**Министерство науки и высшего образования Рф**

**ФГБОУ ВО «БРЯНСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**Кафедра «Информатика и программное обеспечение»**

**КРУСОВАЯ РАБОТА**

**по дисциплине «Защита информации»**

**Всего листов 27**

Студент гр. О-19-ИВТ1-ПО-Б

Зач. кн.№ 19.0281

\_\_\_\_\_\_\_\_\_\_\_Бабаев М.Д.

«12» октября 2022 г.

Преподаватель

\_\_\_\_\_\_\_\_\_Дергачев К.В.

«12» октября 2022 г.

**Брянск** **2022 г.**

# Описание Алгоритма DES

## Общее описание

DES ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Data Encryption Standard) — алгоритм для [симметричного](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80) [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), разработанный фирмой [IBM](https://ru.wikipedia.org/wiki/IBM) и утверждённый правительством [США](https://ru.wikipedia.org/wiki/%D0%A1%D0%A8%D0%90) в 1977 году как официальный стандарт ([FIPS](https://ru.wikipedia.org/wiki/FIPS) 46-3). Размер блока для DES равен 64 [битам](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82). В основе алгоритма лежит [сеть Фейстеля](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D1%8C_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F) с 16 циклами ([раундами](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%83%D0%BD%D0%B4_(%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8))) и [ключом](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), имеющим длину 56 [бит](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82). Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований.

Для DES рекомендовано несколько режимов:

1. [ECB](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F#Electronic_Codebook_(ECB)) - режим «электронной кодовой книги» (простая замена);
2. [CBC](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F#Cipher_Block_Chaining_(CBC)) - режим сцепления блоков;
3. [CFB](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F#Cipher_Feedback_(CFB)) - режим обратной связи по [шифротексту](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82);
4. [OFB](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F#Output_Feedback_(OFB)) - режим обратной связи по выходу;

В рамках данной курсовой работы будет рассматриваться режим CBC

## Схема шифрования

Схема шифрования DES представлена на рис. 1. Она состоит из начальной и конечной перестановки (ранее было реализовано аппаратно), и 16 раундов шифрования. Исходный текст разбивается на блоки по 64 бита. Далее, блок разделяется на L и R блоки по 32 бита (левый и правый). Правый блок преобразуется при помощи функции f c применением ключа 48 бит. Далее, выполняется операция XOR левого и правого блока.И наконец, на следующей итерации L и R меняются местами.

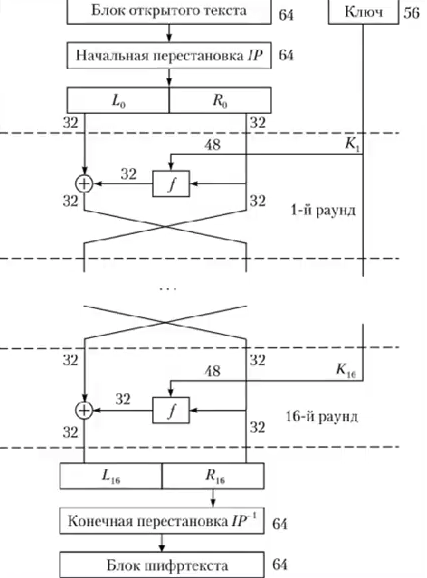


Рис. 1. Схема шифрования DES

## Функция Фейстеля

Схема функции f представлена на рис. 2. Правый блок проходит через функция расширения E (при помощи дублирования некоторых битов), в результате чего на выходе получается 48 битный блок. Далее, происходит операция складывания по модулю 2 с 48 битным ключом k. Далее, результат разделяется на 8 подблоков по 6 бит каждый. Затем, каждый блок трансформируется в новые блок по 4 бита при помощи преобразования S. И наконец, данные блоки проходят стадию перестановки P.

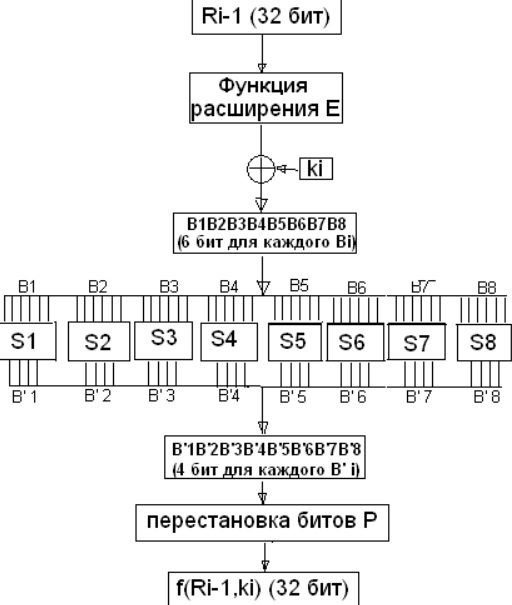


Рис. 2. Функция f

## Генерация ключей

Генерирование ключей представлено на рис. 3. В исходном 64 битном ключе выделяются 56 значащих битов (каждый 8-й бит не учитывается). Далее, 56 битный ключ разделяется на 2 блока, для каждого из которых выполняется перестановка С и D. На каждом раунде происходит циклический сдвиг влево для C и D. Далее, эти блоки складываются и над результирующим блоком происходит сжимающая перестановка, в результате чего получается 48 битный ключ.

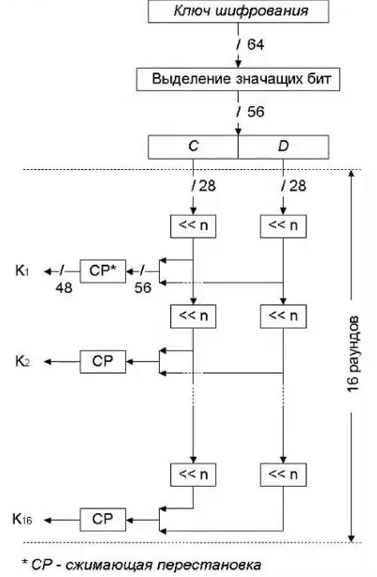


Рис. 3. Преобразование ключей

# Сравнения алгоритма DES с аналогами

Использование сети Фейстеля и размер блока в 64 в DES является достаточно медленным и не используется в программном обеспечении. Короткая длина ключа в 56 бит дает возможность подобрать ключ на основе быстрого полного перебора ключей на современной вычислительной машине.

## 3DES

Этот алгоритм применял алгоритм DES к блоку 3 раза. Длина ключе составляла 112 и 168 бит. Но всё же, благодаря современным методам криптологии и суперкомпьютерам, 3DES также имеет некоторые серьезные уязвимости

## Blowfish

Blowfish - это еще один метод шифрования с симметричным ключом, разработанный [Брюсом Шнайером](https://translated.turbopages.org/proxy_u/en-ru.ru.9636c257-6345f2fd-f57c06ea-74722d776562/https/en.wikipedia.org/wiki/Bruce_Schneier) в 1993 году в качестве альтернативы алгоритму шифрования DES. Его длина ключа составляет 446 бит и намного лучше, чем у DES и 3DES. Поэтому взломать ключ Blowfish сложнее. Он также имеет размер блока 64 бита. Его также можно использовать в программном обеспечении.

## AES

AES - это еще один алгоритм шифрования, который защищает данные от злоумышленников. В настоящее время это один из самых надежных доступных алгоритмов шифрования.

Поскольку AES использует один и тот же ключ как для шифрования, так и для дешифрования данных, это также симметричный тип шифрования. Существует три типа длин ключей шифрования AES 128, 192 и 256 бит. Каждая длина ключа имеет различные возможные комбинации. Он имеет структуру, отличную от других алгоритмов шифрования, он использует сеть подстановки-перестановки.

Хотя длина ключа метода шифрования AES варьируется, размер его блока фиксирован как 128 бит или 16 байт.

Итоговое сравнение алгоритмов шифрования представлено в таблице 1.

Таблица 1

Итоговое сравнение

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | DES | 3DES | Blowfish | AES |
| Длина ключа, бит | 56 | 112/168 | 448 | 128/192/256 |
| Размер блока, бит | 64 | 64 | 64 | 128 |
| Скорость | Медленно | Медленно | Быстро | Быстро |
| Защита | Не достаточная | Не достаточная | Достаточная | Отличная |
| Основан на алгоритме | сеть Фейстеля | сеть Фейстеля | сеть Фейстеля | сеть подстановки-перестановки |
| Время, необходимое для перебора всех возможных ключей со скорость 50 млрд ключей в секунду, дней | 400 | 800 | ~3200 | 5\*10^21 |