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

Екатеринбург

 2016

## **Введение**

Криптография — наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации.

Криптографические методы защиты информации - это специальные методы шифрования, кодирования или иного преобразования информации, которые используются для сокрытия содержания информации, подтверждения ее целостности, авторства и т.д.

*Шифр* — совокупность обратимых преобразований множества открытых текстов (т.е. исходного сообщения) на множество зашифрованных текстов, проводимых с целью их защиты.

Российская Федерация имеет свой стандарт шифрования. Этот стандарт закреплен ГОСТом №28147-89.

ГОСТ 28147-89 — блочный шифр с 256-[битным](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82) [ключом](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29) и 32 циклами преобразования, оперирующий 64-битными блоками. Выделяют четыре режима работы ГОСТ 28147-89:

* [простой замены](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%BA%D0%BE%D0%B4%D0%BE%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BD%D0%B8%D0%B3%D0%B8)
* [гаммирование](https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)
* [гаммирование с обратной связью](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B6%D0%B8%D0%BC_%D0%BE%D0%B1%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B9_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8_%D0%BF%D0%BE_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82%D1%83)
* режим выработки [имитовставки](https://ru.wikipedia.org/wiki/%D0%98%D0%BC%D0%B8%D1%82%D0%BE%D0%B2%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B0).

**Цели:**

1. Научиться компилировать и запускать программы GOST и GOST89.
2. Ответить на следующие вопросы:
	1. Что такое блок данных?
	2. Что такое таблица замен и для чего она нужна?
	3. Что такое ключ?
	4. В каком случае (чему должны быть равны ключ и таблица замен) шифрованные данные будут тождественны исходным?
	5. Что такое гаммирование?
	6. Что такое имитовставка? И для чего она нужна?
	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.
4. Модифицировать тестовую программу сжатия файла «GOST 28147-89.xmcd» или «Gost89.exe» так, чтобы она работала быстрее. Критерии сравнения: ускорение должно быть не менее 1% по сравнению с готовым вариантом тестовой программы, который предоставлен вам вместе с исходным кодом.

**Ход работы:**

1. Блок данных – единица обработки информации, в котором определены алгоритмы для криптографических преобразований, таких как шифрование и дешифрование;
2. Таблица замен представляет матрицу 8х16. Каждая строка представляет собой узлы замены, содержащих 16 4-битных заменяющих значений. Таблица 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.
3. Ключ – секретный параметр преобразования, используется для шифрования/дешифрования данных. В представляет собой массив из 8 32-битовых элементов кода.
4. Шифрованные данные будут тождественны исходным, если ключ будет симметричным, а все элементы таблицы замены равны 1.
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  для 64-битовых блоков данных. В ГОСТе для этой цели используется операция побитного сложения по модулю 2, поскольку она является обратной самой себе и, к тому же, наиболее просто реализуется аппаратно.

1. Имитовставка – контрольная комбинация, зависящая от открытых данных и секретной ключевой информации. Целью использования имитовставки является обнаружение всех случайных или преднамеренных изменений в массиве информации.
2. Гаммирование с обратной связью отличается от простого гаммирования 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.
3. Самым быстрым алгоритмом шифрования является простая замена по причине более простой реализации в сравнении со всеми остальными. Режим [простой замены](https://traditio.wiki/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BC%D0%B5%D0%BD%D0%B0&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». Остальные методы шифрования более сложны и занимают больше времени на процесс шифрования.
4. 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. Зависимость не позволит выполнить это шифрование параллельно, в отличие от прочих методов.
5. Проблемы простого шифрования: В простом шифровании при шифровании 2 одинаковых блоков текста мы получим одинаковые шифртексты. 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.

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

**Ход работы:**

В ходе данной лабораторной работы мы прошли введение в криптографические методы защиты информации. Мы изучили теорию, связанную с ГОСТ 28147-89, в частности режимов его работы: простой замены, гаммирования, гаммирования с обратной ставкой и выработки имитоставки, ответили на вопросы и ознакамливались с решением задач в пакетк MathCAD.