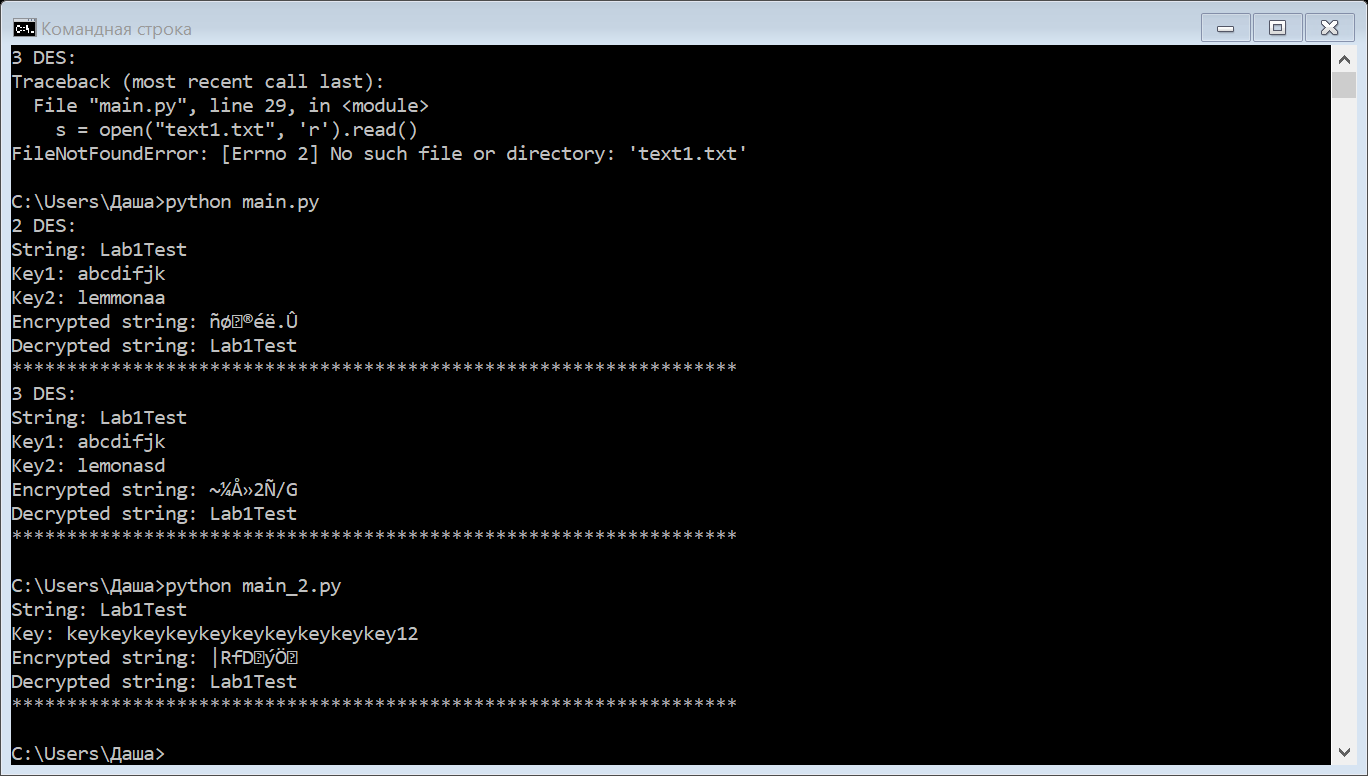
В **режиме гаммирования с обратной связью** для заполнения регистров N1 и N2, начиная со 2-го блока, используется результат зашифрования предыдущего блока открытого текста.

**Работа криптосистемы в режиме гаммирования**



# 4. Результаты выполнения программы





# 5. Выводы

|  |  |
| --- | --- |
| «Достоинства»: | «Недостатки»: |
| Двойной DES | |
| Надежнее обычного DES. | · Подвержен атаке «встреча посередине» |
| Тройной DES | |
| · Не подвержен атаке «встреча посередине»  · Известных криптографических атак на тройной DES не существует.  · Цена подбора ключа в тройном DES равна |  |
| ГОСТ 28147-89 | |
| · Не накладывает ограничений на степень секретности защищаемой информации | · Известны криптографические атаки на ГОСТ 28147-89. |

# 6. КОД ПРОГРАММЫ

**ГОСТ:**

def block\_transformation(B\_32):

B\_i = ""

S = (

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

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

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

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

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

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

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

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

)

for i in range(8):

temp = B\_32[4\*i: 4\*(i+1)]

value = int(("".join(temp[:])), 2)

cur = str(bin(S[i\*8 + value])[2:])

if len(cur) != 4:

cur = '0'\*(4 - len(cur)) + cur

B\_i = B\_i[:]+cur

B\_32 = "".join(B\_i)

return B\_32

def generation\_keys(key):

text\_bin = []

for symbol in key:

symbol\_bin = bin(ord(symbol))[2:]

if len(symbol\_bin) != 8:

symbol\_bin = '0'\*(8-len(symbol\_bin)) + symbol\_bin

text\_bin.append(symbol\_bin)

text\_bin = "".join(text\_bin)

return text\_bin

def splittingFileIntoBlocks(file):# split file on blocks with length 64 chars in binary form

text\_bin = []

for symbol in file:

symbol\_bin = bin(ord(symbol))[2:]

if len(symbol\_bin) != 8:

symbol\_bin = '0'\*(8-len(symbol\_bin)) + symbol\_bin

text\_bin.append(symbol\_bin)

text\_bin = "".join(text\_bin)

temp = len(text\_bin) % 64

if temp != 0:

text\_bin += "".join('0' for i in range(64 - temp))

block\_count = int(len(text\_bin) / 64)

blocks = [list(text\_bin[64\*i: 64\*(i+1)]) for i in range(block\_count)]

return blocks

def GOST(key, string):

file = string

blocks = splittingFileIntoBlocks(file)# split file on blocks with length 64 chars in binary form

#blocks = initial\_permutation(blocks)

key1 = generation\_keys(key)

for block in blocks:

for k in range(3):

for i in range(8):

L = block[:32]

R = block[32:]

k = key1[32\*i:32\*(i+1)]

R\_temp = int(("".join(R[:])), 2)

k\_temp = int(("".join(k[:])), 2)

R1 = (R\_temp + k\_temp) % (2 \*\* 32)

R1 = str(bin(R1))

R1 = R1[2:]

if len(R1) != 32:

R1 = '0'\*(32 - len(R1)) + R1

R1 = block\_transformation(R1)

R1 = R1[11:] + R1[:11]

R1\_temp = int(("".join(R1[:])), 2)

L\_temp = int(("".join(L[:])), 2)

R1 = R1\_temp ^ L\_temp

R1 = str(bin(R1))

R1 = R1[2:]

if len(R1) != 32:

R1 = '0'\*(32 - len(R1)) + R1

L = R[:]

R = R1[:]

block[:32] = L

block[32:] = R

for i in range(8):

L = block[:32]

R = block[32:]

k = key1[32\*(7-i):32\*((7-i)+1)]

R\_temp = int(("".join(R[:])), 2)

k\_temp = int(("".join(k[:])), 2)

R1 = (R\_temp + k\_temp) % (2 \*\* 32)

R1 = str(bin(R1))

R1 = R1[2:]

if len(R1) != 32:

R1 = '0'\*(32 - len(R1)) + R1

R1 = block\_transformation(R1)

R1 = R1[11:] + R1[:11]

R1\_temp = int(("".join(R1[:])), 2)

L\_temp = int(("".join(L[:])), 2)

R1 = R1\_temp ^ L\_temp

R1 = str(bin(R1))

R1 = R1[2:]

if len(R1) != 32:

R1 = '0'\*(32 - len(R1)) + R1

L = R[:]

R = R1[:]

block[:32] = L

block[32:] = R

resstr = ""

for block in blocks:

for i in range(8):

byte = block[8\*i: 8\*(i+1)]

byte = chr(int(("".join(byte)), 2))

resstr += byte

return resstr

def decryptStrFunction(key, string):

file = string

blocks = splittingFileIntoBlocks(file)

key1 = generation\_keys(key)

for block in blocks:

for i in range(8):

L = block[:32]

R = block[32:]

k = key1[32\*i:32\*(i+1)]

L\_temp = int(("".join(L[:])), 2)

k\_temp = int(("".join(k[:])), 2)

L1 = (L\_temp + k\_temp) % (2 \*\* 32)

L1 = str(bin(L1))

L1 = L1[2:]

if len(L1) != 32:

L1 = '0'\*(32 - len(L1)) + L1

L1 = block\_transformation(L1)

L1 = L1[11:] + L1[:11]

L1\_temp = int(("".join(L1[:])), 2)

R\_temp = int(("".join(R[:])), 2)

L1 = L1\_temp ^ R\_temp

L1 = str(bin(L1))

L1 = L1[2:]

if len(L1) != 32:

L1 = '0'\*(32 - len(L1)) + L1

R = L[:]

L = L1[:]

block[:32] = L

block[32:] = R

for k in range(3):

for i in range(8):

L = block[:32]

R = block[32:]

k = key1[32\*(7-i):32\*((7-i)+1)]

L\_temp = int(("".join(L[:])), 2)

k\_temp = int(("".join(k[:])), 2)

L1 = (L\_temp + k\_temp) % (2 \*\* 32)

L1 = str(bin(L1))

L1 = L1[2:]

if len(L1) != 32:

L1 = '0'\*(32 - len(L1)) + L1

L1 = block\_transformation(L1)

L1 = L1[11:] + L1[:11]

L1\_temp = int(("".join(L1[:])), 2)

R\_temp = int(("".join(R[:])), 2)

L1 = L1\_temp ^ R\_temp

L1 = str(bin(L1))

L1 = L1[2:]

if len(L1) != 32:

L1 = '0'\*(32 - len(L1)) + L1

R = L[:]

L = L1[:]

block[:32] = L

block[32:] = R

resstr = ""

for block in blocks:

for i in range(8):

byte = block[8\*i: 8\*(i+1)]

byte = chr(int(("".join(byte)), 2))

resstr += byte

return resstr

**Двойной и тройной DES:**

print ("2 DES: ")

s = open("text.txt", 'r').read()

print ("String: " + s)

key = "abcdifjk"

key2 = "lemmonaa"

print ("Key1: " + key)

print ("Key2: " + key2)

s1 = DES("".join(bin(ord(i))[2:] for i in key), s)

#s2 = ""

s2 = DES("".join(bin(ord(i))[2:] for i in key2), s1)

print ("Encrypted string: " + s2)

s3 = decryptStrFunction("".join(bin(ord(i))[2:] for i in key2), s2)

s4 = decryptStrFunction("".join(bin(ord(i))[2:] for i in key), s3)

s2.encode('utf8')

import codecs

f = codecs.open("text\_1.txt", 'w', 'utf8')

f.write(s2)

f.close()

print("Decrypted string: " + s4)

f = open("text\_2.txt", 'w').write(s4)

print ("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*")

print ("3 DES: ")

s = open("text1.txt", 'r').read()

#s = open("text.txt", 'r').read()

print ("String: " + s)

key = "abcdifjk"

key2 = "lemonasd"

print ("Key1: " + key)

print ("Key2: " + key2)

s1 = DES("".join(bin(ord(i))[2:] for i in key), s)

s2 = decryptStrFunction("".join(bin(ord(i))[2:] for i in key2), s1)

s3 = DES("".join(bin(ord(i))[2:] for i in key), s2)

print ("Encrypted string: " + s3)

f = codecs.open("text1\_1.txt", 'w', 'utf8')

f.write(s3)

f.close()

s2 = decryptStrFunction("".join(bin(ord(i))[2:] for i in key), s3)

s1 = DES("".join(bin(ord(i))[2:] for i in key2), s2)

s1 = decryptStrFunction("".join(bin(ord(i))[2:] for i in key), s1)

print("Decrypted string: " + s1)

f = open("text1\_2.txt", 'w').write(s1)

print ("\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*")