**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

**«**Разработка систем аутентификации и криптографии**»**

**Лабораторная работа 1** на тему

«Алгоритм шифрования AES»

**Выполнила:**

магистрант гр. N42514c

Ли Ю.В.

**Проверил:**

Фёдоров И. Р.

Санкт-Петербург

2020

**Цель работы:** научиться программировать криптографические алгоритмы.

**Задача:** реализовать алгоритм шифрования AES с длиной ключа 128 бит, подписать получившийся исполняемый файл электронной подписью.

**Средства реализации:**

IDE: PyCharm 2020.1.2. Выбрана по причине удобства интерфейса и заточенности под Python.

Язык Python 3 - выбран как простой и эффективный.

Операционная система: Windows 10.

**Описание алгоритма:**

Advanced Encryption Standard (AES), также известный как Rijndael — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит).

AES является стандартом, основанным на алгоритме Rijndael. Для AES длина input (блока входных данных) и State (состояния) постоянна и равна 128 бит, а длина шифроключа K составляет 128, 192, или 256 бит. При этом исходный алгоритм Rijndael допускает длину ключа и размер блока от 128 до 256 бит с шагом в 32 бита. Для обозначения выбранных длин input, State и Cipher Key в 32-битных словах используется нотация Nb = 4 для input и State, Nk = 4, 6, 8 для Cipher Key соответственно для разных длин ключей.

*Используемые процедуры*

AddRoundKey() трансформация при шифровании и обратном шифровании, при которой Round Key XOR’ится c State. Длина RoundKey равна размеру State (то есть если Nb = 4, то длина RoundKey равна 128 бит или 16 байт)

InvMixColumns() трансформация при расшифровании, которая является обратной по отношению к MixColumns()

InvShiftRows() трансформация при расшифровании, которая является обратной по отношению к ShiftRows()

InvSubBytes() трансформация при расшифровании, которая является обратной по отношению к SubBytes()

MixColumns() трансформация при шифровании, которая берёт все столбцы State и смешивает их данные (независимо друг от друга), чтобы получить новые столбцы

RotWord() функция, использующаяся в процедуре Key Expansion, которая берёт 4-байтовое слово и производит над ним циклическую перестановку

ShiftRows() трансформации при шифровании, которые обрабатывают State, циклически смещая последние три строки State на разные величины

SubBytes() трансформации при шифровании, которые обрабатывают State, используя нелинейную таблицу замещения байтов (S-box), применяя её независимо к каждому байту State

SubWord() функция, используемая в процедуре Key Expansion, которая берёт на входе четырёхбайтовое слово и, применяя S-box к каждому из четырёх байтов, выдаёт выходное слово

Используемые операции:

* исключающее ИЛИ;
* умножение в поле Галуа по модулю;
* сдвиг байт.

Стандарт AES опубликован как FIPS 197.

**Исходный код:**

<https://github.com/julialiv09/Cryptography/tree/main/lab1>

**Выводы:**

В ходе проделанной работы был реализован алгоритм шифрования AES-128, а также подписан исполняемый файл.