Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина «Операционные системы и среды»

**ОТЧЕТ**

к лабораторной работе

на тему:

**«Симметричная криптография. Стандарт шифрования ГОСТ 28147-89.»**

|  |  |
| --- | --- |
|  | Выполнил:  Слуцкий Никита Сергеевич,  студент группы 053505 |
|  | Проверил: Лещенко Евгений Александрович, ассистент каф. Информатики |

Минск 2023

СОДЕРЖАНИЕ

[Введение 3](#_Toc145861817)

[1 Краткие теоретические сведения 3](#_Toc145861818)

[1.1 Сеть Фейстеля 3](#_Toc145861819)

[1.2 ГОСТ 28147-89 4](#_Toc145861820)

[1.3 Гаммирование с обратной связью 4](#_Toc145861821)

[2 Ход выполнения работы 5](#_Toc145861822)

[Заключение 5](#_Toc145861823)

[Приложение А Листинг кода 6](#_Toc145861824)

# ВВЕДЕНИЕ

Целью данной лабораторной работы является реализация алгоритма симметрического шифрования ГОСТ 28147-89 в режиме, соответствующем варианту задания, с использованием выбранного языка программирования.

Задачей ставится реализовать программнре средства шифрования и дешифрования текстовых файлов при помощи стандарта шифрования ГОСТ 28147-89 в режиме гаммирования с обратной связью (3-й вариант).

# Краткие теоретические сведения

## 1.1 Сеть Фейстеля

Сеть Фейстеля, или конструкция – один из методов построения блочных шифров. Сеть состоит из ячеек, называемых ячейками Фейстеля. На вход каждой ячейки поступают данные и ключ. На выходе каждой ячейки получают изменённые данные и изменённый ключ. Все ячейки однотипны, и говорят, что сеть представляет собой определённую многократно повторяющуюся (итерированную) структуру. Ключ выбирается в зависимости от алгоритма шифрования/расшифрования и меняется при переходе от одной ячейки к другой. При шифровании и расшифровании выполняются одни и те же операции; отличается только порядок ключей. На рисунке 1 изображена схема сети.

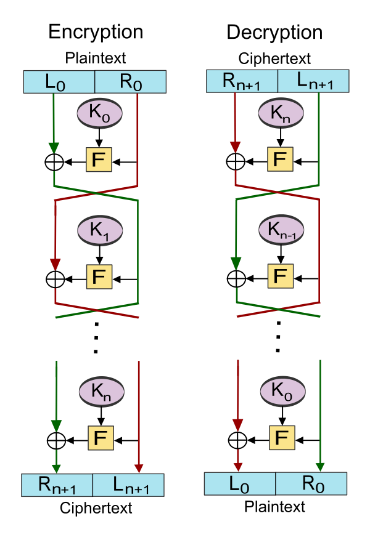


Рисунок 1. Схематичное изображение сети Фейстеля

## ГОСТ 28147-89

ГОСТ 28147-89 – государственный стандарт СССР (а позже межгосударственный стандарт СНГ), описывающий алгоритм симметричного блочного шифрования и режимы его работы.

Является примером DES-подобных криптосистем, созданных по классической итерационной схеме Фейстеля. ГОСТ 28147-89 – блочный шифр с 256-битным ключом и 32 циклами (называемыми раундами) преобразования, оперирующий 64-битными блоками. Основа алгоритма шифра – сеть Фейстеля.

Выделяют четыре режима работы ГОСТ 28147-89:

* простой замены;
* гаммирование;
* гаммирование с обратной связью;
* режим выработки имитовставки.

Описание действия базового алгоритма опускается.

## 1.3 Гаммирование с обратной связью

В режиме гаммирования с обратной связью текст всё так же разбивается на блоки. Вводится дополнительный параметр – начальный гамма-блок. Шифруется с помощью метода простой замены сам гамма-блок, а затем поэлементно складывается по модулю 2 с блоком. Полученный результат - и есть результат шифрования блока. Гамма-блок, в свою очередь, также перезаписывается получившимся значением. Таким образом на каждой итерации значение гаммы разное, оно получается из предыдущего шага. Отсюда и название режима. На рисунках 2, 3 изображена схема шифрования и дешифрования с использованием этого режима.

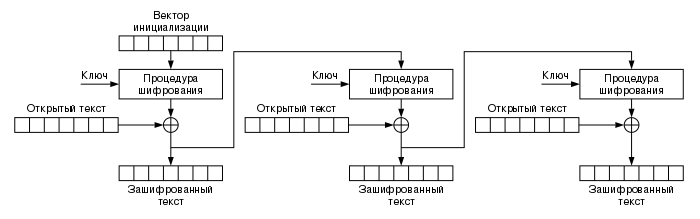


Рисунок 2. Схема шифрования в режиме гаммирования с обратной связью

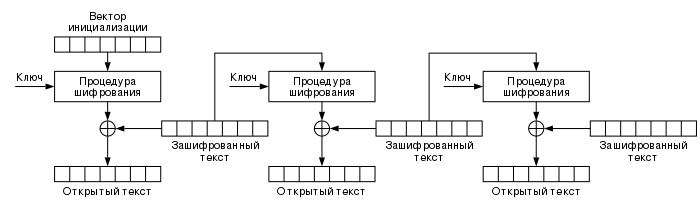


Рисунок 3. Схема дешифрования в режиме гаммирования с обратной связью

# 2 Ход выполнения работы

Программное средство написано на языке программирования C++. В файлах gost28147\_89.hpp и gost28147\_89.cpp находятся, соответственно, заголовки и тела функций, реализующих непосредственно шифрование. В такой же группе файлов utils находятся вспомогательные функции для ввода, вывода, работы со строками и массивами. Программа написана на современном стандарте языка C++ 17 с использованием контейнеров STL, итераторов и современного «синтаксического сахара», а также некоторых практик по именованию из Google Style Guide для написания читаемого кода.

В приложении с листингом кода предоставлена вырезка кода с функцией шифрования в режиме гаммирования с обратной связью.

# Заключение

В ходе выполнения данной работы было произведено ознакомление с теорией о сети Фейстеля и алгоритме симметричного шифрования ГОСТ 28147-89, реализовано программное средство для шифрования и расшифрования файлов с использованием данного шифрования в режиме гаммирования с обратной связью. Цели лабораторной работы можно считать достигнутыми.

# ПРИЛОЖЕНИЕ А

(Листинг кода)

std::vector<uint8\_t> encrypt\_by\_gost28147\_89\_with\_gamma(

const std::vector<uint8\_t> &open\_text,

const std::vector<uint8\_t> &key,

const std::vector<uint8\_t> &initial\_gamma

)

{

validate\_key(key); // throws if key.length % 32 !== 0

validate\_open\_text(open\_text); // throws if open\_text.length % 8 !== 0

validate\_initial\_gamma(initial\_gamma); // throws if gamma length is not 8

std::vector<std::vector<uint8\_t>> blocks{split\_vector\_on\_blocks(open\_text, 8)};

std::vector<uint32\_t> sub\_keys{get\_uint32\_subkeys(key)};

std::vector<uint8\_t> response{}; // result

std::vector<uint8\_t> gamma(std::cbegin(initial\_gamma), std::cend(initial\_gamma));

for (const auto &block : blocks)

{

std::vector<uint8\_t> crypted\_gamma{crypt\_block(gamma, sub\_keys, ACT\_ENCRYPT)}; // encrypt or decrypt gamma

std::vector<uint8\_t> crypted\_gamma\_xored\_with\_block{apply\_gamma(block, crypted\_gamma)}; // xor it with block

gamma = slice\_vector(crypted\_gamma\_xored\_with\_block, 0, crypted\_gamma\_xored\_with\_block.size()); // override gamma

for (const auto &value : crypted\_gamma\_xored\_with\_block)

{

response.push\_back(value);

}

}

return response;

}