Федеральное государственное образовательное бюджетное учреждение высшего образования

«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ

РОССИЙСКОЙ ФЕДЕРАЦИИ»

(Финансовый университет)

**Колледж информатики и программирования**

Самостоятельная работа № 1 по дисциплине

МДК.02.02 «Криптографические средства и методы защиты информации»

На тему: «Программная реализация симметричного криптографического алгоритма DES»

Студент группы 3ОИБАС*-№ группы*

|  |  |
| --- | --- |
| *Королев Тимофей Андреевич* | «31» 01 2023 г. |

Основная профессиональная образовательная программа по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Форма обучения очная

Проверили: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Рой А.В.,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Рой О.В.

Москва

2020

Оглавление

[Введение 3](#_Toc126253461)

[Цель работы 3](#_Toc126253462)

[Задачи работы: 3](#_Toc126253463)

[Надежность использования DES 4](#_Toc126253464)

[Основная часть 5](#_Toc126253465)

[Теоретические сведенья 5](#_Toc126253466)

[Выводы 14](#_Toc126253467)

[Список литературы 15](#_Toc126253468)

# Введение

Применение алгоритма DES является актуальной и за:

* резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации;
* резкое увеличение объёмов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
* сосредоточение в единых базах данных информации различного назначения и различной принадлежности;
* высокие темпы роста парка персональных компьютеров, находящиеся в эксплуатации в самых разных сферах деятельности;
* резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
* бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;
* повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;
* развитие глобальной сети Internet, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

Цель работы: Получить навыки по реализации алгоритма DES.

# Задачи работы:

* Изучить теорию по теме «Зарубежные симметричные алгоритмы DES, AES, IDEA. Алгоритмы DES и AES: Основные сведения.»
* Изучить примеры выполнения заданий
* Выполнить задания по своему варианту, подробно описав решение.

Объектом исследования является: алгоритм шифрования DES.

Предметом исследования является симметричные алгоритмы шифрования.

## Надежность использования DES

Приведем несколько практических рекомендаций, обеспечивающих безопасность зашифрованных данных. Ключи DES нужно менять довольно часто, чтобы предотвратить атаки, требующие анализа достаточно большого количества данных. Если говорить о защите передаваемых данных, то необходимо найти защищенный способ передачи DES ключа от отправителя к получателю. Обе эти проблемы решаются с помощью алгоритма RSA или какой-либо другой асимметричной криптосистемы: для каждого сеанса связи создается новый DES ключ, зашифровывается общим ключом получателя и в таком виде передается получателю. В таких обстоятельствах криптосистема RSA выступает как инструмент повышения защищенности DES (или любого другого секретно-ключевого шифра).

Если использовать DES для шифрования файлов на жестком диске, то часто менять ключи малореально, так как для этого необходимо расшифровать, а затем зашифровать все файлы новым ключом. Вместо этого можно создать главный ключ DES, каким будет зашифрованный список ключей DES, используемых для шифрования файлов; в этом случае главный ключ можно менять так часто как это нужно. Но так как главный ключ более привлекателен для атаки чем отдельные DES ключи, то его разумно шифровать алгоритмом Triple DES.

На практике используются несколько официально определенные режимы шифрования DES; каждый из этих режимов имеет разные свойства. Режим ЕСВ (электронная кодовая книга) последовательно шифрует каждый 64-битный блок открытого текста тем самым 56-битным ключом DES. В режиме СВС (формирование цепочки блока шифра) каждый 64-битный блок открытого текста перед шифрованием DES ключом логически суммируется (XOR) с предыдущим блоком зашифрованного текста. Таким образом, шифрование каждого следующего блока зависит от предыдущих блоков и поэтому тот же 64-битный блок открытого текста может быть представлен различными блокам зашифрованного текста в зависимости от его размещения в исходном сообщении. СВС позволяет защититься от некоторых атак, но не от полного поиска или дифференциального криптоанализа. Режим CFB (шифрование с обратной связью) позволяет использовать DES блоками длиной менее 64 бит. Подробные описания различных режимов DES приведены в [NIS80]. Режим OFB по существу позволяет использовать DES как потоковый шифр. Из перечисленных режимов DES наиболее широко на практике используется режим СВС, являющийся частью нескольких стандартов. Для повышения защиты можно использовать режим СВС с тройным шифрованием.

# Основная часть

## Теоретические сведенья

Одной из наиболее известных криптографических систем с закрытым ключом является *DES – Data Encryption Standard*. Эта система первой получила статус государственного стандарта в области шифрования данных. Она разработана специалистами фирмы IBM и вступила в действие в США 1977 году. Алгоритм *DES* широко использовался при хранении и передаче данных между различными вычислительными системами; в почтовых системах, в электронных системах чертежей и при электронном обмене коммерческой информацией. Стандарт *DES* реализовывался как программно, так и аппаратно. Предприятиями разных стран был налажен массовый выпуск цифровых устройств, использующих *DES* для шифрования данных. Все устройства проходили обязательную сертификацию на соответствие стандарту.

Несмотря на то, что уже некоторое время эта система не имеет статуса государственного стандарта, она по-прежнему широко применяется и заслуживает внимания при изучении блочных шифров с закрытым ключом.

Длина ключа в алгоритме *DES* составляет 56 бит. Именно с этим фактом связана основная полемика относительно способности *DES* противостоять различным атакам. Как известно, любой блочный шифр с закрытым ключом можно взломать, перебрав все возможные комбинации ключей. При длине ключа 56 бит возможны 256 разных ключей. Если компьютер перебирает за одну секунду 1 000 000 ключей (что примерно равно 220), то на перебор всех 256 ключей потребуется 236 секунд или чуть более двух тысяч лет, что, конечно, является неприемлемым для злоумышленников.

Однако возможны более дорогие и быстрые вычислительные системы, чем персональный компьютер. Например, если иметь возможность объединить для проведения параллельных вычислений миллион процессоров, то максимальное время подбора ключа сокращается примерно до 18 часов. Это время не слишком велико, и криптоаналитик, оснащенный подобной дорогой техникой, вполне может выполнить вскрытие данных, зашифрованных DESза приемлемое для себя время.

Вместе с этим можно отметить, что систему *DES* вполне можно использовать в небольших и средних приложениях для шифрования данных, имеющих небольшую ценность. Для шифрования данных государственной важности или имеющих значительную коммерческую стоимость система *DES* в настоящее время, конечно, не должна использоваться. В 2001 году после специально объявленного конкурса в США был принят новый стандарт на блочный шифр, названный *AES (Advanced Encryption Standard)*, в основу которого был положен шифр *Rijndael*, разработанный бельгийскими специалистами. Этот шифр рассматривается в конце лекции.

Основные параметры *DES*: размер блока 64 бита, длина ключа 56 бит, количество раундов – 16. *DES* является классической сетью Фейштеля с двумя ветвями. Алгоритм преобразует за несколько раундов 64-битный входной блок данных в 64-битный выходной блок. Стандарт *DES* построен на комбинированном использовании перестановки, замены и гаммирования. Шифруемые данные должны быть представлены в двоичном виде.

Шифрование

Общая структура *DES* представлена на рис. 4.1. Процесс шифрования каждого 64-битового блока исходных данных можно разделить на три этапа:

1. начальная подготовка блока данных;
2. 16 раундов "основного цикла";
3. конечная обработка блока данных.

На первом этапе выполняется *начальная перестановка* 64-битного исходного блока текста, во время которой биты определенным образом переупорядочиваются.

На следующем (основном) этапе блок делится на две части (ветви) по 32 бита каждая. Правая ветвь преобразуется с использованием некоторой функции F и соответствующего *частичного ключа*, получаемого из основного ключа шифрования по специальному алгоритму преобразования ключей. Затем производится обмен данными между левой и правой ветвями блока. Это повторяется в цикле 16 раз.

Наконец, на третьем этапе выполняется перестановка результата, полученного после шестнадцати шагов основного цикла. Эта перестановка обратна начальной перестановке.



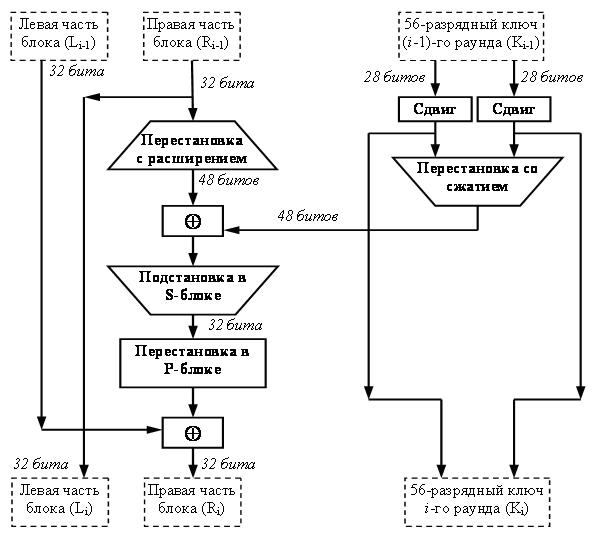
**Рис. 4.1.**Общая схема DES

Рассмотрим более подробно все этапы криптографического преобразования по стандарту *DES*.

На первом этапе 64-разрядный блок исходных данных подвергается начальной перестановке. В литературе эта операция иногда называется "забеливание" – whitening. При начальной перестановке биты блока данных определенным образом переупорядочиваются. Эта операция придает некоторую "хаотичность" исходному сообщению, снижая возможность использования криптоанализа статистическими методами.

Одновременно с начальной перестановкой блока данных выполняется начальная перестановка 56 бит ключа. Из рис. 4.1. видно, что в каждом из раундов используется соответствующий 48-битный частичный ключ Ki. Ключи Ki получаются по определенному алгоритму, используя каждый из битов начального ключа по нескольку раз. В каждом раунде 56-битный ключ делится на две 28-битовые половинки. Затем половинки сдвигаются влево на один или два бита в зависимости от номера раунда. После сдвига определенным образом выбирается 48 из 56 битов. Так как при этом не только выбирается подмножество битов, но и изменяется их порядок, то эта операция называется "перестановка со сжатием". Ее результатом является набор из 48 битов. В среднем каждый бит исходного 56-битного ключа используется в 14 из 16 подключей, хотя не все биты используются одинаковое количество раз.

Далее выполняется основной цикл преобразования, организованный по сети Фейштеля и состоящий из 16 одинаковых раундов. При этом в каждом раунде ( рис. 4.2) получается промежуточное 64-битное значение, которое затем обрабатывается в следующем раунде.



**Рис. 4.2.**Структура одного раунда DES

Левая и правая ветви каждого промежуточного значения обрабатываются как отдельные 32-битные значения, обозначенные L и R.

Вначале правая часть блока Ri расширяется до 48 битов, используя таблицу, которая определяет перестановку плюс расширение на 16 битов. Эта операция приводит размер правой половины в соответствие с размером ключа для выполнения операции XOR. Кроме того, за счет выполнения этой операции быстрее возрастает зависимость всех битов результата от битов исходных данных и ключа (это называется "лавинным эффектом"). Чем сильнее проявляется лавинный эффект при использовании того или иного алгоритма шифрования, тем лучше.

После выполнения перестановки с расширением для полученного 48-битного значения выполняется операция XOR с 48-битным подключом Ki. Затем полученное 48-битное значение подается на вход блока подстановки S (от англ. *Substitution* - подстановка), результатом которой является 32-битное значение. Подстановка выполняется в восьми блоках подстановки или восьми S-блоках (S-boxes). При выполнении этой операции 48 битов данных делятся на восемь 6-битовых подблоков, каждый из которых по своей таблице замен заменяется четырьмя битами. Подстановка с помощью S-блоков является одним из важнейших этапом *DES*. Таблицы замен для этой операции специально спроектированы специалистами так, чтобы обеспечивать максимальную безопасность. В результате выполнения этого этапа получаются восемь 4-битовых блоков, которые вновь объединяются в единое 32-битовое значение.

Далее полученное 32-битовое значение обрабатывается с помощью перестановки Р (от англ. *Permutation* – перестановка), которая не зависит от используемого ключа. Целью перестановки является максимальное переупорядочивание битов такое, чтобы в следующем раунде шифрования каждый бит с большой вероятностью обрабатывался другим S-блоком.

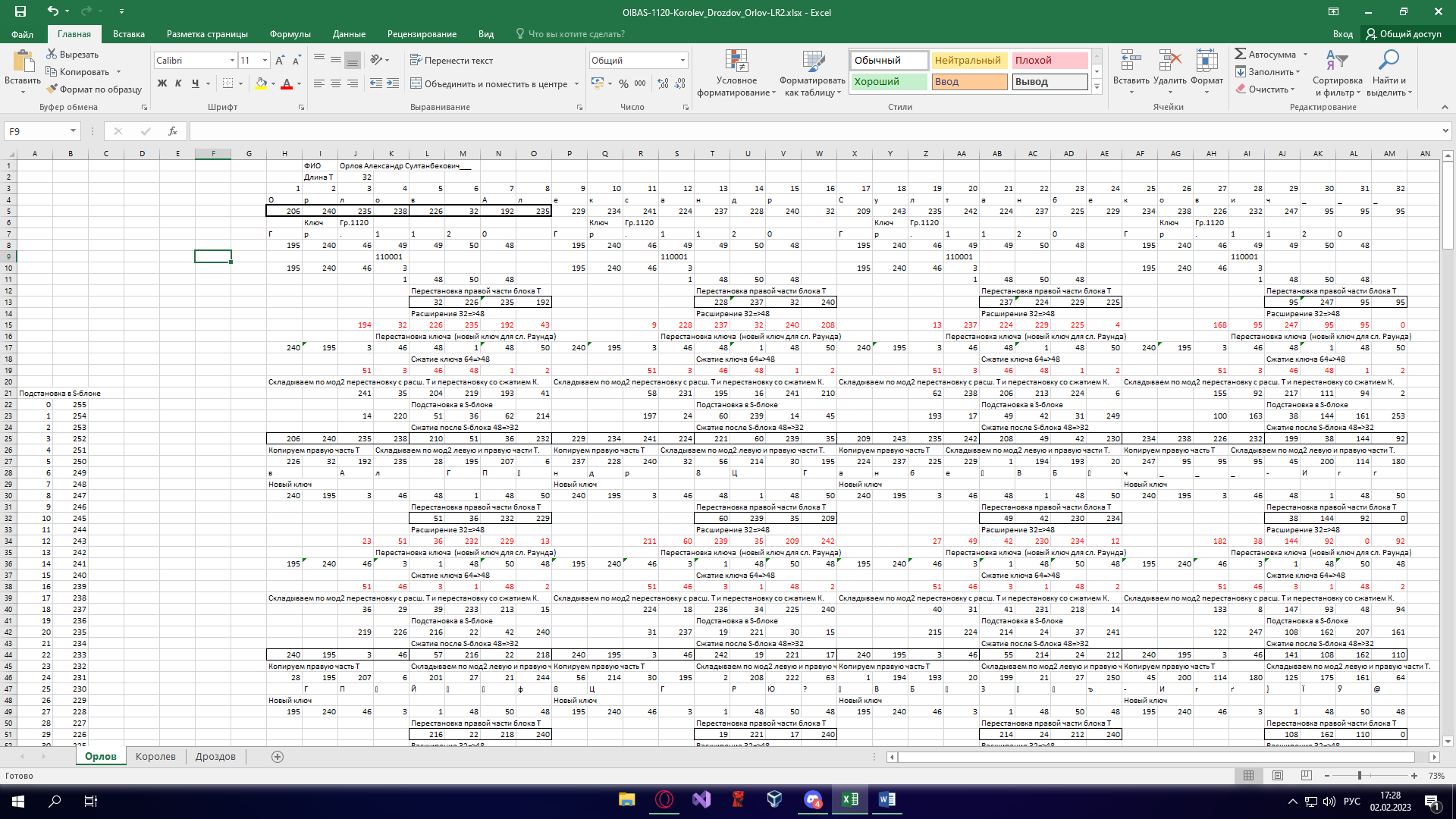
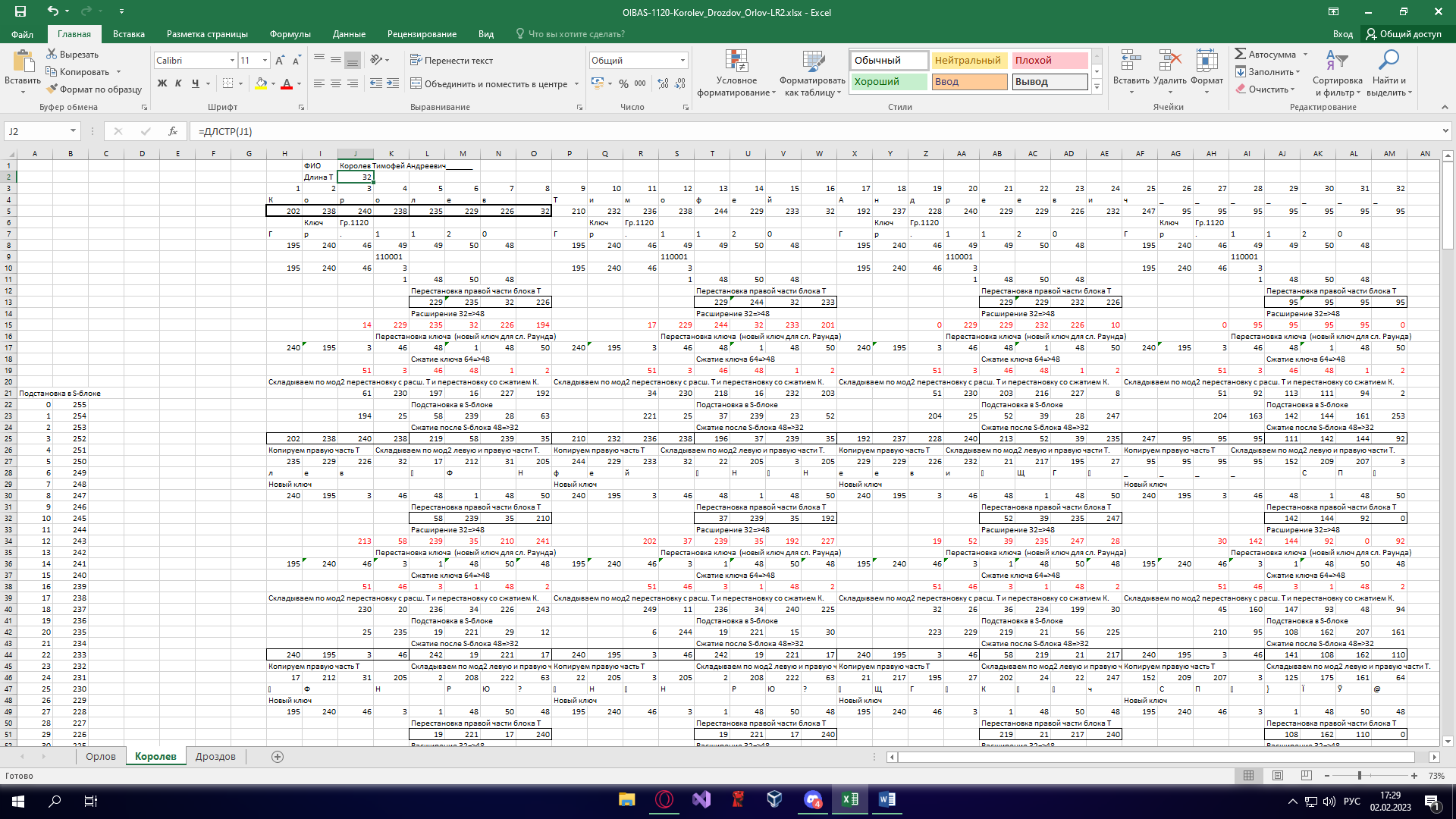
И, наконец, результат перестановки объединяется с помощью операции XOR с левой половиной первоначального 64-битового блока данных. Затем левая и правая половины меняются местами, и начинается следующий раунд.

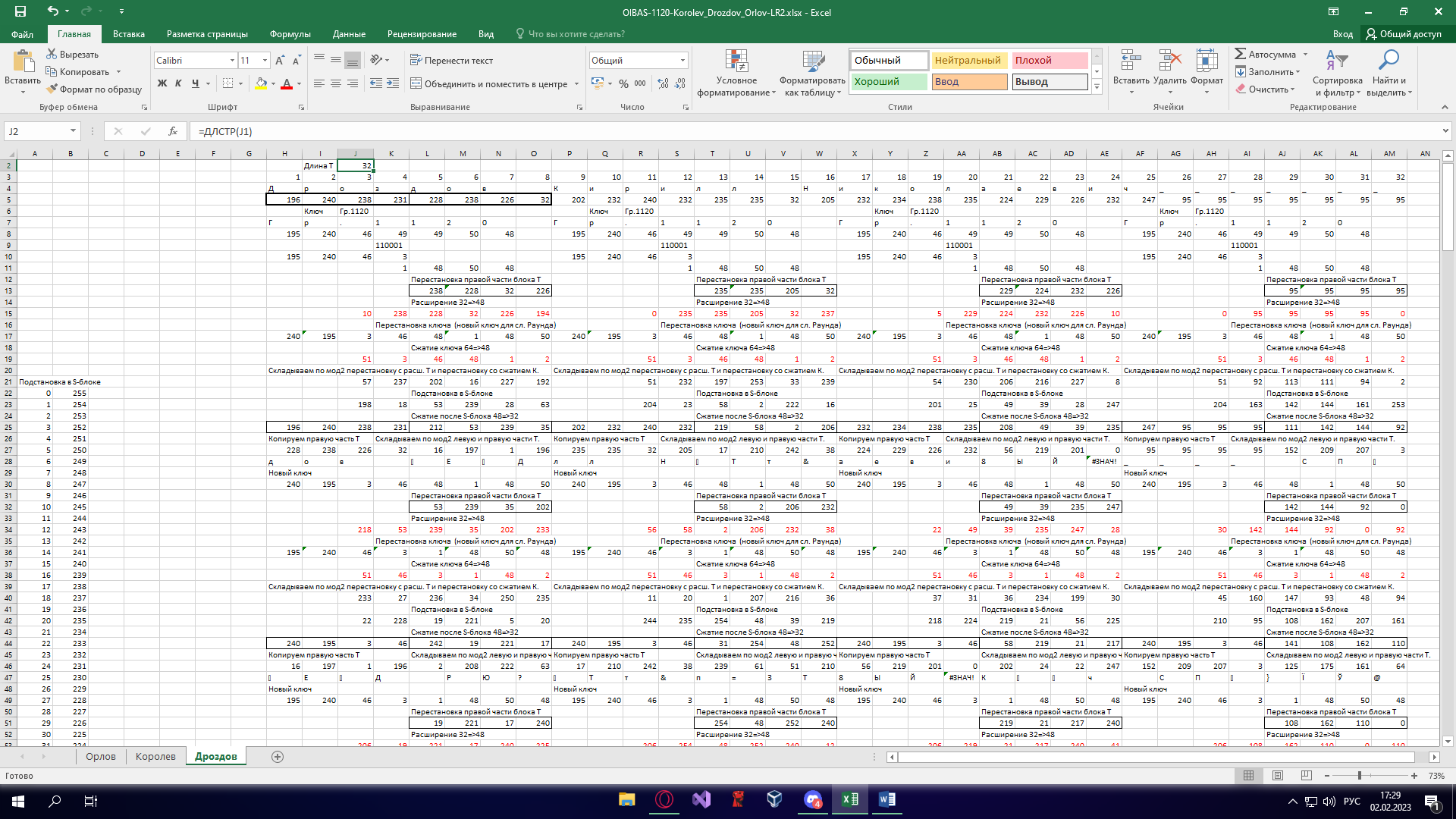
После шестнадцати раундов шифрования выполняется конечная перестановка результата. Эта перестановка инверсна (обратна) начальной перестановке.

После выполнения всех указанных шагов блок данных считается полностью зашифрованным и можно переходить к шифрованию следующего блока исходного сообщения.

Если Вы внимательно прочитали описание *DES*, то убедились, что разработчики приложили все силы для того, чтобы сделать процесс вскрытия зашифрованных сообщений как можно более трудным. Даже простое описание *DES* на бумаге выглядит достаточно сложным, что уж говорить про его программную реализацию! Разработать правильно и оптимально функционирующую программу полностью в соответствии с *DES*, наверно, под силу только опытным программистам. Некоторые трудности возникают при программной реализации, например, начальной перестановки или перестановки с расширением. Эти сложности связаны с тем, что первоначально планировалось реализовывать *DES* только аппаратно. Все используемые в стандарте операции легко выполняются аппаратными блоками, и никаких трудностей с реализацией не возникает. Однако через некоторое время после публикации стандарта разработчики программного обеспечения решили не стоять в стороне и тоже взяться за создание систем шифрования. В дальнейшем *DES* реализовывался и аппаратно, и программно.

Шифровку наших фамилий проводили с использованием ключа Гр.1120. Для каждой ФИО было проделано 16 раундов шифрования.





# Выводы

В ходе данной лабораторной работы цели и задачи были выполнены.

Теоретическая часть по этой теме была изучена и усвоена.

Был реализован алгоритм симметричного шифрования DES в редакторе электронных таблиц Excel.

# Список литературы

* <https://intuit.ru/studies/courses/691/547/lecture/12377?page=1>
* <https://studbooks.net/2202437/informatika/nadezhnost_ispolzovaniya>
* <https://ru.wikipedia.org/wiki/DES>
* <https://www.bibliofond.ru/view.aspx?id=871839>
* А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин.
* Основы криптографии.
* A. Menezes, Pvan Oorschot, S. Vanstone. Handbook of Applied Cryptography