МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

**«Челябинский государственный университет»**

**(ФГБОУ ВО «ЧелГУ»)**

Математический факультет

Кафедра компьютерной безопасности и прикладной алгебры

**КУРСОВАЯ РАБОТА**

**Реализация и сравнение алгоритмов симметричного шифрования на примере DES и LOKI97**

Выполнил студент:

**Гутров Роман Михайлович**

группы МК-201

очной формы обучения

специальности

10.05.01 Компьютерная безопасность

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

«\_\_\_» июля 2022 г.

Научный руководитель:

Ручай Алексей Николаевич

Должность: зав. кафедрой

Ученая степень: канд.физ.-мат. наук

Ученое звание: доцент

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

«\_\_\_» июля 2022 г.

Научный руководитель:

Панасенко Дмитрий Игоревич

Должность: ст. преподаватель

Ученая степень: нет

Ученое звание: нет

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

«\_\_\_» июля 2022 г.

**Оглавление**

[**Введение** 3](#_Toc108203240)

[**1. Базовые определения** 4](#_Toc108203241)

[**2. Применение симметричного шифрования** 5](#_Toc108203242)

[**3.Математическая модель симметрического шифрования** 5](#_Toc108203243)

[**4.Сеть Фейстеля** 5](#_Toc108203244)

[**5.Алгоритм симметричного шифрования DES** 6](#_Toc108203245)

[**5.1 Схема шифрования алгоритма** 6](#_Toc108203246)

[**5.2 Начальная и конечная перестановка** 7](#_Toc108203247)

[**5.3 Раунды** 7](#_Toc108203248)

[**5.4 Основная функция** 8](#_Toc108203249)

[**5.5 Генерация ключей для раундов** 10](#_Toc108203250)

[**5.6 Схема расшифрования** 11](#_Toc108203251)

[**6. Алгоритм симметричного шифрования LOKI97** 11](#_Toc108203252)

[**6.1 Схема шифрования алгоритма** 11](#_Toc108203253)

[**6.2 Основная функция .** 12](#_Toc108203254)

[**6.2.1 KP-перестановка.** 12](#_Toc108203255)

[**6.2.2 -перестановка** 12](#_Toc108203256)

[**6.2.3 -boxes** 13](#_Toc108203257)

[**6.2.4 P – перестановка** 13](#_Toc108203258)

[**6.2.5 Конечные S-боксы.** 13](#_Toc108203259)

[**6.3 Процедура расширения ключа** 13](#_Toc108203260)

[**6.4 Схема расшифрования** 14](#_Toc108203261)

[**7. Сравнение и тестирование работы алгоритмов DES и LOKI97** 15](#_Toc108203262)

[**Заключение** 15](#_Toc108203263)

[**Список литературы** 16](#_Toc108203264)

[**Приложение** 17](#_Toc108203265)

# **Введение**

Информация уже давно стала одним из самых важных и ценных ресурсов. Поэтому проблема ее защиты встает очень остро. С целью разрешить эту проблему появилась такая наука, как криптография.

В начале двадцатого века криптографией занимались в основном госструктуры, с целью передачи зашифрованных сообщений. Сегодня же шифрование используется повсеместно: шифрование паролей, сообщений, документов, аудио и видео информации, цифровые подписи. Шифрование позволяет скрыть информацию от посторонних и сохранить ее от злоумышленников.

Сегодня, алгоритмы шифрования делятся на симметричные и ассиметричные. Основное различие – симметричные алгоритмы используют одни и те же ключи для шифрования и дешифрования, в то время как ассиметричные используют разные.

Симметричное шифрование позволяет работать с большим объемом данных, т.к. быстрее работают, поскольку не требуют формирования новых ключей для дешифрования.

Целью данной работы является реализация и сравнение двух алгоритмов симметричного шифрования: DES и LOKI97.

**Основная часть**

# **1. Базовые определения**

Шифр – семейство обратимых отображений множества последовательностей блоков текстов (сообщений) открытых в множество последовательностей блоков текстов (сообщении) шифрованных и обратно, задаваемых функцией шифрования. Каждое из отображений определяется некоторым параметром, называемым ключом, и описывается некоторым алгоритмом шифрования, реализующим один из режимов шифрования.

Ключ – изменяемый элемент (параметр), каждому значению которого однозначно соответствует одно из отображений, реализуемых криптосистемой. Все возможные значения ключа составляют множество ключевое криптосистемы.

Симметричное шифрование – способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации.

Ассиметричное шифрование – метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом.

Алгоритмы шифрования – алгоритм зашифрования, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков текста открытого, имеющих фиксированную длину. Представляет собой алгоритм простой замены блоков текста фиксированной длины.

Сеть Фейстеля – способ построения цикла (раунда) шифрования в алгоритмах шифрования итеративных (блочных) на основе регистра сдвига нелинейного длины 2 с функцией обратной связи, зависящей от ключа циклового (раундового).

Раунд – один шаг шифрования, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации путём применения круговой функции.

# **2. Применение симметричного шифрования**

Симметричное шифрование потребляет относительно мало системных ресурсов, по сравнению с другими методами шифрования. Благодаря этому оно применяется в основном для быстрого шифрования больших объемов данных.

Симметричное шифрование, например, применяется в мессенджерах с целью защиты передаваемых сообщений, а сервисы для видеосвязи используют его для защиты аудио и видео потоков. Так же симметричное шифрование имеет широкое применение в банковском деле и приложениях с карточными транзакциями. Этот вид шифрования позволяет обеспечить высокую скорость шифрования и высокую защиту данных.

Более того, AES, преемник DES – идеальный алгоритм для беспроводных сетей, которые используют протокол WPA2.

Но несмотря на все преимущества симметричное шифрование не может использоваться для формирования цифровых подписей и сертификатов, потому что секретный ключ при использовании этого метода должен быть известен всем, что противоречит идее цифровой подписи.

# **3.Сеть Фейстеля**

Сеть Фейстеля – один из методов построения блочных шифров. Сеть состоит из ячеек, называемых ячейками Фейстеля. На вход каждой ячейки поступают данные и ключ. На выходе каждой ячейки получают изменённые данные и изменённый ключ. Все ячейки однотипны, и говорят, что сеть представляет собой определённую многократно повторяющуюся (итерированную) структуру. Ключ выбирается в зависимости от алгоритма шифрования/расшифрования и меняется при переходе от одной ячейки к другой. При шифровании и расшифровании выполняются одни и те же операции; отличается только порядок ключей. Ввиду простоты операций сеть Фейстеля легко реализовать как программно, так и аппаратно.

# **4.Алгоритм симметричного шифрования DES**

Стандарт шифрования данных DES (Data Encryption Standard) – блочный шифр с симметричными ключами, разработан Национальным Институтом Стандартов и Технологии.

## **4.1 Схема шифрования алгоритма**

Алгоритм принимает 64-битовый открытый текст и порождает 64-битовый зашифрованный текст и наоборот. В обоих случаях для шифрования 64-битового блока используется один и тот же 56-битовый ключ. Процесс шифрования состоит из двух перестановок, которые называют начальной и финальной перестановками, и 16 раундов Фейстеля. Каждый раунд использует различные сгенерированные 48-битовые ключи. На рисунке 1 изображена схема алгоритма.

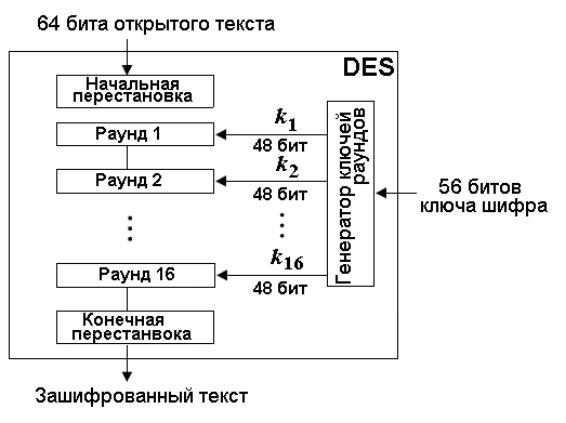


Рисунок 1. Схема алгоритма DES

## **4.2 Начальная и конечная перестановка**

На вход начальной и конечной перестановки поступает 64 бита, которые затем переставляются в соответствии с заданными таблицами (Таблица 1).



Таблица 1. IP-перестановки

Эти перестановки взаимно обратны. Таким образом на выходе получаем блок размером 64 бит, который состоит из тех же битов, что и входной блок. Другими словами, 58-й бит на входе начальной перестановки переходит в 1-ую позицию на выходе из нее. А финальная перестановка 1-ый входной бит переведет в 58-ую позицию на выходе. Обе перестановки не имеют никакого значения в крипто стойкости алгоритма.

## **4.3 Раунды**

DES использует 16 раундов. Каждый раунд DES применяет шифр Фейстеля. (Рисунок 2)

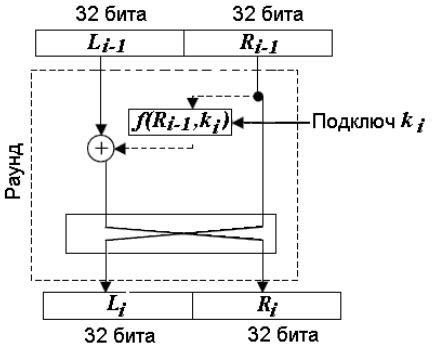


Рисунок 2. Схема раунда DES

Раунд принимает полублоки от предыдущего раунда (или начального) и создает полублоки для входа в следующий раунд (или конечный блок перестановки). Все необратимые элементы сосредоточены в функции .

## **4.4 Основная функция**

Функция с помощью 48-битового ключа раунда зашифровывает 32 правых бит , чтобы получить на выходе 32-битовый результат. Функция содержит 4 составляющие (Рисунок 3): операция XOR, P-бокс расширения, группу S-боксов и прямой бокс.

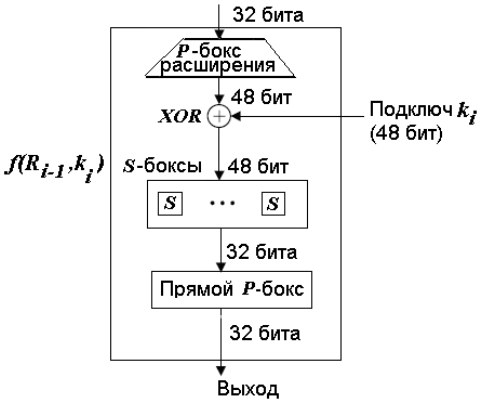


Рисунок 3. Схема основной функции.

P-бокс расширяет 32-битовый блок до 48 битов, чтобы согласовать его размер с размером ключа раунда. Блок делится на 8 секций по 4 бита, каждая секция затем расширяется до 6 бит. Отношения между входом и выходом могут быть как определены математически, так и заданы таблицей (Таблица 2).



Таблица 2. P-бокс расширения.

После расширения блока, используется операция XOR над блоком и ключом раунда

Затем, после суммирования с ключом, блок из 48 бит делится на 8 последовательных 6-битовых векторов , каждый из которых заменяется на 4-битовый вектор с помощью S-боксов (Приложение 1). Чтобы найти в S-боксе шифрообозначения вектора, надо:

1. из 1-го и последнего битов вектора образовать двоичное число, перевести его в десятичную систему. Это будет номер строки m (m = 0,1,2,3);
2. из 2-го, 3-го, 4-го и 5-го бита вектора образовать двоичное число, перевести его в десятичную систему. Это будет номер столбца l (l = 0,...,15);
3. Число, стоящее в S -боксе на пересечении m-ой строки и l-го столбца, будет шифрообозначение
4. Шифрообозначение перевести в двоичную систему. Это число будет новым 6-битным значением.

Таким образом, после S-боксов мы получаем 8 4-битовых векторов , которые объединяют в 32-битовый блок. Далее биты блока переставляются в прямом P-боксе согласно таблице (Таблица 3).



Таблица 3. Прямой P-бокс

После 16-го раунда DES правый и левый блоки уже не меняются местами, а объединяются в блок и подвергаются финальной перестановке .

## **4.5 Генерация ключей для раундов**

DES создает 16 раундовых ключей по 48 битов из ключа шифра на 56 бит. Ключевое расписание состоит из этапов:

1. Перестановка сжатия 64-битового ключа до 56 бит для удаления битов проверки. Из исходного ключа удаляют биты 8,16,24,32,40,48,56,64 и переставляют остальные биты согласно таблице (Таблица 4).



Таблица 4. Удаление проверочных бит из исходного ключа

1. После перестановки 56 битов, ключ делится на два блока по 28 бита каждый. Далее для генерации раундовых ключей из блоков с помощью операции циклического сдвига влево на 1-2 бита строятся блоки . В раундах 1,2,9,16 смещение – на 1 бит, в других – на 2 бита. После определения блоков биты этих блоков объединяются в 56-битовый ключ.
2. Перестановка сжатия (Таблица 5) изменяет 56 битов на 48 битов, которые образуют раундовый ключ.



Таблица 5. Перестановка сжатия

## **4.6 Схема расшифрования**

Для расшифрования применяются те же действия, что и для шифрования, за исключением раундовых ключей – они используются в обратном порядке. Т.е. для 1-го раунда используется 16-ый раундовый ключ.

# **5. Алгоритм симметричного шифрования LOKI97**

Блочный алгоритм с симметричными ключами. lOKI97 шифрует данные блоками по 128 битов и использует ключи размером 128, 192 и 256 битов.

## **5.1 Схема шифрования алгоритма**

Алгоритм базируется на сети Фейстеля: данные шифруемого блока разбиваются на два субблока по 64 бита, над одним из которых выполняются следующие операции:

1. Сложение с первым фрагментом ключа раунда по модулю .
2. Наложение функции , выполняющей нелинейное преобразование данных и использующей в качестве аргумента второй аргумент ключа раунда.
3. Сложение по модулю с третьим фрагментом ключа раунда.

После выполнения перечисленных действий обработанный субблок накладывается на другой применением операции XOR, после чего субблоки меняются местами (за исключением последнего раунда). Схема алгоритма приведена на рисунке 1.1:

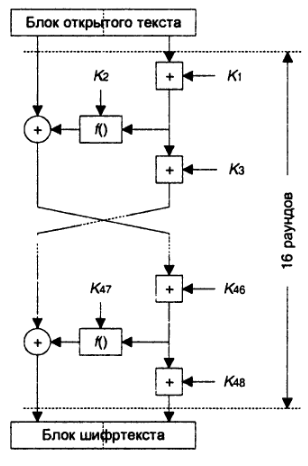


Рисунок 1.1. Схема шифрования алгоритма LOKI97

## **5.2 Основная функция .**

Основная функция алгоритма LOKI97. Используется в раундах сети Фейстеля и для расширения ключа до 256 бит. Сама функция состоит из KP-перестановки, E-перестановки, -перестановок, P-перестановки и конечной -перестановки.

### **5.2.1 KP-перестановка.**

KP (Keyed Permutation) – простая перестановка входных данных на основе младших 32 битов используемого функцией фрагмента ключа раунда , где i – номер раунда. Шаги выполнения перестановки:

1. Входные данные разбиваются на два субблока по 32 бита.
2. Для каждого единичного бита фрагмента ключа выполняется перестановка соответствующих ему битов субблоков между собой. Т.е. если нулевой бит ключа имеет значение 1, то нулевой бит первого субблока входных данных принимает значение нулевого бита второго субблока и наоборот.

### **5.2.2 -перестановка**

E (Expansion) – генерация 96-битной последовательности на основе 64-битного результата операции KP. Последовательность формируется на основе следующих битов входа: [4-0,63-56,58-48,52-40,42-32,34-24,28-16,18-8,12-0].

### **5.2.3 -boxes**

(Substitution boxes) – таблицы замен. обрабатывает 13-битные фрагменты 96-битной последовательности, полученной операцией , – 11-битные фрагменты. Замена выполняется согласно следующим формулам (в формулах указаны шестнадцатеричные константы):

### **5.2.4 P – перестановка**

P-перестановка – побитовая перестановка входной последовательности согласно таблице 1.1:

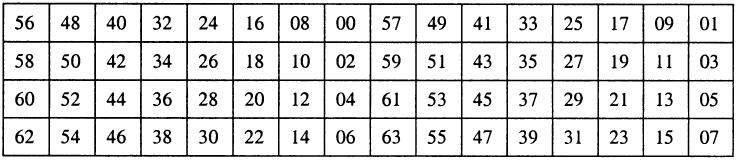


Таблица 1.1. P-перестановка

### **5.2.5 Конечные S-боксы.**

64-битный результат перестановки P и 32-битная старшая часть фрагмента ключа раунда повторно обрабатываются таблицей замен. Входная 64-битная последовательность поровну (по 8 битов) распределяется между таблицами, а из фрагмента ключа раунда берутся недостающие биты до необходимых 13 или 11 битов. После формирования S-таблиц снова выполняется преобразование согласно формулам.

После всех преобразований субблоки меняются местами (за исключением последнего раунда) и объединяются в один 128-битовый блок.

## **5.3 Процедура расширения ключа**

Процедура расширения ключа позволяет на основе ключа шифрования получить 48 фрагментов ключей раундов , по три из которых используются в каждом раунде алгоритма.

В начале процедуры выполняется инициализация исходной 256-битной ключевой последовательности, которая, в зависимости от длины ключа шифрования, выполняется одним из следующих способов:

1. 256-битный ключ используется в неизменном виде
2. 192-битный ключ дополняется результатом применения описанной выше функции , которая в качестве обрабатываемых данных (первый аргумент) использует первые 64 бита ключа шифрования, а в качестве подключа (второй аргумент) – следующие 64 бита ключа шифрования.
3. 128-битный ключ дополняется результатом применения функции с обратным относительно 192-битного ключа порядком аргументов, а затем дополняется аналогичным 192-битному ключу образом.

Дальнейшая обработка исходной ключевой последовательности основана на сети Фейстеля (Рисунок 1.2), после каждого раунда которой получается фрагмент ключа раунда алгоритма.

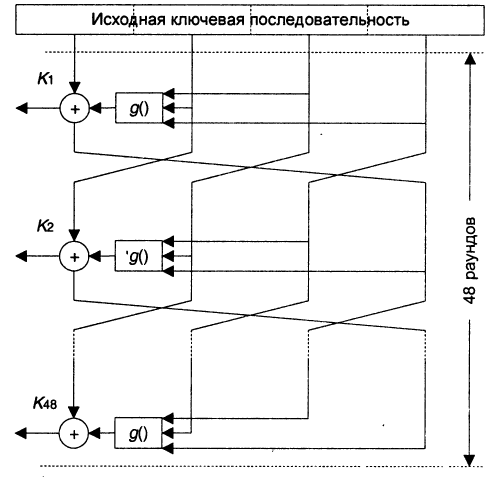


Рисунок 1.2. Схема получения фрагментов ключа раунда

В каждом раунде три 64-битных фрагмента текущего состояния ключевой последовательности обрабатываются функцией и накладываются операцией XOR на оставшийся 64-битный фрагмент. Функция описывается следующим образом: , где:

i-номер текущего раунда процедуры расширения ключа;

∆ - константа, равная: ∆ = .

## **5.4 Схема расшифрования**

Для расшифрования применяются те же действия, что и для шифрования, за исключением раундовых ключей – они используются в обратном порядке. Т.е. для 1-го раунда используется 16-ый раундовый ключ.

# **6. Сравнение и тестирование работы алгоритмов DES и LOKI97**

Результат работы алгоритмов представлен в таблице 3.1

|  |  |  |  |
| --- | --- | --- | --- |
| Алгоритм | Размер файла | Время шифрования | Время дешифрования |
| DES | 330 Кб | 1.517 c | 1.491 c |
| 1 Мб | 4.446 c | 4.399 c |
| 100 Мб | 470.122 c | 479.730 |
| 1000 Мб | 4676.847 с | 5390.203 с |
| LOKI97 | 330 Кб | 0.901 c | 890 c |
| 1 Мб | 2.629 c | 2.626 c |
| 100 Мб | 268.864 с | 268.928 с |
| 1000 Мб | 2774.584 c | 2760.802 c |

Таблица 3.1. Сравнение алгоритмов DES и LOKI97

# **Заключение**

В ходе работ мы изучили, реализовали и сравнили алгоритмы симметричного шифрования DES и LOKI97. Исходя из результатов работ алгоритмов наибольшую эффективность показывает алгоритм LOKI97. Это связано с тем, что алгоритм использует блок размером 128 бит, против 64 бит у DES. Так же, LOKI97 использует ключ большего размера: 256 бит, что делает его более безопасным и криптостойким в сравнении с DES. Все поставленные задачи были выполнены.

# **Список литературы**

[1] Сушко С.А. Практическая криптология [Текст]: учебник для вузов. – 116

с.

[2] Панасенко С. П. Алгоритмы шифрования [Текст]: специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.

[3] DES [Электронный ресурс]: Википедия. Свободная энциклопедия. - Режим доступа: <https://ru.wikipedia.org/wiki/DES>

# **Приложение**

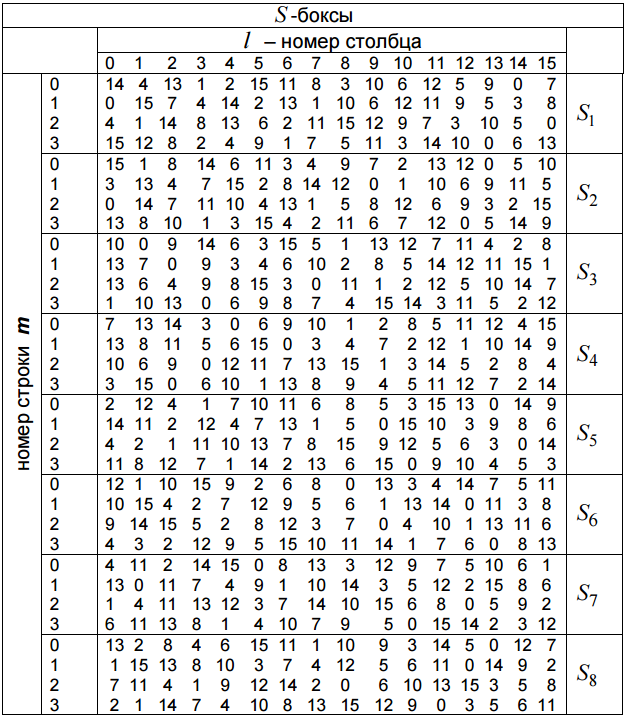


Таблица S – перестановок

Код DES

Main.cpp

DES.cpp

DES.h

Код LOKI97

Main.c

LOKI.cpp

LOKI.h