ПЕТРОЗАВОДСКТЙ ГОСУДАРСТВЕННИЙ УНИВЕРСИТЕТ ИНСТИТУТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАТИКИ И МАТЕМАТИЧЕСКОГО ОБЕСПЕЧЕНИЯ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Отчет о лабораторной работе №4 по курсу <<Информационная безопасность и зашита информации>>

**Тема:** **Шифрование произвольного файла методом гаммирования**

Выполнил: студент 2 курса группы 22206 Шарипов Отабек

**Проверил: СОКОЛОВ ВЛАДИСЛАВ ЕВГЕНЬЕВИЧ**

**Петрозаводск 2022г**

**Содержание**

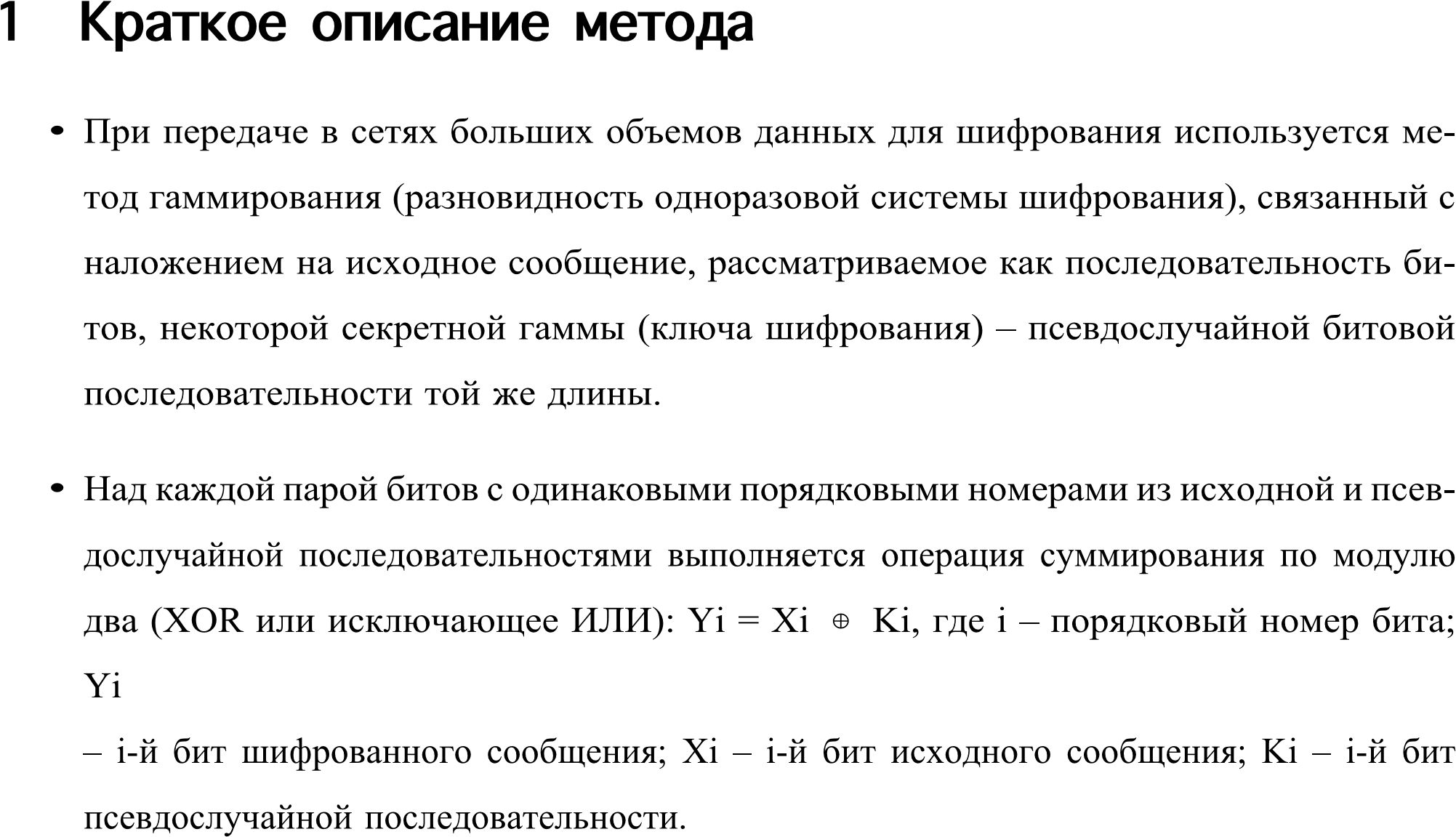
1 Краткое описание метода

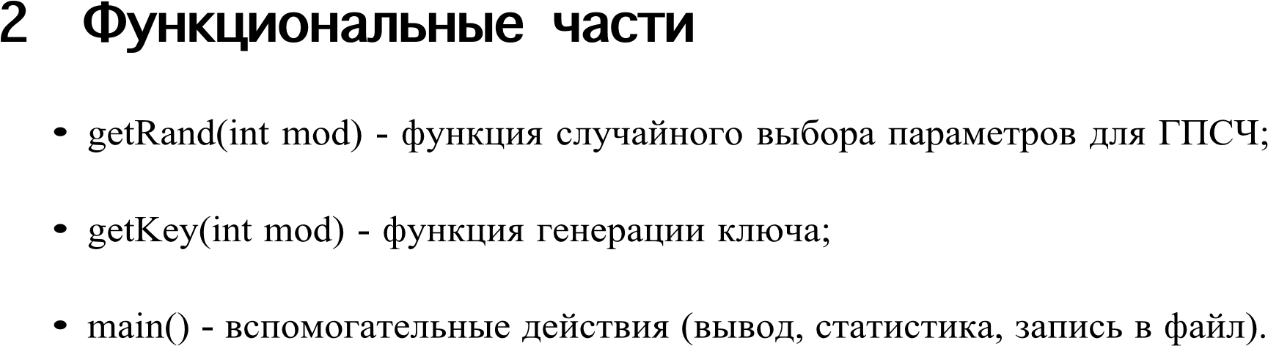
2 Функциональные части

3 Фрагменты программной реализации

4 Как работает программа

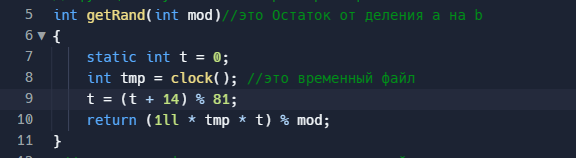
Заключение



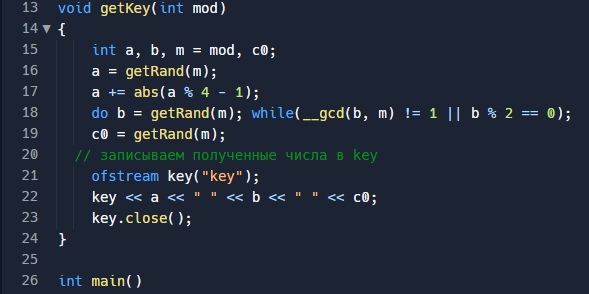


**3 Фрагменты программной реализации**

Функция случайного выбора параметров для ГПСЧ в зависимости от времени суток.

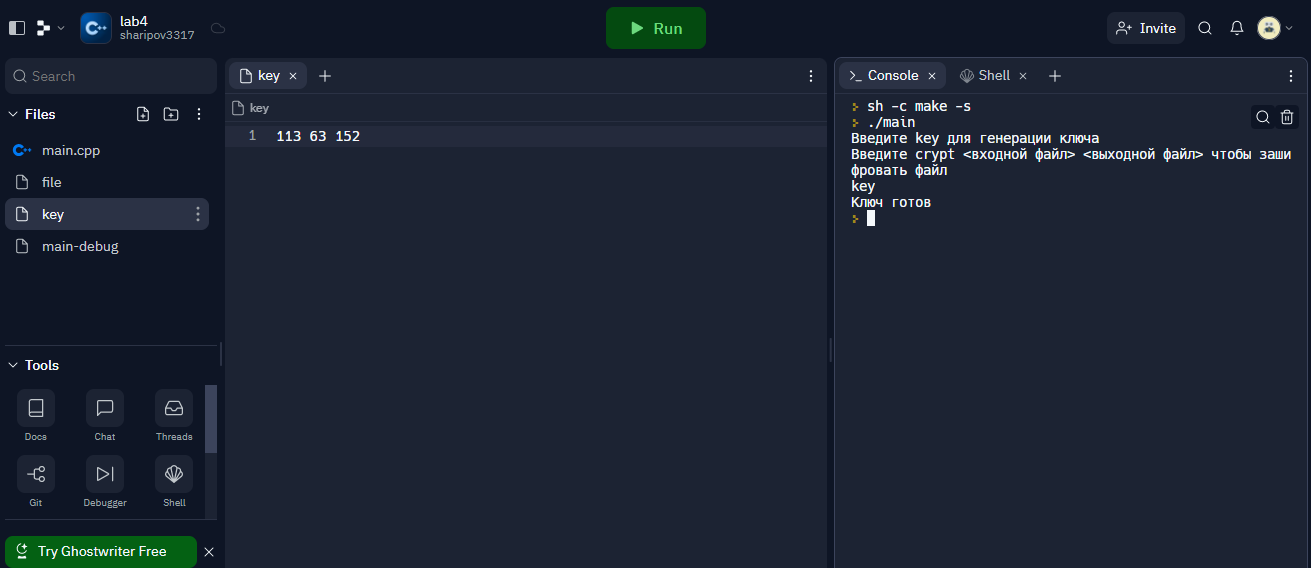


Функция генерации ключа.

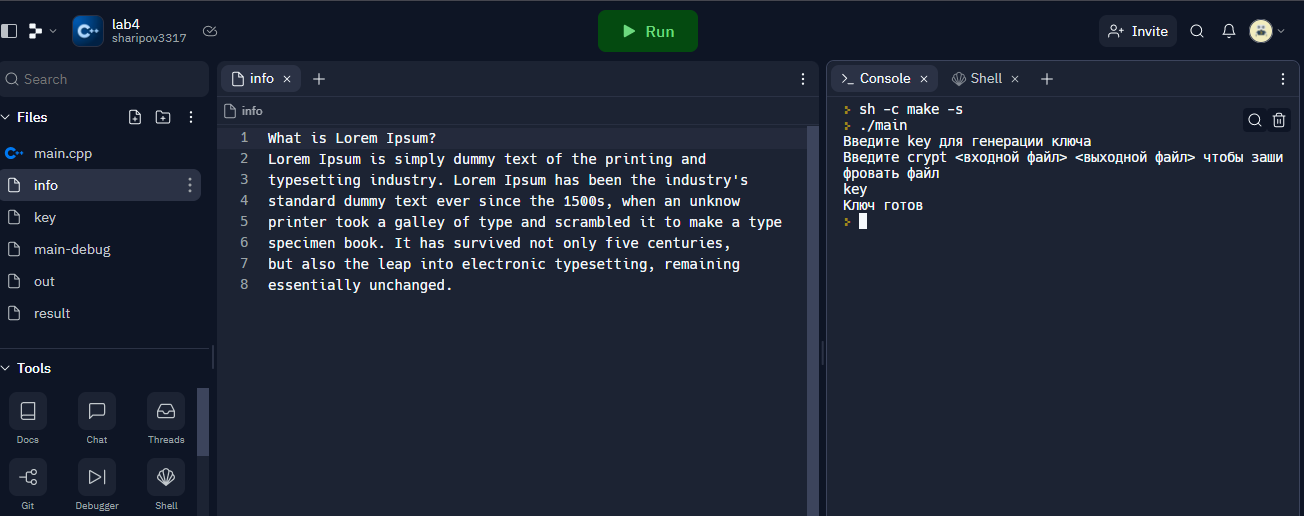


**4 Как работает программа**

У нас есть три основных файла. После запуска программы вводим в консоль слово (key) для генерации псевдослучайных чисел. И в нашем файле с именем key мы получили три значения чисел. Теперь у нас есть ключи.

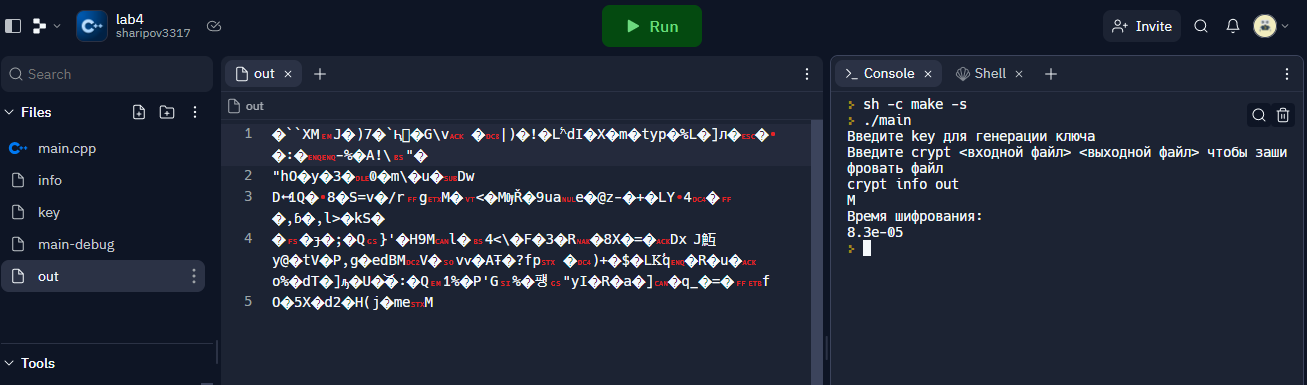


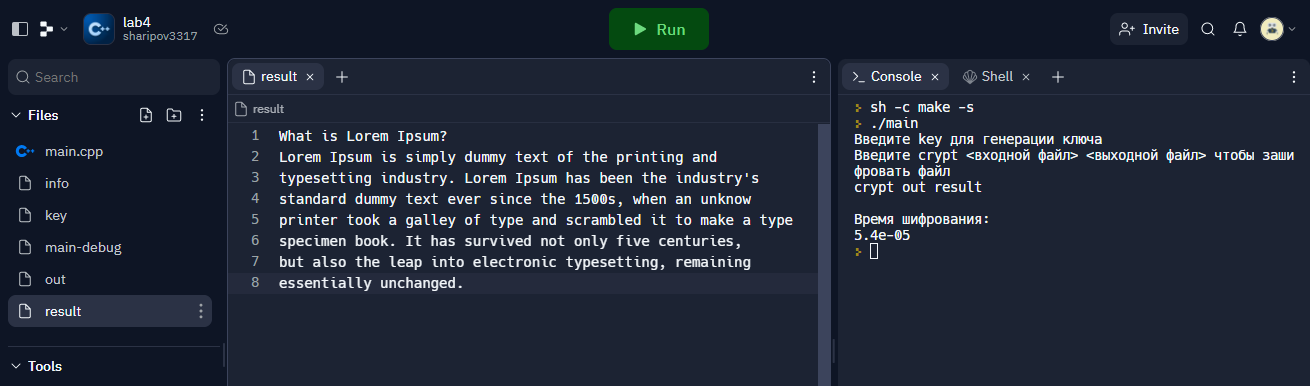
Теперь перейдем к нашему файлу с именем (info). Мы храним в этом файле данные любого типа. У нас простой текс.



Мы перезапускаем нашу программу, вводим ключевое слово crypt в консоль и вводим названия нашего info файла и создаем новый файл, пишем новое названия для файла.

Как видите, мы назвали файл out. Мы гаммировали текст в info файле в out файл. Наша программа сработала успешно.



Теперь Возвращаем текст в прежнее состояние. В консоли напишем Crypt out и название нового файла например result и появляется новый файл и текст возвращается в исходное состояние.

**Заключение**

Теперь мы знаем, как применять блочные алгоритмы шифрования для работы с сообщениями произвольной длины с использованием режима гаммирования. Это позволяет избежать основного недостатка режима прямой замены (если шифруемое сообщение содержит в себе одинаковые или повторяющиеся блоки, то на выходе мы тоже получим зашифрованные одинаковые или повторяющиеся блоки).

**Извините за ошибки.**