

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Санкт-Петербургский государственный технологический институт (технический университет)»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| УГНС | | 09.00.00 | Информатика и вычислительная техника | | |
| Направление подготовки | | 09.03.01 | Информатика и вычислительная техника | | |
| Направленность (профиль) | |  | Системы автоматизированного проектирования | | |
| Форма обучения | |  | очная | | |
|  | |  |  | | |
| Факультет | |  | Информационных технологий и управления | | |
| Кафедра | |  | Систем автоматизированного проектирования и управления | | |
| Учебная дисциплина | |  | Программирование | | |
| Курс | II | | | Группа | 404 |

Отчёт по лабораторной № 2

Вариант № 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Исполнитель: |  |  |  |  |
| обучающийся группы 404 |  |  |  | Д. К. Азаров |
|  |  | (дата, подпись) |  |  |
|  |  |  |  |  |
| Проверили: |  |  |  | И. Г. Корниенко |
|  |  | (дата, подпись) |  | А. К. Федин |

### 1 Постановка задачи

Создать интерфейс ICipher, который определяет методы поддержки шифрования строк. В интерфейсе объявляются два метода Encode() и Decode(), которые используются для шифрования и дешифрования строк, соответственно. Реализовать классы шифрования ГОСТ 28147-89, Гаммирование.

### 2 Исходные данные

Строка и ключ.

### 3 Особые ситуации

Необходимо рассмотреть следующую особую ситуацию в шифровании по ГОСТ 28147-89:

1. Длина ключа должна быть 256 бит;
2. Кол-во бит в строке должно быть кратно 64.

Необходимо рассмотреть следующую особую ситуацию в шифровании по ГОСТ 28147-89:

1. Длина ключа не должна превышать размер текста.

### 4 Математические методы и алгоритмы решения задач

#### Шифрование по ГОСТ 28147-89:

#### **Зашифровывание:**

1. Открытые данные разбиваются на блоки по 64 бита.
2. Далее производится ввод первого блока в накопители N1 и N2. При этом биты открытой информации вводятся следующим образом: 1-й бит открытой информации — в 1-й разряд накопителя N1, ..., 32-й — в 32-й разряд накопителя N1, 33-й — в 1-й разряд накопителя N2 и так далее, пока 64-й бит открытой информации не будет введен в 32-й разряд накопителя N2.
3. В КЗУ вводится ключ длиной 256 бит способом, рассмотренным в статье.

#### **Производится зашифрование открытых данных в режиме простой замены (в 32 цикла):**

* 1. В первом цикле содержимое регистра N1 суммируется с заполнением X0 из КЗУ по модулю 232 в сумматоре СМ1.
  2. В блоке подстановки K производится замена 32 бит информации, поступившей из сумматоре СМ1.
  3. В регистре сдвига R осуществляется циклический сдвиг на 11 в сторону старшего разряда.
  4. Информация с регистра сдвига R и накопителя N2 суммируется по модулю 2 в сумматоре СМ2.
  5. Старое заполнение накопителя N1 переписывается в накопитель N2.
  6. Результат с выхода сумматора СМ2 переписывается в накопитель N1.
  7. Первый цикл заканчивается.

1. Последующие циклы аналогичны первому, с тем лишь отличием, что во 2-м цикле вводится ключ X1, в 8-м — X7, в 9-м — X0 и так далее в том же порядке до 24 цикла. С 25 по 32 цикл ключ вводится в обратном порядке: X7 — в 25-м, X0 — в 32-м.
2. После 32-го цикла в N1 информация сохраняется, а вот результат с выхода сумматора СМ2 переписывается в N2.
3. Заполнение N1 и N2 и есть первый блок зашифрованных данных.
4. Следующие блоки зашифровываются аналогично.

#### **Расшифровывание:**

Расшифровывание осуществляется по тому же алгоритму, что и зашифровывание, только на вход накопителей N1 и N2 поступают разбитые на блоки по 64 бита зашифрованные данные. Важным отличием является еще и то, что в прямом порядке (с X0 по X7) ключ вводится только в первых 8 циклах РПЗ, в остальных — в обратном (с X7 по X0).А так, после прохождения 32 циклов в накопителях N1 и N2 содержатся блоки открытых данных.

Шифрование Гаммированием:

***Шифрование:***

1. Заполняется ключ до размера текста циклическим копированием введенного ключа;
2. Каждый символ текста складывается по модулю 2 с соответствующим символом ключа.

#### **Расшифровывание:**

Аналогично с шифрованием, но на вход поступает зашифрованный текст.

### 5 Форматы представления данных

Таблица - Классы, используемые в программе

|  |  |  |  |
| --- | --- | --- | --- |
| **Название** | **Имя переменной** | **Тип** | **Описание** |
| Gost28147\_89 | - | - | Реализует шифрование по ГОСТ 28147-89 |
| replacementBlock | Byte[,] | Таблица замены |
|  | **Метод** | **Тип** | **Описание** |
|  | Encode | Byte[] | Кодирование |
|  | Decode | String | Декодирование |
|  | Coding | Byte[] | Алгоритм шифрования |
|  | SumFromMod\_2\_Degree\_32 | UInt32 | Сложение по модулю 2 |
|  | SubstitutionBlock | UInt32 | Замена блоков |
|  | ShiftingRegister | UInt32 | Сдвиг влево на 11 |
|  | SumFromMod\_2 | UInt32 | Сумма по модулю 2 |
| GammaXoring | - | - | Реализует шифрование Гаммированием |
| **Метод** | **Тип** | **Описание** |
| Encode | Byte[] | Кодирование |
| Decode | String | Декодирование |
| Coding | Byte[] | Алгоритм шифрования |
|  | FillKeyBytes | Byte[] | Заполнение ключа |

### 6 Структура программы

Таблица - Интерфейсы, используемые в программе

|  |  |
| --- | --- |
| **Имя** | **Описание** |
| ICipher | Кодировка – Декодировка строк |

### 7 Блок-схем алгоритмов программы

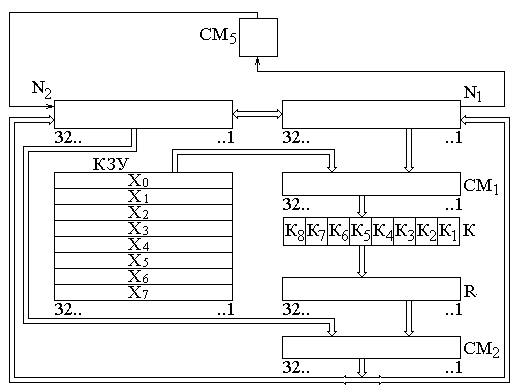


Рисунок – Блок-схема алгоритма шифрования по ГОСТ 28147-89

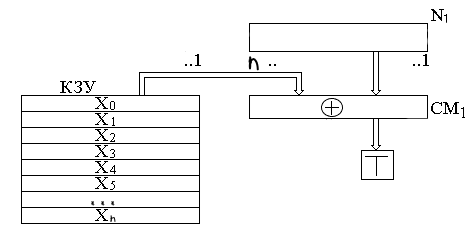


Рисунок - Блок-схема алгоритма шифрования Гаммированием

### 8 Описание хода выполнения лабораторной работы

1. В ходе лабораторной работы было создано решение (Solution) в интегрированной среде разработки Microsoft Visual Studio C# WinForms 2019. В нем был создан проект.
2. В ходе лабораторной работы выявлена ошибка – пользователь мог ввести некорректную длину ключа, было принято решение добавлять ‘\0’ в конец переданной строки.
3. В ходе лабораторной работы выявлена ошибка – можно было передать некорректный размер зашифрованного текста. Было принято решение вызывать ошибку ‘throw’.
4. В ходе лабораторной работы выявлена ошибка – можно было передать некорректный размер ключа. Было принято решение вызывать ошибку ‘throw’.
5. В ходе лабораторной работы выявлена ошибка – использовалось сложение по модулю 2 int чисел, а не сложение по модулю 2 бит этих чисел. Было принято использовать оператор ‘^’ для сложения чисел.

### 9 Результаты работы программы

В результате вычислений программа выводит зашифрованный / расшифрованный текст.

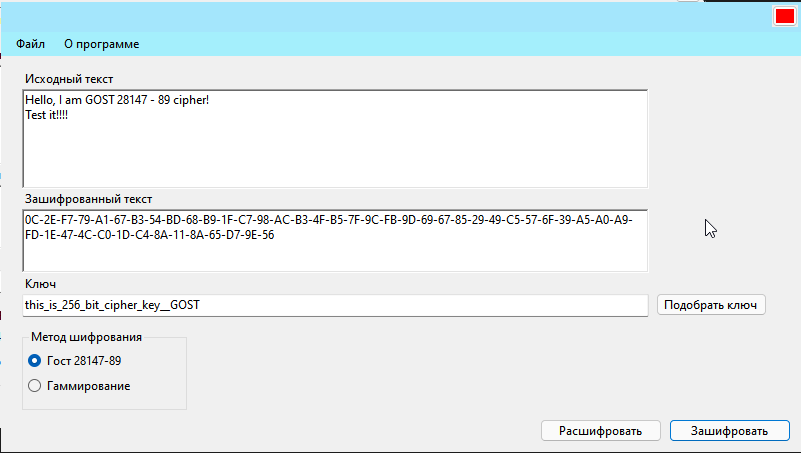


Рисунок – Шифрование по ГОСТУ

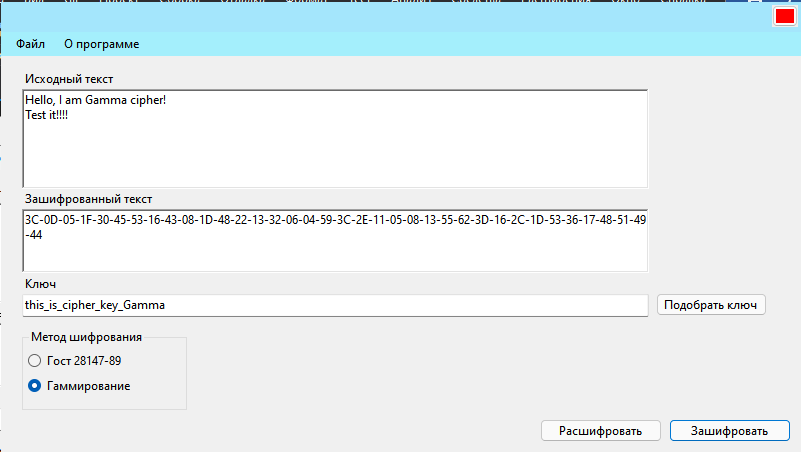


Рисунок - Шифрование Гамморованием

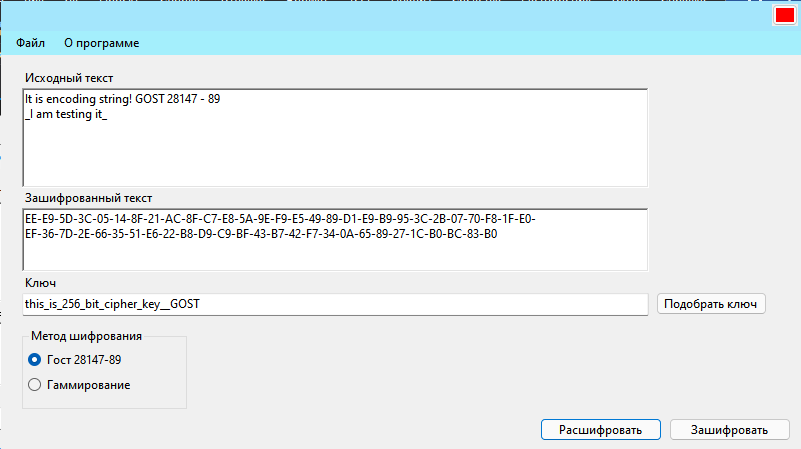


Рисунок – Расшифровывание ГОСТ

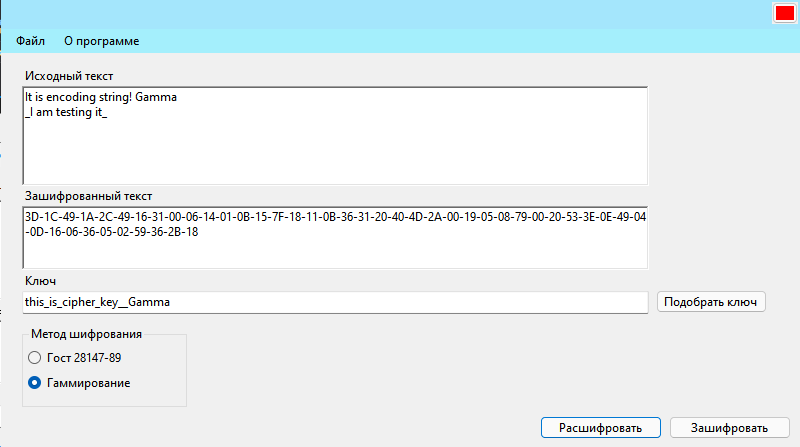


Рисунок – Расшифровывание Гаммой

### 10 Исходный текст программы

[Начало dan.cpp ---]

[--- Конец dan.cpp]