**Министерство науки и высшего образования Российской Федерации**

**ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина»**

Кафедра «школы бакалавриата (школа)»

Оценка работы\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель от УрФУ Попов В.Ю.

Тема задания на практику

Ускоренное шифрование на основе разделения секрета

ОТЧЕТ

Вид практики Производственная практика

Тип практики Практика по получению профессиональных умений и опыта профессиональной деятельности

Студент Кулаков В.С.

**ФИО студента**

Специальность (направление подготовки) 10.05.01 Компьютерная безопасность

Группа МЕН-541015

Екатеринбург 2019

# **Введение**

Актуальность проблемы сокрытия информации существует с момента появления самой информации. Ещё в Древнем Риме Цезарь использовал шифр сдвига, который был частным случаем шифра простой замены для передачи секретной информации (например в зону военных действий). В настоящее время потребность сокрытия информации наиболее актуальна для электронных устройств и сетей. С увеличением важности и количества информации на современные шифры накладываются различные дополнительные сложности. Во-первых алгоритм должен быть стойким, что достигается путём увеличения ключа шифрования и сложностью вычисления данных. Во-вторых алгоритм должен быть быстрым и сложность вычисления алгоритма должна быть всё же значительно меньше сложности его взлома, ведь нам же не хочется ждать шифрования/расшифрования столько же времени сколько потратит взломщик. Наиболее современным алгоритмом шифрования информации является AES. Для этого алгоритма существуют все возможные ухищрения в ускорении вплоть до реализации команд процессора. Самым стойким вариантом AES является AES256. Однако чем длиннее ключ тем тяжелее вычисления. Предложено для ускорения процесса шифрования реализовать схему разделения секрета которая позволит разгрузить AES и ускорить его работу за счёт увеличения потребляемой памяти. Также разделение секрета позволяет разделить информацию между группой участников не позволяя обладателю части взломать весь секрет.

**Объект исследования** – алгоритм шифрования с разделением секрета.

**Целью работы** является реализация алгоритма шифрования на основе AES256 и внедрённым алгоритмом разделения секрета с возможностью восстановления секрета при деструктивной активности одного из участников.

В работе решаются следующие задачи:

* Рассмотрение вариантов внедрения разделения секрета
* Подбор параметров разделения секрета
* Анализ скорости работы алгоритма и сравнение его с AES256

# **Глава 1 Алгоритм AES**

## **Описание**

Для того чтобы составить алгоритм работающий лучше другого алгоритма необходимо изначально осознать и реализовать исходный. Итак алгоритм AES – симметричный итеративный блоковый алгоритм.

Характеристики AES:

* Работает с 128-bit блоками данных (16 байт)
* Три типа ключа 128/192/256
* Три типа раундов 10/12/14 в зависимости от ключа
* Все раунды идентичны, кроме последнего

Операции шифра происходят в поле Галуа GF(28) по модулю многочлена x8+x4+x3+x+1.

**Элемент поля:** Битовый многочлен

**Операция сложения:**

Где

**Операция умножения:**

Перемножение многочлена работает по обычным алгебраическим правилам и взятие многочлена по модулю x8+x4+x3+x+1.

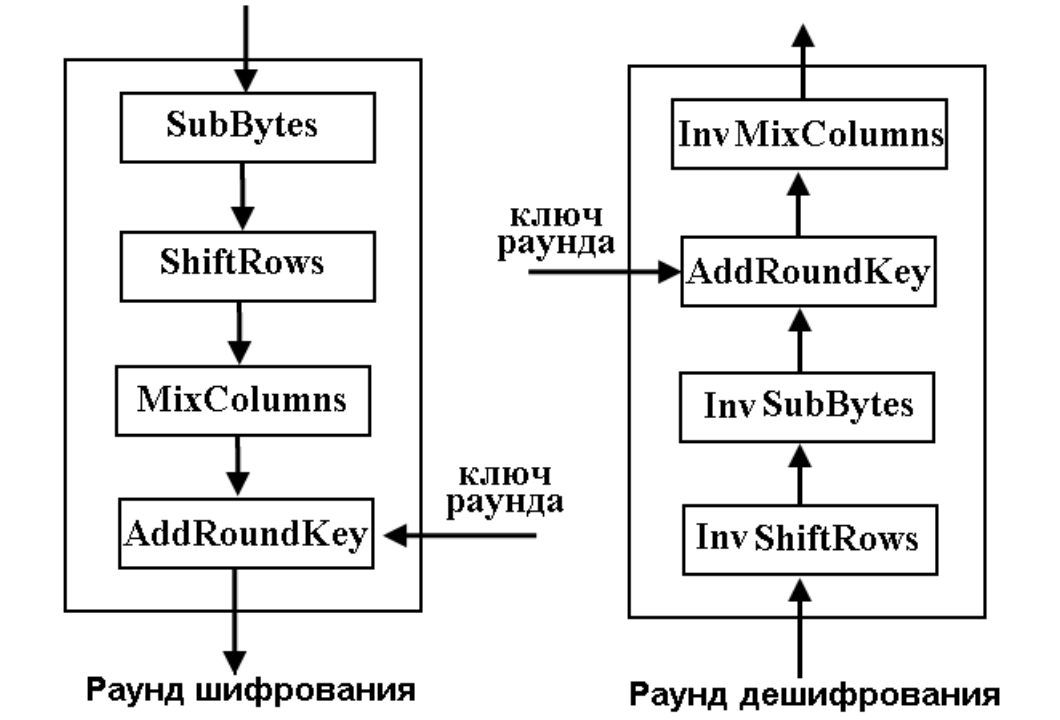
Но для более быстро умножения возьмём таблицу ([приложение 1](#_№1_Таблицы_степени)) степени и логарифма в поле Галуа GF(28) над многочленом x+1. Теперь умножение:

Так же вычисляем обратный элемент обходя тяжёлый алгоритм Эвклида:

Данные в алгоритме AES раскладываются в виде квадрата 16 байт(4x4):

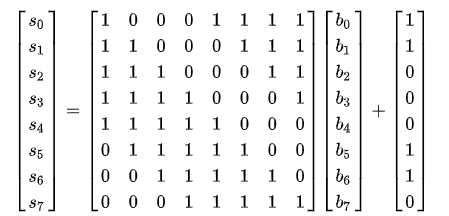
Сам алгоритм шифрования и дешифрования состоит из 4 процедур циклически применяемых к блоку в течение 14 раундов.

1 раунд шифрования:

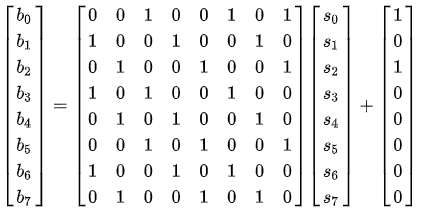


## **Процедуры преобразования состояний**

1. Процедура SubBytes производит над каждым байтом преобразование вида:



Но для ускорения в памяти просто хранится матрица Sbox ([Приложение 2](#_№2_Матрицы_Sbox)) по которой заменяются байты. Обратное преобразование процедура InvSubBytes выглядит так (Таблица InvSbox [Приложение 2](#_№2_Матрицы_Sbox)):



2. Процедура ShiftRows просто сдвигает строчки блока

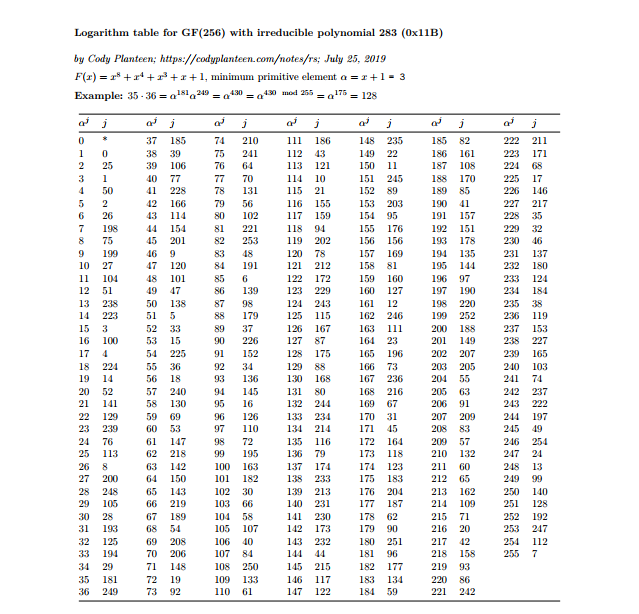
## **Процедура расширения ключа**

При инициализации шифра ключом происходит расширение этого ключа на все раунды работы алгоритма, так как рассматривается алгоритм c 256-bit(32 byte) ключом, то нужно расширить его на 14 раундов или 15 16-bit слов (так как размер блока с которым работает AES 128 bit для любого ключа).

Для AES256 процедура заполнения выглядит так:

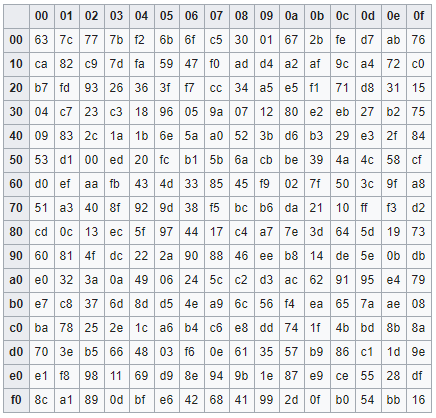
Приложения

## №1 Таблицы степени и логарифма GF(28)

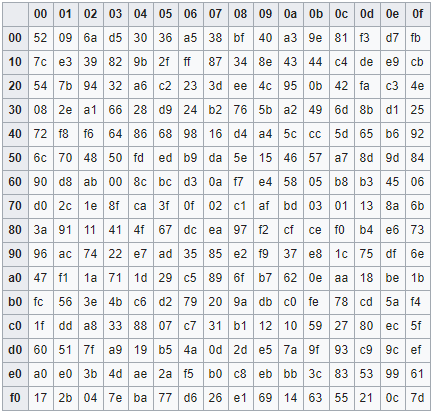


## №2 Матрицы Sbox и InvSbox

Sbox



InvSbox



Оглавление

[**Министерство науки и высшего образования Российской Федерации** 1](#_Toc23308665)

[**ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина»** 1](#_Toc23308666)

[Кафедра «школы бакалавриата (школа)» 1](#_Toc23308667)

[Оценка работы\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 1](#_Toc23308668)

[ОТЧЕТ 1](#_Toc23308669)

[**Введение** 2](#_Toc23308670)

[**Глава 1 Алгоритм AES** 3](#_Toc23308671)

[**Описание** 3](#_Toc23308672)

[Процедура расширения ключа 4](#_Toc23308673)

[Приложения 5](#_Toc23308674)

[№1 Таблицы степени и логарифма GF(28) 5](#_Toc23308675)

[№2 7](#_Toc23308676)