**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.

«18» октября 2022 г.

Преподаватель

\_\_\_\_\_\_\_\_\_Дергачев К.В.

«18» октября 2022 г.

**Брянск** **2022 г.**

# Аналитическая часть

## DES

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.

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.

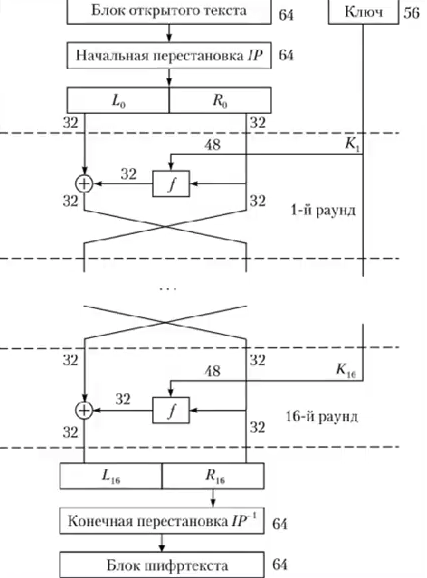


Рис. 1. Схема шифрования DES

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.

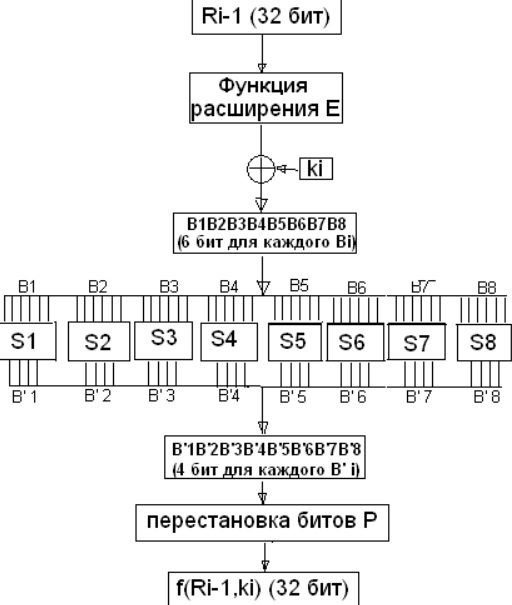


Рис. 2. Функция f

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.

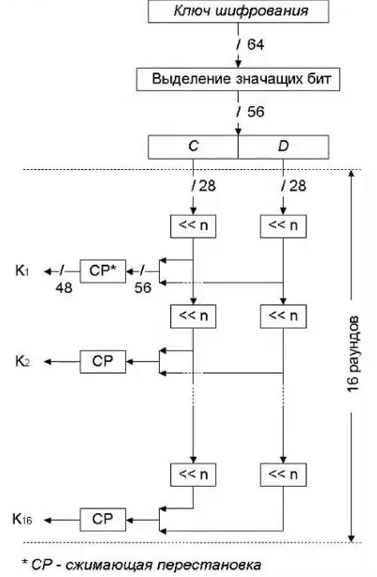


Рис. 3. Преобразование ключей

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

Triple DES (3DES) — симметричный [блочный шифр](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80), созданный [Уитфилдом Диффи](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%84%D1%84%D0%B8,_%D0%A3%D0%B8%D1%82%D1%84%D0%B8%D0%BB%D0%B4), [Мартином Хеллманом](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD,_%D0%9C%D0%B0%D1%80%D1%82%D0%B8%D0%BD) и Уолтом Тачманном в [1978 году](https://ru.wikipedia.org/wiki/1978_%D0%B3%D0%BE%D0%B4) 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/%D0%9F%D0%BE%D0%BB%D0%BD%D1%8B%D0%B9_%D0%BF%D0%B5%D1%80%D0%B5%D0%B1%D0%BE%D1%80) ключа.

Схема шифрования 3DES представлена на рис. 4.

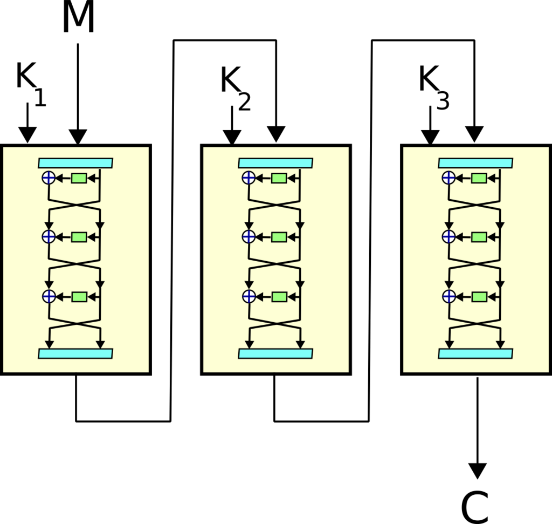


Рис. 4. Схема шифрования 3DES

Как видно из рис. 4 данный алгоритм применял алгоритм DES к блоку 3 раза, где k1, k2 и k3 – ключи для каждого DES-шага. Варианты выбора ключей таковы:

1. Все ключи независимы
2. Все ключи равны
3. k1 = k3, k1 и k2 независимы

Самым безопасным является первый вариант: длина ключа DES равна 56 битов, а длина 3DES в 3 раза больше, то есть равна 168 битов (в каждом байте 64-разрядного ключа DES используется только 7 битов, поэтому на самом деле длина ключа равна 56 битов, а не 64, и длина ключа 3DES равна 168, а не 192 бита).

Второй вариант является несколько менее стойким, с длиной ключа, равной 2 × 56 = 112 бит. Однако, этот вариант шифрования более надежен, чем обычное двойное шифрование с помощью DES с ключами k1 и k2.

Третий вариант эквивалентен по надежности DES: здесь длина ключа тоже равна 56 битам. При использовании алгоритма DES-EDE3, из-за такого выбора ключей, шифрование (первый шаг) и расшифрование (второй шаг) сводят друг друга на нет. Такой выбор ключей теперь не рекомендуется [национальным институтом стандартов и технологий](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%BE%D0%B2_%D0%B8_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9) (НИСТ) и не поддерживается стандартом ISO/IEC 18033-3.

Каждый ключ DES хранится и передается как 8 байтов, каждый байт - с [нечетным паритетом](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82_%D1%87%D1%91%D1%82%D0%BD%D0%BE%D1%81%D1%82%D0%B8), так что полный набор ключей займет 24 байта в первом варианте, 16 во втором и 8 в третьем.

## 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.

Алгоритм представлен на рис. 5.

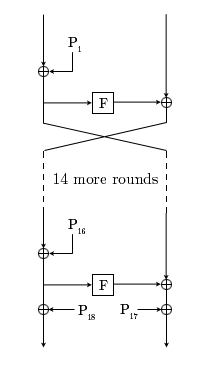


Рис. 5. Схема шифрования Blowfish

Параметрами алгоритма являются:

1. Секретный ключ K (от 32 до 448 бит)
2. 32-битные ключи шифрования P1…P18
3. 32-битные таблицы замен S1…S4

Сам алгоритм разделён на 2 этапа

1. Формирование ключей шифрования по секретному ключу. Здесь происходит инициализация массивов P и S при помощи секретного ключа K. В начале, массивы P инициализируются мантиссой числа Пи, а затем производится операция XOR над P и соответствующими 32 битами ключа. Далее происходит шифрование ключей и таблиц замен: алгоритм шифрования 64-битного блока, используя инициализированные ключи и таблицы замен шифрует 64-битную нулевую строку. Результат записывается в P1 и P2. P1 и P2 шифруются изменёнными значениями ключей и таблиц замен. Результат записывается в P3 и P4. Так продолжается до изменения всех ключей и таблиц замен.
2. Шифрование текста полученными ключами и F(x), представленной на рис 6, с предварительным разбиением на блоки по 64 бита. Если невозможно разбить начальный текст точно на блоки по 64 бита, используются различные [режимы шифрования](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) для построения сообщения, состоящего из целого числа блоков. Суммарная требуемая память 4168 байт.

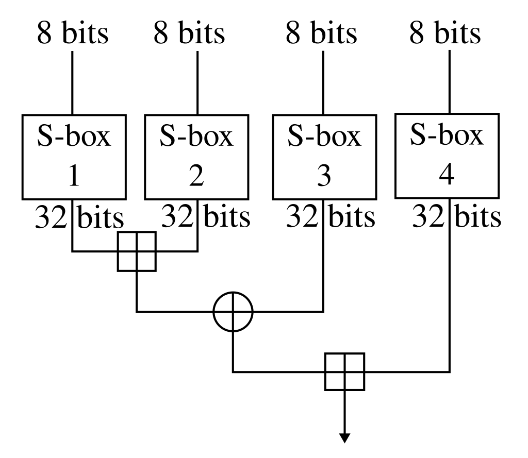


Рис. 6. Функция F(x) в Blowfish

Функция F(x) работает по следующему принципу: она принимает блок в 32 бита и проделывает над ним следующие операции:

1. 32-битный блок делится на блоки по 8 бит (X1, X2, X3, X4).
2. Первый и второй блок складываются по модулю 232 , полученный результат складывается по модулю 2 с третьим блоком, и наконец, полученный блок складываются по модулю 232 с последним.
3. Результат данных операций – значение функции F(x).

## AES

AES - [симметричный алгоритм](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%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) [блочного шифрования](https://ru.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80) (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта [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) [правительством США](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE_%D0%A1%D0%A8%D0%90) по результатам [конкурса AES](https://ru.wikipedia.org/wiki/AES_(%D0%BA%D0%BE%D0%BD%D0%BA%D1%83%D1%80%D1%81)). Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником [DES](https://ru.wikipedia.org/wiki/DES).

Предварительно входные данные разбиваются на блоки по 16 байт, если полный размер не кратен 16 байтам, то данные дополняется до размера, кратного 16 байтам. Блоки представляются в виде матрицы 4x4 — state. Далее происходит процедура расширения ключа и к каждому блоку state применяются операции 2-4. Итак, алгоритм состоит из следующих шагов:

1. Расширение ключа - KeyExpansion;
2. Начальный раунд - сложение state с основным ключом;
3. 9 раундов шифрования, каждый из которых состоит из преобразований: SubBytes, ShiftRows, MixColumns, AddRoundKey/
4. Финальный раунд, состоящий из преобразований: SubBytes, ShiftRows, AddRoundKey

**SubBytes** - замена байтов state по таблице S-box. Каждый байт представляется в виде двух шестнадцатеричных чисел b = (x, y), где x определяется 4 старшими разрядами b, а y — 4 младшими. В таблице S-box размера 16x16 находятся значения для замены исходного байта: значение b' на пересечении строки x и столбца y S-box используется в качестве замены исходному байту b.

**ShiftRows** - циклический сдвиг строк state. Нулевая строка остается на месте, первая смещается влево на 1 байт, вторая на 2 байта и третья на 3 соответственно.

**MixColumns** - умножения каждого столбца state на фиксированную матрицу. Таким образом осуществляется линейное преобразование над столбцами state. Причем умножение и сложение производится по правилам, описанным выше.

**AddRoundKey -** раундовый ключ поэлементно добавляется к state с помощью поразрядного XOR.

**KeyExpansion -** процедура расширения основного ключа для создания раундовых ключей, которые затем используются в раундах шифрования. Расширенный ключ состоит из 44 четырехбайтовых слов (wi): 4 слова на основной ключ и по 4 слова на 10 раундовых ключей. Таким образом, полная длина расширенного ключа составляет 1408 бит.

Операция расширения ключа использует массив Rcon и состоит из следующих действий:

1. Четыре слова основного ключа переносятся в первые четыре слова расширенного ключа.
2. Если число i без остатка делится на 4, то
3. Иначе:

Операция RotByte производит циклическую перестановку байта исходного слова:

## Режимы работы

Существуют следующие режимы работы

1. Режим ECB (режим электронной кодовой книги), где каждый блок шифруется отдельно. Представлен на рис. 7.

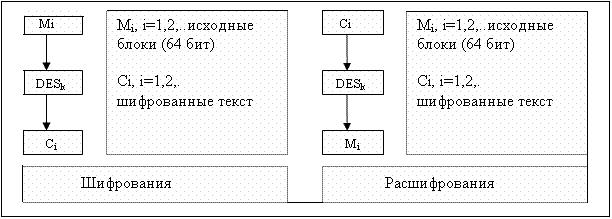


Рис. 7. Режим ECB

1. Режим CBC (режим сцепления блоков), где каждый очередной блок перед зашифрованием складывается по модулю 2 с предыдущим блоком. Представлен на рис. 8.

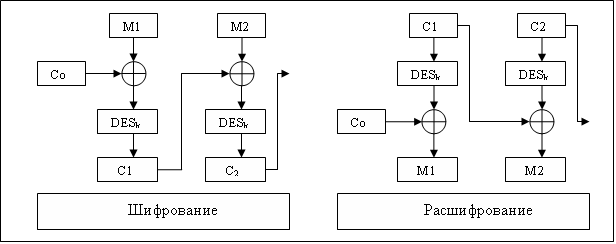


Рис. 8. Режим CBC

1. Режим CFB (режим обратной связи по шифртексту), в которой вырабатывается начальная гамма . Начальный вектор является синхропосылкой и предназначен для того, чтобы разные наборы данных шифровались по-разному с применением одного и того же секретного ключа. Синхропосылка посылается получателю в открытом виде вместе с зашифрованным файлом. Представлен на рис. 9.

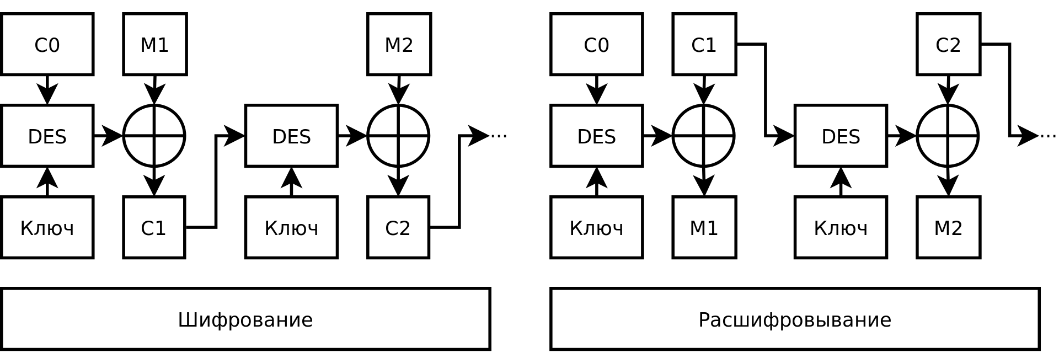


Рис. 9. Режим CFB

1. Режим OFB (режим обратной связи по выходу), где вырабатывается блочная гамма . Представлен на рис. 10.

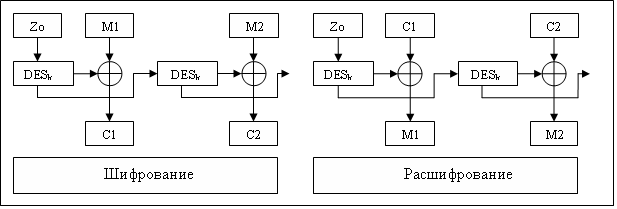


Рис. 10. Режим OFB

## Сравнительный анализ

Сравнительный анализ всех вышеупомянутых алгоритмов представлен 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 |
| Размер подблока, бит | 32 | 32 | 32 | 256 |
| Количество раундов | 16 | 16\*3 | 16 | 11 |
| Количество раундовых ключей | 16 | 16\*3 | 18 | 11 |
| Используемые операции | сложение по модулю 2, циклический сдвиг | сложение по модулю 2, циклический сдвиг | Сложение по модулю 232 сложение по модулю 2 | сложение по модулю 2, циклический сдвиг |
| Скорость | Медленно | Медленно | Быстро | Быстро |
| Структура | 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 |