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**

КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ. АЛГОРИТМ КРИПТОПРЕОБРАЗОВАНИЯ – ГОСТ 28147-89

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

Екатеринбург

 2016

**Цель:** ознакомиться с алгоритмом криптопреобразования ГОСТ 28147-89, выполнить практическое задание:

1. Научиться компилировать и запускать программы GOST и GOST89.
2. Ответить на следующие вопросы: 1) Что такое блок данных в ГОСТ 28147-89? 2) Что такое таблица замен в ГОСТ 28147-89 и для чего[[1]](#footnote-1)) она нужна? 3) Что такое ключ в ГОСТ 28147-89? 4) В каком случае (чему должны быть равны ключ и таблица замен) шифрованные данные будут тождественны исходным в ГОСТ 28147-89? 5) Что такое гаммирование в ГОСТ 28147-89? 6) Что такое имитовставка в ГОСТ 28147-89 и для чего она нужна в ГОСТ 28147-89? 7) Чем гаммирование с обратной связью отличается от простого гаммирования? 8) Какой алгоритм простое шифрование, гаммирование или гаммирование с обратной связью быстрее и почему? 9) Какой алгоритм простое шифрование, гаммирование или гаммирование с обратной связью не может выполняться параллельно, т.е. на нескольких процессорах? Почему? 10) Почему ГОСТ рекомендует использование гаммирования для шифрования, чем гаммирование лучше простого шифрования?
3. Предложить и реализовать алгоритм прямого перебора ключей для взлома ГОСТ 28147-89.

**Ход работы:**

**Ответы на вопросы**

1) Блок данных – единица обработки информации, в которой находятся алгоритмы для криптографических преобразований, т.е. шифрования и дешифрования.

2) Таблица замен является вектором, содержащим восемь узлов замены. Каждый узел замены, в свою очередь, является вектором, содержащим шестнадцать 4-битовых элементов замены, которые можно представить в виде целых чисел от 0 до 15, все элементы одного узла замены обязаны быть различными. Таким образом, таблица замен может быть представлена в виде матрицы размера 8x16 или 16x8, содержащей 4-битовые заменяющие значения. Для языков программирования, в которых двумерные массивы расположены в оперативной памяти по строкам, естественным является первый вариант (8x16). Тогда узлы замены будут строками таблицы замен. Таким образом, общий объем таблицы замен равен: 8 узлов x 16 элементов/узел x 4 бита/элемент = 512 бит = 64 байта. Таблица замен является дополнительным 512-битовым ключом, т.е. используется для шифрования.

Таблица замен является долговременным ключевым элементом, то есть действует в течение гораздо более длительного срока, чем отдельный ключ. Предполагается, что она является общей для всех узлов шифрования в рамках одной системы криптографической защиты. Даже при нарушении конфиденциальности таблицы замен стойкость шифра остается чрезвычайно высокой и не снижается ниже допустимого предела. Таблица замен необходима для поблочной замены 32-битного значения полученного в результате сложения младшей половины преобразуемого блока с используемым элементом ключа. Замена необходима для обеспечения криптостойкости алгоритма.

3) Ключом в данном алгоритме служит массив из восьми 32-битных чисел. Таким образом, длина ключа составляет 256 бит. Ключ можно представить как таблицу, в которой 8 строк и 32 столбца. Такая конфигурация ключа необходима для работы алгоритма. Ключ необходим для шифрования/расшифровки сообщений (данных). Ключ – это секретный параметр криптопреобразования.

4) В готовой программе шифрованные данные будут тождественны исходным в случае, когда ключ симметричный и все элементы таблицы замен единицы.

*5) Гаммирование* – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Для наложения гаммы при зашифровании и ее снятия при расшифровании должны использоваться взаимно обратные бинарные операции, например, сложение и вычитание по модулю 264 для 64-битовых блоков данных. В ГОСТе для этой цели используется операция побитового сложения по модулю 2, поскольку она является обратной самой себе и, к тому же, наиболее просто реализуется аппаратно.

Операция сложения по модулю 2 часто обозначается , то есть можно записать:

6) Имитовставка — специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных. Имитовста́вка обычно применяется для обеспечения целостности и защиты от фальсификации передаваемой информации.

7) Гаммирование с обратной связью похоже на режим гаммирования и отличается от него только способом выработки элементов гаммы – очередной элемент гаммы вырабатывается как результат преобразования по циклу 32-З предыдущего блока зашифрованных данных, а для зашифрования первого блока массива данных элемент гаммы вырабатывается как результат преобразования по тому же циклу синхропосылки. Этим достигается зацепление блоков – каждый блок шифртекста в этом режиме зависит от соответствующего и всех предыдущих блоков открытого текста. Поэтому данный режим иногда называется гаммированием с зацеплением блоков. На стойкость шифра факт зацепления блоков не оказывает никакого влияния. Шифрование в режиме гаммирования с обратной связью обладает теми же особенностями, что и шифрование в режиме обычного гаммирования, за исключением влияния искажений шифртекста на соответствующий открытый текст.

8) Самым быстрым алгоритмом шифрования является простая замена, так как его реализация самая простая.

Режим [простой замены](https://traditio.wiki/w/index.php?title=Простая_замена&action=edit&redlink=1) принимает на вход данные, размер которых кратен 64-м битам. Результатом шифрования является входной текст, преобразованный блоками по 64 бита в случае зашифрования циклом «32-З», а в случае расшифрования — циклом «32-Р».

9) Алгоритм шифрования у режима гаммирования с обратной связью похож на алгоритм режима простого гаммирования, однако гамма формируется на основе предыдущего блока зашифрованных данных, так что результат шифрования текущего блока зависит также и от предыдущих блоков. Именно эта зависимость не позволит выполнить это шифрование (гаммирование с обратной связью) параллельно, в отличие от гаммирования.

10) Проблемы простого шифрования: В простом шифровании при шифровании 2 одинаковых блоков текста мы получим одинаковые шифр-тексты. Из-за этого криптоаналитик придет к выводу об идентичности блоков, что является недопустимым для серьезного шифра. Также, если длина массива не кратна 64 битам, появится проблема с дополнением последнего неполного блока памяти (увеличение числа шифртекста нежелательна, а заполнение пустых блоков нулями или фиксированными 0-1, приведет к возможности перебором определить содержимое, что делает алгоритм некриптостойким). Т.о., очень сильно ограничивается возможность применения шифра. Потому ГОСТ рекомендует использование такого метода для шифрования ключевых данных. Эти проблемы решаются при шифровании гаммированием. Потому оно и рекомендуется ГОСТом.

**Предложить и реализовать алгоритм прямого перебора ключей для взлома ГОСТ 28147-89:**

Перебрать мы можем все ключи, но проблема заключается в том, чтобы найти из всех ключей — нужный! Тогда можно применить следующий алгоритм:

Сначала генерируем все возможные сообщения и ключи. Далее шифруем сгенерированные нами сообщения сгенерированными ключами. Шифруем не все сообщение целиком, а по блокам. Затем сравниваем шифр с перехваченными данными. Может оказаться, что ключи совпадают, поэтому шифруем следующий блок данных и снова сравниваем — совпадающих ключей окажется меньше. Продолжаем до тех пор, пока не останется 1-2 ключа, с помощью который уже точно сможем отличить истинное сообщение.

Не заметил дополнительных мыслей относительно предыдущего оратора (Борисенко). Замечания те же самые.

**Вывод**

В ходе данной лабораторной работы ознакомились с алгоритмом криптопреобразования – ГОСТ 28147-89 и получили практические навыки его использования.

1. [↑](#footnote-ref-1)