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**

РЕАЛИЗАЦИЯ КРИПТОПРЕОБРАЗОВАНИЯ ПО МЕТОДУ RSA

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

Екатеринбург

2016

**ЦЕЛЬ РАБОТЫ**

1. Установить экспериментально значения исходных строк, при которых программа перестает функционировать правильно. Изменяя размер исходной строки N пределах от одного символа до 1000 символов произвести измерения затрат времени Δt на шифрование, дешифрование AES. Замеры произвести на одном и том же компьютере не менее чем в 20 точках диапазона. Построить графики зависимости Δt от N.
2. Ответить на вопросы:
3. Зачем (свои соображения) нужна таблица замен и как она повышает криптостойкость алгоритма? Ведь таблица постоянная, в отличие от ГОСТ.
4. Оценить сравнительную криптостойкость AES и ГОСТ 28147-89. Какой из алгоритмов более стоек?
5. Какой аналог алгоритма гаммирования ГОСТ 28147-89 есть в стандарте AES?
6. Можно ли реализовать алгоритм гаммирования ГОСТ 28147-89 в рамках AES?
7. Какой аналог алгоритма генерации имитовставки ГОСТ 28147-89 есть в стандарте AES?

**ХОД РАБОТЫ**

1. В ходе выполнения работы было выяснено, что программа перестает работать при превышении количества символов в стоке 1024 штук. Шифрование происходит поблочно в 128 бит. Ограничение в 1024 символов объясняется понятием «Конечное поле» («поле Галуа»).

Ниже приведен рисунок на котором изображено зависимость времени от количество символов (в строке).

Рисунок №1. Зависимость t от N

Эта зависимость является монотонно возрастающей функцией (рисунок №2) и возрастает она ступенчато т.к. шифруется поблочно.

Рисунок №2. Таблица с результатами эксперимента.

Столбец 0 - длина строки, столбец 1 - время

**ОТВЕТЫ НА ВОПРОСЫ**

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

Таблица замен (S-box) – это промежуточная операция шифрования, цель которой изменить порядок у группы битов. Надежность ее высока благодаря замещению, построенному по нелинейному принципу.

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

На текущие время ГОСТ конкурирует с AES-256. У каждого есть свои недостатки. На самом деле ГОСТ менее требователен к вычислительным мощностям чем AES, которому требуется 4 раза больше аппаратных логических вентилей (выполнение операций на 32 и 8 битных платформах, где уступает ГОСТ). Структура у ГОСТ, в частности, диффузия проще, однако компенсируется большим количеством раундов, дополнительной нелинейностью и диффузией, обеспечиваемой сложением по модулю.

Оба способа имеют высокую криптографическую стойкость, в данное время ни один из этих алгоритмов не имеют алгоритма взлома (за исключением подбора). Однако скорость AES оказывается немного быстрее, приблизительно на 15%. – Я так и не понял: кто же криптостойче?

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

Counter mode, CTR (режим счетчика) - предполагает возврат на вход соответствующего алгоритма блочного шифрования значения некоторого счётчика, накопленного с момента старта. Режим делает из блочного шифра потоковый, то есть генерирует последовательность, к которой применяется операция XOR(сложение по модулю) с текстом сообщения. Исходный текст и блок зашифрованного текста имеют один и тот же размер блока, как и основной шифр. Режим CTR предусматривает следующие операции.

Шифрование в режиме CTR

Расшифровка в режиме CTR

 — значение счётчика для i-го блока.

Значения счётчика должны быть уникальными для каждого блока открытого, кодируемого данным шифром при данном ключе (в противном случае, блоки шифротекста, зашифрованные с помощью идентичных значений счётчика оказываются под угрозой). – Откуда берем значение счетчика осталось загадкой.

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

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. – Вроде из битов всегда можно сделать байты и наооборот?

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

Poly1305.

Это MAC (Message authentication code), работающий совместно с AES или любым другим шифром по вашему желанию. Он считает 16 байтный (128 бит) MAC, используя 256 битный ключ AES, который разделяется на два по 128 бит  (k,r)и  соль  (nonce).
Он разбивает сообщение на блоки по 16 байт и работает с ними как с коэффициентами полинома в r по модулю простого числа 2130.
Результат получается на 4 байта меньше, чем обычный HMAC-SHA1 (Hash-based Message Authentication Code - Secure Hash Algorithm 1 - особый хэш для проверки целостности переданной информации), не имеет проблем с безопасностью  и  работает  быстрее. – Если честно – не очень то понятно: как?