Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего профессионального образования

«Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»

**Кафедра технической физики**

**ОТЧЕТ**

**по лабораторной работе**

Алгоритм AES ⎯ Пример современного симметричного Компрессия данных или измерение и избыточность информации Криптопреобразования

|  |  |
| --- | --- |
| Студент: | Пицхелаури С.С. |
| Группа: | Фт-430203 |
|  |  |
| Преподаватель: | Александров О. Е. |

Екатеринбург

 2016

## Введение

Все известные алгоритмы шифрования делятся на два типа.

Симметричные ⎯ с единственным секретным ключом для шифрования и дешифрования (они же single-key). Симметричные алгоритмы также подразделяются на два семейства: потоковые (шифрование данных посимвольно) и блочные (шифрование данных кусками – блоками – из нескольких символов конечной и фиксированной длины).

Асимметричные ⎯ с двумя ключами: открытым ключом (или public-key) и закрытым ключом (или private-key). Первый ключ служит только для шифрования, второй ⎯ для дешифрования.

Каждый из указанных типов криптоалгоритмов имеет свои достоинства и недостатки. Так основным недостатком симметричных методов является необходимость организации закрытого канала для передачи ключа. А основным достоинством ⎯ быстрота выполнения криптопреобразования. И наоборот, асимметричные алгоритмы более медленные в выполнении криптопреобразования, но не требуют закрытых каналов обмена ключами, т.к. открытый ключ не позволяет произвести дешифровку, а передавать закрытый ключ не нужно.

В данной лабораторной работе будет рассмотрен один из современных стандартов симметричного шифрования – AES.

Advanced Encryption Standard (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_%28%D0%BA%D0%BE%D0%BD%D0%BA%D1%83%D1%80%D1%81%29). По состоянию на [2009 год](https://ru.wikipedia.org/wiki/2009_%D0%B3%D0%BE%D0%B4) AES является одним из самых распространённых алгоритмов симметричного шифрования. Поддержка AES (и только его) введена фирмой [Intel](https://ru.wikipedia.org/wiki/Intel) в семейство процессоров [x86](https://ru.wikipedia.org/wiki/X86), начиная с Intel Core i7-980X Extreme Edition, а затем на процессорах [Sandy Bridge](https://ru.wikipedia.org/wiki/Sandy_Bridge).

## Постановка задачи

Для ознакомления с алгоритмом криптопреобразования AES необходимо выполнить следующие задачи:

1. Используя методичку и программу изучить пошаговое действие алгоритма AES.

2. Установить экспериментально значения исходных строк, при которых программа перестает функционировать правильно. Попытаться объяснить эти ограничения.

3. Изменяя размер исходной строки *N* пределах от одного символа до 1000 символов произвести измерения затрат времени Δ*t* на шифрование, дешифрование AES. Замеры произвести на одном и том же компьютере не менее чем в 20 точках диапазона. Построить графики зависимости Δ*t* от *N*. Предложить и обосновать теоретическую зависимость Δ*t* от *N* в пределе больших *N*. Прокомментировать результаты с точки зрения оценки производительности AES.

4.Ответить на вопросы:

a) Зачем (свои соображения) нужна таблица замен и как она повышает криптостойкость алгоритма? Ведь таблица постоянная, в отличие от ГОСТ.

б) Оценить сравнительную криптостойкость AES и ГОСТ 28147-89. Какой из алгоритмов более стоек?

в) Какой аналог алгоритма гаммирования ГОСТ 28147-89 есть в стандарте AES?

г) Можно ли реализовать алгоритм гаммирования ГОСТ 28147-89 в рамках AES?

д) Какой аналог алгоритма генерации имитовставки ГОСТ 28147-89 есть в стандарте AES?

## Ход работы

## Ответы на вопросы

**1. Зачем нужна таблица замен и как она повышает криптостойкость алгоритма? Ведь таблица постоянная, в отличие от ГОСТ.**

Таблица замен – операция шифрования, в результате которого каждые группы битов заменяются по нелинейному принципу. Это затрудняет криптоанализ и повышает криптостойкость алгаритма.

**2. Оценить сравнительную криптостойкость AES и ГОСТ 28147-89. Какой из алгоритмов более стоек?**

Оба алгоритма обладают высокой криптостойкостью – ни тот, ни другой не имеют алгоритм взлома, кроме метода подбора. — Ну и вообще никак КОЛИЧЕСТВЕННО не сравнить?

**3. Какой аналог алгоритма гаммирования ГОСТ 28147-89 есть в стандарте AES?**

Режим счетчка CTR - аналог гаммирования ГОСТа. Здесь есть простейший генератор псевдослучайных данных, который прибавляет константы к предыдущему значению в пределах разрядной сетки блока. Если эта константа – единица, то выход такого генератора распадается на последовательность пар значений, различающихся в одном бите, что может привести к применению к шифру дифференцированного криптоанализа. – Значению чего?

**4. Можно ли реализовать алгоритм гаммирования ГОСТ 28147-89 в рамках AES?**

Гаммирование нельзя реализовать в AES ввиду своих особенностей (в гаммировании оперируют битами, а в AES байтами). – из битов всегда можно сделать байты и наоборот

**5. Какой аналог алгоритма генерации имитовставки ГОСТ 28147-89 есть в стандарте AES?**

Poly1305-AES, где в качестве ключа используется 128 битный ключ для AES, 106 битный дополнительный код, а также создаётся 128 битная псевдослучайная генерация. Poly1305-AES вычисляет 16-байтовый аутентификатор сообщения любой длины, используя 16-байтовое число (уникальное число сообщения) и 32-байтовый секретный ключ. Злоумышленники не могут изменить или подделать сообщение, если отправитель сообщения передает аутентификатор наряду с каждым сообщением, и приемник сообщения проверяет каждый аутентификатор. – Т.е. имитовставка есть, но как считать непонятно.

## Вывод

В ходе данной лабораторной работы прошло ознакомление с алгоритмом криптопреобразования – AES. Были получены практические навыки использования данного алгоритма.