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 КРИПТОПРЕОБРАЗОВАНИЯ

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

Екатеринбург

2016

## Цель:

Используя методичку и программу изучить пошаговое действие алгоритма AES. Установить экспериментально значения исходных строк, при которых программа ПЕРЕСТАЕТ функционировать правильно. Попытаться объяснить эти ограничения. Изменяя размер исходной строки *N* пределах от одного символа до 1000 символов произвести измерения затрат времени *t* на шифрование, дешифрование AES. Замеры произвести на одном и том же ком компьютере не менее чем в 20 точках диапазона. Построить графики зависимости *t* от *N*. Предложить и обосновать теоретическую зависимость *t* от *N* в пределе больших *N*. Прокомментировать результаты с точки зрения оценки производительности AES.

Ответить на вопросы:

1. Зачем нужна таблица замен и как она повышает криптостойкость алгоритма?
2. Оценить сравнительную криптостойкость AES и ГОСТ 28147-89. Какой из алгоритмов более стоек?
3. Какой аналог алгоритма гаммирования ГОСТ 28147-89 есть в стандарте AES?
4. Можно ли реализовать алгоритм гаммирования ГОСТ 28147-89 в рамках AES?
5. Какой аналог алгоритма генерации имитовставки ГОСТ 28147-89 есть в стандарте AES?

## Ход работы

Изменяя размер исходной строки *N* пределах от одного символа до 1000 символов произвели измерения затрат времени *t* на шифрование AES. Построили график зависимости *t* от *N* (Рисунок 2).

Рисунок 1. Результат работы программы

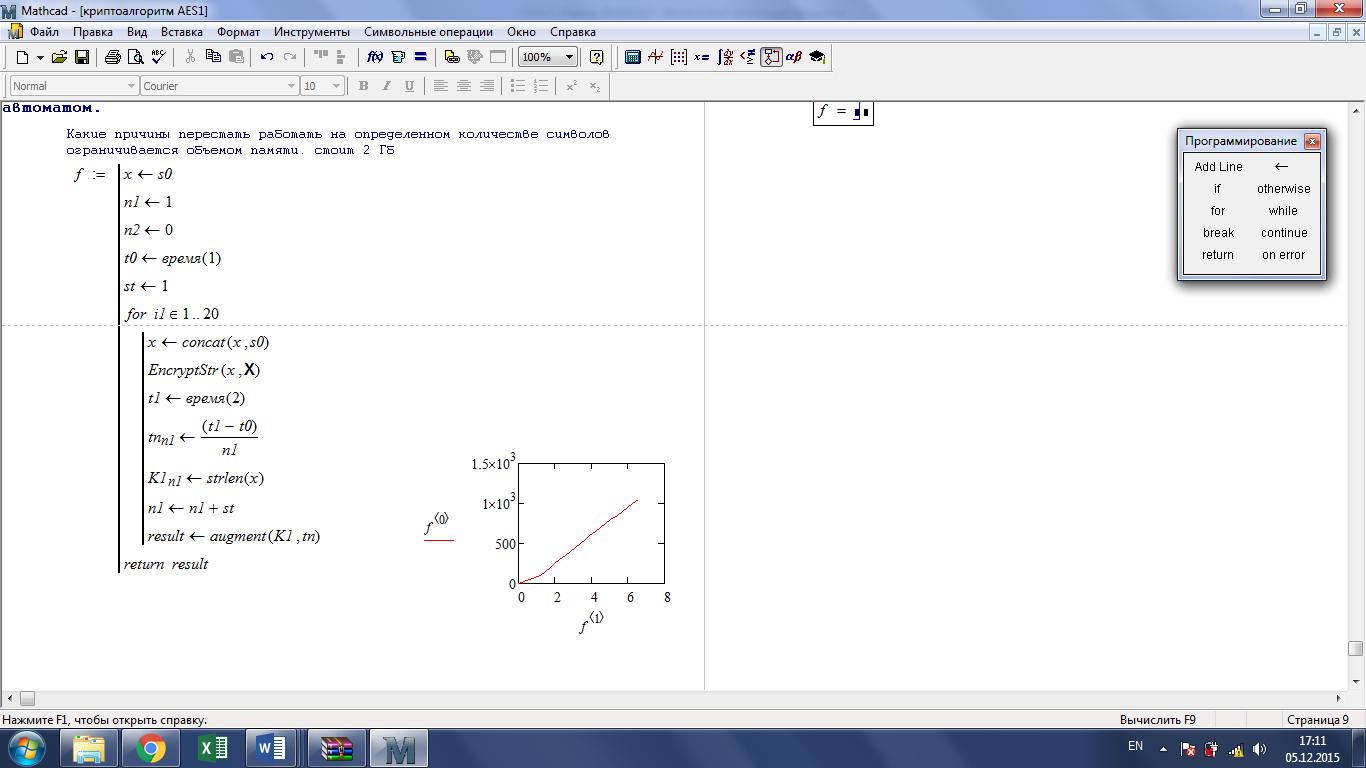


Рисунок 2. Зависимость времени шифрования от длины строки

Как можно видеть по рисунку 2, чем длиннее строка, тем больше времени тратится на шифрование. Сам алгоритм не имеет ограничения на длину строки, он зашифрует столько данных, сколько есть, тут дело лишь во времени. Длина строки может быть ограничена самой программой Mathcad.

**Ответы на вопросы**

***1) Зачем нужна таблица замен и как она повышает криптостойкость алгоритма?***

Таблица замен представляет собой 256-байтый *массив* и используется для *замены одного байта другим*. Цель применения таблицы замен  *затруднить* линейный и дифференциальный *криптоанализ* (т.к. замещение производится по нелинейному принципу).

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

Отечественный криптостандарт ГОСТ был принят, фактически, на 10 лет раньше начала конкурса AES, однако *оба обладают высокой криптографической стойкость,* в данное время ни один из них не имеет алгоритм взлома (за исключением подбора, от этого никто не застрахован).

Стоит также отметить, что если сравнивать производительность алгоритмов ГОСТ 28147-89 и AES, то на 32-битных платформах ГОСТ медленнее криптостандарта США на 10-20%.

За один раунд в AES преобразуются все биты входного блока, по этой причине он может позволить себе меньшее число раундов преобразования, что можно рассматривать, как некоторую компенсацию за потери при реализации режима обратного шифрования.

Таким образом, алгоритм AES опережает ГОСТ 28147-89. – хоть как-то КОЛИЧЕСТВЕННО можно оценить криптостойкость?

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

У режима гаммирования есть аналог в американском стандарте — *режим счетчика (CTR)*. В этом режиме используется простейший генератор псевдослучайных данных, который заключается просто в прибавлении единицы или другой константы к предыдущему значению в пределах разрядной сетки блока. Если прибавляется единица, то выход такого генератора распадается на последовательность дифференциальных пар, т.е. пар значений, различающихся в одном бите, что создает предпосылки для использования против шифра дифференциального криптоанализа. – Предыдущему значению чего?

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

Нет. Так как одной из особенностей гаммирования по ГОСТ 28147-89 является то, что при изменении одного бита шифротекста изменяется один бит расшифрованного текста (это сделано с целю повышения помехозащищённости). А алгоритм AES оперирует байтами. Поэтому гаммирование ГОСТ нельзя реализовать в рамках AES. – из битов всегда можно сделать байты и наоборот

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

*Poly1305-AES (аналог CBC-MAC)*: в качестве ключа используется 128-битный ключ для AES, 106-битный дополнительный код, а также создаётся 128-битная псевдослучайная генерация. Сообщение разбивается на 16-байтные куски, которые становятся коэффициентами полинома в r (одноразовый ключ), оценивается по модуля простого числа  .

## Вывод

В ходе данной лабораторной работы ознакомились с алгоритмом криптопреобразования – AES. Получили практические навыки использования данного алгоритма.