## **1. Введение**

В современном мире остро стоит вопрос о безопасности. Обеспечение безопасности является важным аспектом деятельности любой компании. Для обеспечения безопасности используется множество различных средств, как аппаратных, так и программных. Одним из таких средств является шифрование данных.

Шифрование — обратимое преобразование информации в целях сокрытия от [неавторизованных](https://ru.wikipedia.org/wiki/Авторизация) лиц, с предоставлением, в это же время, [авторизованным](https://ru.wikipedia.org/wiki/Авторизация) пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения [конфиденциальности](https://ru.wikipedia.org/wiki/Конфиденциальность) передаваемой информации.

Одним из самых распространенных алгоритмов для шифрования является DES и его модификации. DES — алгоритм для [симметричного](https://ru.wikipedia.org/wiki/Симметричный_шифр) [шифрования](https://ru.wikipedia.org/wiki/Шифрование), разработанный фирмой [IBM](https://ru.wikipedia.org/wiki/IBM) и утвержденный правительством [США](https://ru.wikipedia.org/wiki/США) в 1977 году как официальный стандарт. Размер блока для DES равен 64 [битам](https://ru.wikipedia.org/wiki/Бит). В основе алгоритма лежит [сеть Фейстеля](https://ru.wikipedia.org/wiki/Сеть_Фейстеля) с 16 циклами ([раундами](https://ru.wikipedia.org/wiki/Раунд_(в_криптографии))) и [ключом](https://ru.wikipedia.org/wiki/Ключ_(криптография)), имеющим длину 56 [бит](https://ru.wikipedia.org/wiki/Бит). Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований.

В ходе данной лабораторной работы необходимо изучить теоретическую часть об алгоритме шифрования DES, который необходимо использовать для шифрования данных, и на ее основании создать приложение, реализующее алгоритм DES.

1. **Теоретическая часть**

## **2.1. Алгоритм шифрования DES**

DES (англ. Data Encryption Standard) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3). Размер блока для DES равен 64 битам. В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Прямым развитием DES в настоящее время является алгоритм Triple DES (3DES). В 3DES шифрование/расшифровка выполняются путём троекратного выполнения алгоритма DES.

***Схема шифрования с помощью алгоритма DES:***

* ***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.

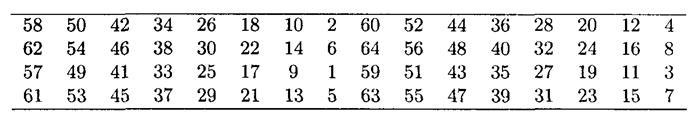


Рисунок 1 - DES. Начальная перестановка

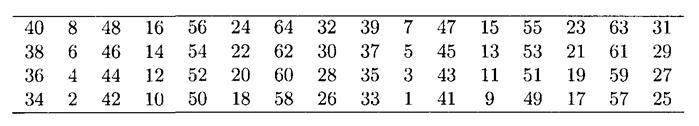


Рисунок 2 - DES. Заключительная перестановка

* ***Последовательность преобразований отдельного раунда***

Теперь рассмотрим последовательность преобразований, используемую в каждом *раунде*.

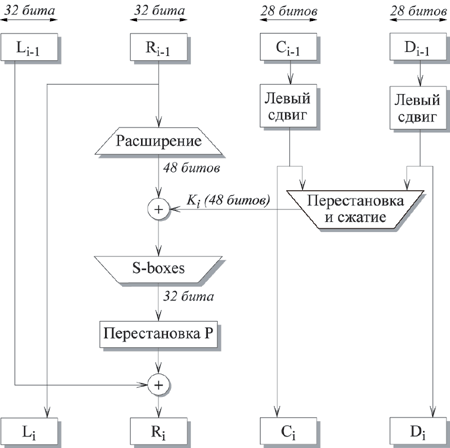


Рисунок 3 - i-ый раунд DES

64-битный входной блок проходит через 16 *раундов*, при этом на каждой итерации получается промежуточное 64-битное значение. Левая и правая части каждого промежуточного значения трактуются как отдельные 32-битные значения, обозначенные *L* и *R*. Каждую итерацию можно описать следующим образом:

Li = Ri-1

Ri = Li-1 F(Ri-1, Ki)

Где обозначает операцию XOR.

Таким образом, выход левой половины *Li* равен входу правой половины *Ri-1*. Выход правой половины *Ri*является результатом применения операции XOR к *Li-1* и функции *F*, зависящей от *Ri-1* и *Ki*.

Рассмотрим функцию *F* более подробно.

*Ri*, которое подается на вход функции *F*, имеет длину 32 бита. Вначале Ri расширяется до 48 бит, используя таблицу, которая определяет перестановку плюс расширение на 16 бит. Расширение происходит следующим образом. 32 бита разбиваются на группы по 4 бита и затем расширяются до 6 бит, присоединяя крайние биты из двух соседних групп. Например, если часть входного сообщения

. . . efgh ijkl mnop . . .

то в результате расширения получается сообщение

. . . defghi hijklm lmnopq . . .

После этого для полученного 48-битного значения выполняется операция XOR с 48-битным *подключом Ki*. Затем полученное 48-битное значение подается на вход функции подстановки, результатом которой является 32-битное значение.

Подстановка состоит из восьми *S-boxes,* каждый из которых на входе получает 6 бит, а на выходе создает 4 бита. Эти преобразования определяются специальными таблицами. Первый и последний биты входного значения *S-box* определяют номер строки в таблице, средние 4 бита определяют номер столбца. Пересечение строки и столбца определяет 4-битный выход. Например, если входом является 011011, то номер строки равен 01 (строка 1) и номер столбца равен 1101 (столбец 13). Значение в строке 1 и столбце 13 равно 5, т.е. выходом является 0101.

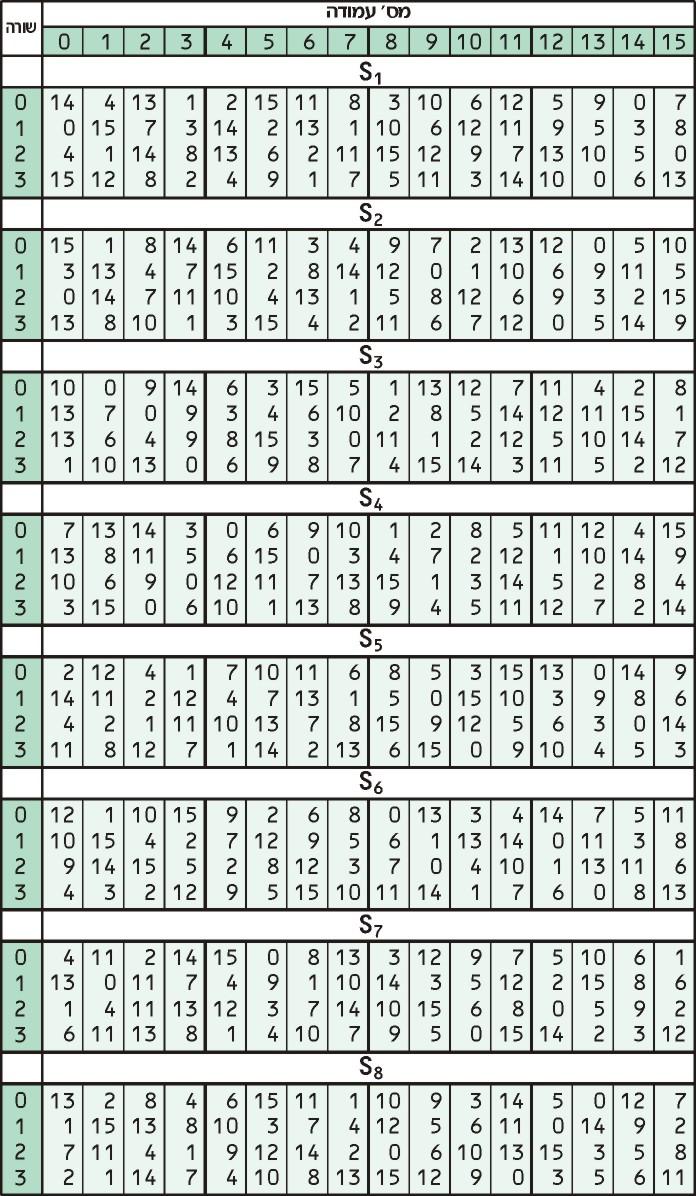


Рисунок 4 - S-boxes

Далее полученное 32-битное значение обрабатывается с помощью перестановки *Р*, целью которой является максимальное переупорядочивание бит, чтобы в следующем *раунде* шифрования с большой вероятностью каждый бит обрабатывался другим *S-box*.

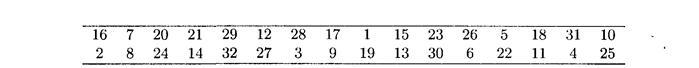


Рисунок 5 - Перестановка с помощью Р-блоков

* ***Создание подключей***

Ключ для отдельного *раунда Ki*состоит из 48 бит. Ключи *Ki* получаются по следующему алгоритму. Для 56-битного ключа, используемого на входе алгоритма (если используется 64-битный ключ, то, как видно из рис. 6 убираются биты 64, 56, 48, 40, 32, 16, 8), вначале выполняется перестановка в соответствии с таблицей Permuted Choice 1 (РС-1).

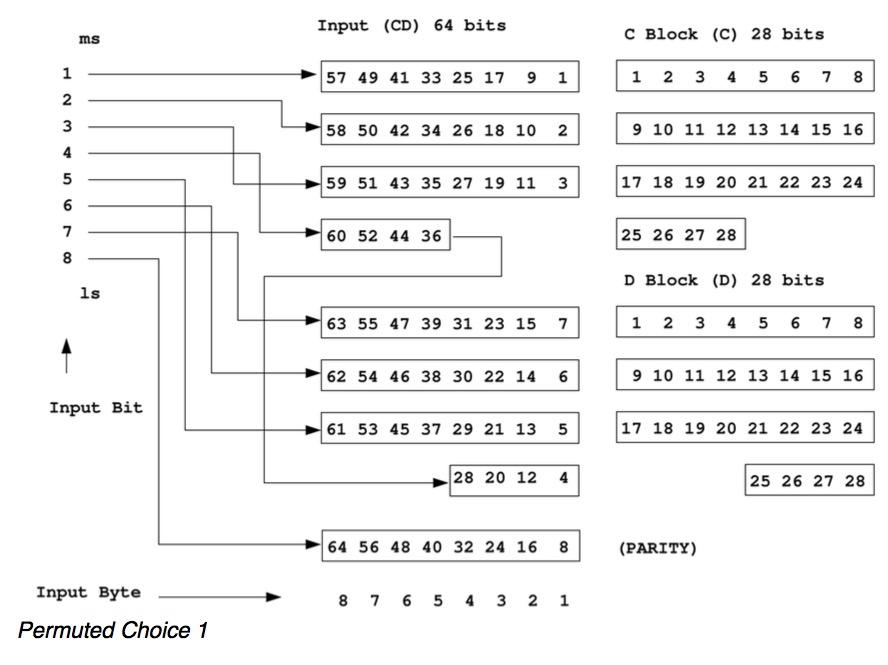


Рисунок 6 - Схема Permuted Choice

Полученный 56-битный ключ разделяется на две 28-битные части, обозначаемые как C0 и D0 соответственно. На каждом *раунде Ci* и *Di*независимо циклически сдвигаются влево на 1 или 2 бита, в зависимости от номера *цикла*.

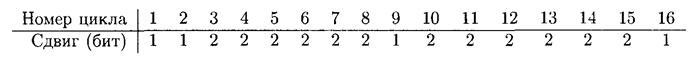


Рисунок 7 - Сдвиг ключа в зависимости от номера цикла

Полученные значения являются входом следующего *раунда*. Они также представляют собой вход в Permuted Choice 2 (РС-2), который создает 48-битное выходное значение, являющееся входом функции *F*(*Ri-1*, *Ki*).

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*.

## **2.2. Двойной DES**

Наиболее логичным способом противодействия полному перебору ключа DES выглядит многократное шифрование данных алгоритмом DES с различными ключами. Следующий алгоритм получил название Double DES (двойной DES):

где: — половины двойного ключа алгоритма Double DES, каждая из которых представляет собой обычный 56-битный ключ DES; Е — функция шифрования блока данных обычным алгоритмом DES. Если бы при двойном шифровании DES выполнялось следующее свойство:  для любых значений, то двойное шифрование не приводило бы к усилению против полного перебора ключа — всегда нашелся бы такой ключ *k*, *однократное* шифрование которым было бы эквивалентно двукратному шифрованию на ключах, а для нахождения ключа к достаточно было бы перебрать 255 ключей. Double DES действительно удваивает эффективный размер ключа— до 112 битов, а при современном развитии вычислительной техники полный перебор 112-битного ключа невозможен.

## **2.3. Тройной DES**

Triple DES (3DES) — симметричный [блочный шифр](https://ru.wikipedia.org/wiki/Блочный_шифр), созданный [Уитфилдом Диффи](https://ru.wikipedia.org/wiki/Диффи,_Уитфилд), [Мартином Хеллманом](https://ru.wikipedia.org/wiki/Хеллман,_Мартин) и Уолтом Тачманном в [1978 году](https://ru.wikipedia.org/wiki/1978_год) на основе алгоритма [DES](https://ru.wikipedia.org/wiki/DES) с целью устранения главного недостатка последнего — малой длины ключа (56 бит), который может быть взломан методом [полного перебора](https://ru.wikipedia.org/wiki/Полный_перебор) ключа. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше — время, требуемое для криптоанализа 3DES, может быть в миллиард раз больше, чем время, нужное для вскрытия DES. 3DES используется чаще, чем DES, который легко взламывается при помощи сегодняшних технологий (в [1998 году](https://ru.wikipedia.org/wiki/1998_год) организация [Electronic Frontier Foundation](https://ru.wikipedia.org/wiki/Electronic_Frontier_Foundation), используя специальный компьютер *DES Cracker*, вскрыла DES за 3 дня). 3DES является простым способом устранения недостатков DES. Алгоритм 3DES построен на основе DES, поэтому для его реализации возможно использовать программы, созданные для DES. Официальное название алгоритма, используемое в стандартах - TDEA или Triple DEA (англ. Triple Data Encryption Algorithm). Однако, термин "3DES" используется более широко поставщиками, пользователями и разработчиками криптосистем.

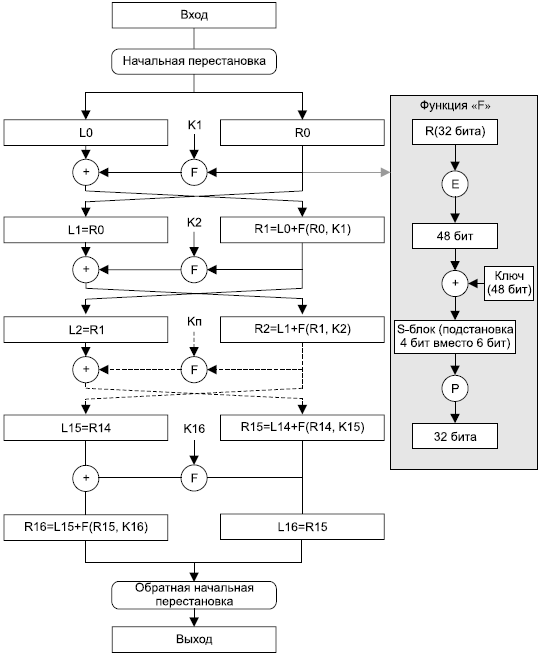
Существует 2 основных варианта шифрования алгоритмом 3DES: 3-key Triple DES и 2-key Triple DES. Как видно из названия, принципиальное различие этих методов - количество ключей (три и два соответственно). В свою очередь, каждый из этих алгоритмов имеет по 2 разных типа: EEE (encryption-encryption-encryption) и EDE (encryption-decryption-encryption) шифрование. Начнем с трех ключей:

* DES-EEE3: Исходный текст шифруется три раза, используя разные ключи.
* DES-EDE3: Исходный текст шифруется, затем дешифруется (уже другим ключом), затем снова шифруется (третьим ключом). Наглядное представление можно увидеть ниже.
* DES-EEE2: Исходный текст шифруется три раза, однако ключи на первом и последнем шаге одинаковые.
* DES-EDE2: Исходный текст шифруется, затем дешифруется (другим ключом), затем снова шифруется (ключом, используемым при первом шифровании).

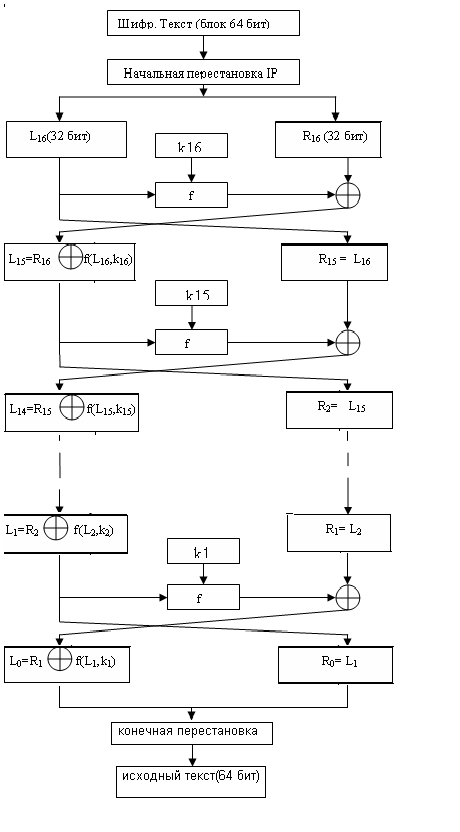
На практике, самый используемый тип 3DES шифрования - DES-EDE3.

## **3. Схема алгоритма**

Общая схема алгоритма *кодирования* для DES.



Общая схема алгоритма *декодирования* для DES.



## **4. Пример работы программы**

Рассмотрим пример программы. В исходном файле содержится текст:

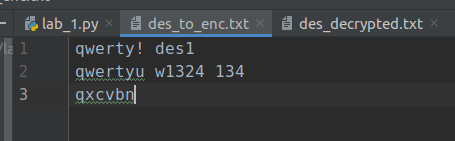


Рисунок 1. Исходный файл для DES

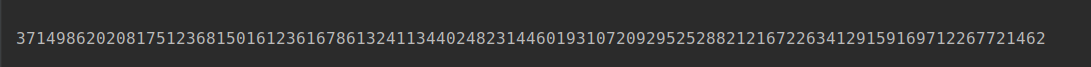


Рисунок 2. Зашифрованный при помощи DES текст

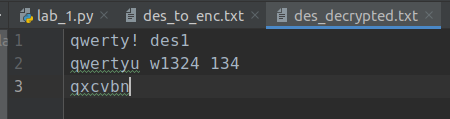


Рисунок 3. Результаты шифрования при помощи DES

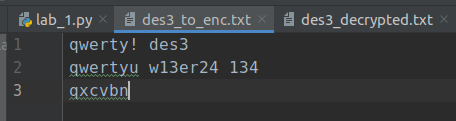


Рисунок 4. Исходный файл для DES3

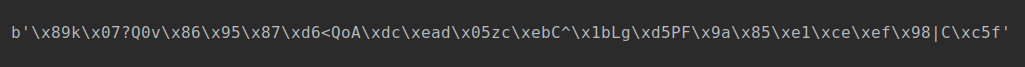


Рисунок 5. Зашифрованный при помощи DES3 текст

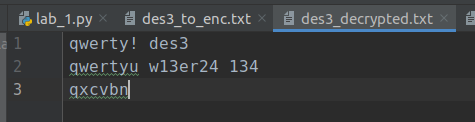


Рисунок 6. Результаты шифрования при помощи DES

## **5. Текст программы**

import unittest

from src.des import des\_decrypt, des\_encrypt, prepare\_des\_key

from src.des import des3\_decrypt, des3\_encrypt, prepare\_des3\_key, prepare\_iv

class TestStringMethods(unittest.TestCase):

def test\_des(self):

key = 'key'

block\_size = 8

key = prepare\_des\_key(key, block\_size)

# 1. Open file 'des3\_to\_enc.txt' & read text

file\_to\_enc = open('resources/lab\_1/des\_to\_enc.txt', 'r')

normal\_text = file\_to\_enc.read()

# 2. Encrypt read text

encrypted\_text = des\_encrypt(key, normal\_text, block\_size)

print()

print(''.join(map(lambda x: str(x), encrypted\_text)))

print()

# 3. Encrypt decrypted text

decrypted\_text = des\_decrypt(key, encrypted\_text, block\_size)

# 4. Save decrypted text to 'decrypted.txt'

decrypted\_file = open('resources/lab\_1/des\_decrypted.txt', 'w')

decrypted\_file.write(decrypted\_text)

self.assertEqual(normal\_text, decrypted\_text)

def test\_des3(self):

key = 'key'

key\_size = 16

block\_size = 8

key = prepare\_des3\_key(key, key\_size)

iv = prepare\_iv(block\_size)

# 1. Open file 'des3\_to\_enc.txt' & read text

file\_to\_enc = open('resources/lab\_1/des3\_to\_enc.txt', 'r')

normal\_text = file\_to\_enc.read()

# 2. Encrypt read text

encrypted\_text = des3\_encrypt(key, iv, normal\_text)

print()

print(encrypted\_text)

print()

# 3. Encrypt decrypted text

decrypted\_text = des3\_decrypt(key, iv, encrypted\_text)

# 4. Save decrypted text to 'decrypted.txt'

decrypted\_file = open('resources/lab\_1/des3\_decrypted.txt', 'w')

decrypted\_file.write(decrypted\_text)

self.assertEqual(normal\_text, decrypted\_text)

if \_\_name\_\_ == '\_\_main\_\_':

unittest.main()

from Crypto.Util.Padding import pad, unpad

from Crypto.Cipher import DES, DES3

from Crypto import Random

def des\_encrypt(key, msg, pad\_block\_size=8):

cipher = DES.new(key, DES.MODE\_ECB)

msg = cipher.encrypt(pad(msg.encode('utf-8'), pad\_block\_size))

return msg

def des\_decrypt(key, msg, pad\_block\_size=8):

decipher = DES.new(key, DES.MODE\_ECB)

msg = decipher.decrypt(msg)

msg = unpad(msg, pad\_block\_size).decode('utf-8')

return msg

def prepare\_des\_key(key, pad\_block\_size=8):

return pad(key.encode('utf-8'), pad\_block\_size)

def des3\_encrypt(key, iv, msg, pad\_block\_size=8):

encipher = DES3.new(key, DES3.MODE\_OFB, iv)

msg = encipher.encrypt(pad(msg.encode('utf-8'), pad\_block\_size))

return msg

def des3\_decrypt(key, iv, msg, pad\_block\_size=8):

decipher = DES3.new(key, DES3.MODE\_OFB, iv)

msg = decipher.decrypt(msg)

msg = unpad(msg, pad\_block\_size).decode('utf-8')

return msg

def prepare\_des3\_key(key, pad\_key\_size=16):

return pad(key.encode('utf-8'), pad\_key\_size)

def prepare\_iv(pad\_block\_size=8):

return Random.new().read(pad\_block\_size) # DES3.block\_size==8

## **6. Вывод**

DES был национальным стандартом США в 1977—1980 гг., но в настоящее время DES используется (с ключом длины 56 бит) только для устаревших систем, чаще всего используют его более криптоустойчивый вид (3DES, DESX). 3DES является простой эффективной заменой DES, и сейчас он рассмотрен как стандарт. В ближайшее время DES и Triple DES будут заменены алгоритмом AES (Advanced Encryption Standard — Расширенный Стандарт Шифрования).