Лабораторная работа №3

Математические основы защиты информации и информационной безопасности

Николаев Дмитрий Иванович, НПМмд-02-24

Содержание

# 1 Цель работы

Изучить работу алгоритма шифрования гаммированием конечной гаммой, а также реализовать его программно.

# 2 Теоретическое введение

## 2.1 Шифрование гаммированием

Из всех схем шифрования простейшей и наиболее надежной является схема однократного использования. Формируется - разрядная случайная двоичная последовательность — ключ шифра. Отправитель производит побитовое сложение по модулю два (mod 2) ключа

и -разрядной двоичной последовательности:

соответствующей посылаемому сообщению:

где — -й бит исходного текста, — -й бит ключа, – операция побитового сложения (XOR), — -й бит получившейся криптограммы

Операция побитного сложения является обратимой, т.е. , поэтому дешифрование осуществляется повторным применением операции к криптограмме

Основным недостатком такой схемы является равенство объема ключевой информации и суммарного объема передаваемых сообщений. Данный недостаток можно убрать, использовав ключ в качестве “зародыша”, порождающего значительно более длинную ключевую последовательность.

Гаммирование — процедура наложения при помощи некоторой функции на исходный текст гаммы шифра, т.е. псевдослучайной последовательности (ПСП) с выходом генератора . Псевдослучайная последовательность по своим статистическим свойствам неотличима от случайной последовательности, но является детерминированной, т.е. известен алгоритм ее формирования. Чаще всего в качестве функции берется операция поразрядного сложения по модулю два или по модулю ( — число букв алфавита открытого текста).

Простейший генератор псевдослучайной последовательности можно представить рекуррентным соотношением:

где — -й член последовательности псевдослучайных чисел, , , — ключевые параметры. Такая последовательность состоит из целых чисел от до . Если элементы и совпадут, то совпадут и последующие участки: , . Таким образом, ПСП является периодической. Знание периода гаммы существенно облегчает криптоанализ. Максимальная длина периода равна . Для ее достижения необходимо удовлетворить следующим условиям:

1. и — взаимно простые числа;
2. делится на любой простой делитель числа ;
3. кратно 4, если кратно 4.

Стойкость шифров, основанных на процедуре гаммирования, зависит от характеристик гаммы — длины и равномерности распределения вероятностей появления знаков гаммы.

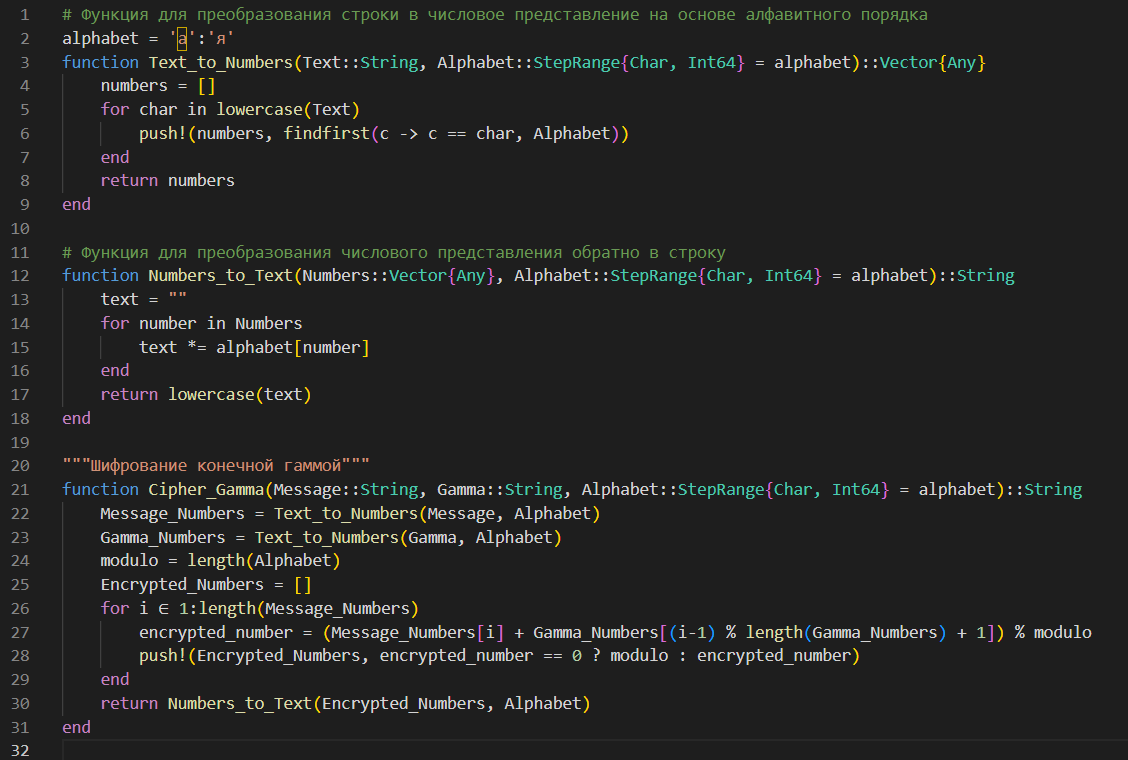
При использовании генератора ПСП получаем бесконечную гамму. Однако, возможен режим шифрования конечной гаммы. В роли конечной гаммы может выступать фраза. Как и ранее, используется алфавитный порядок букв, т.е. буква “а” имеет порядковый номер 1, “б” — 2 и т.д.

Например, зашифруем слово “ПРИКАЗ” (“16 17 09 11 01 08”) гаммой “ГАММА” (“04 01 13 13 01”). Будем использовать операцию побитового сложения по модулю 33 (mod 33). Получаем:

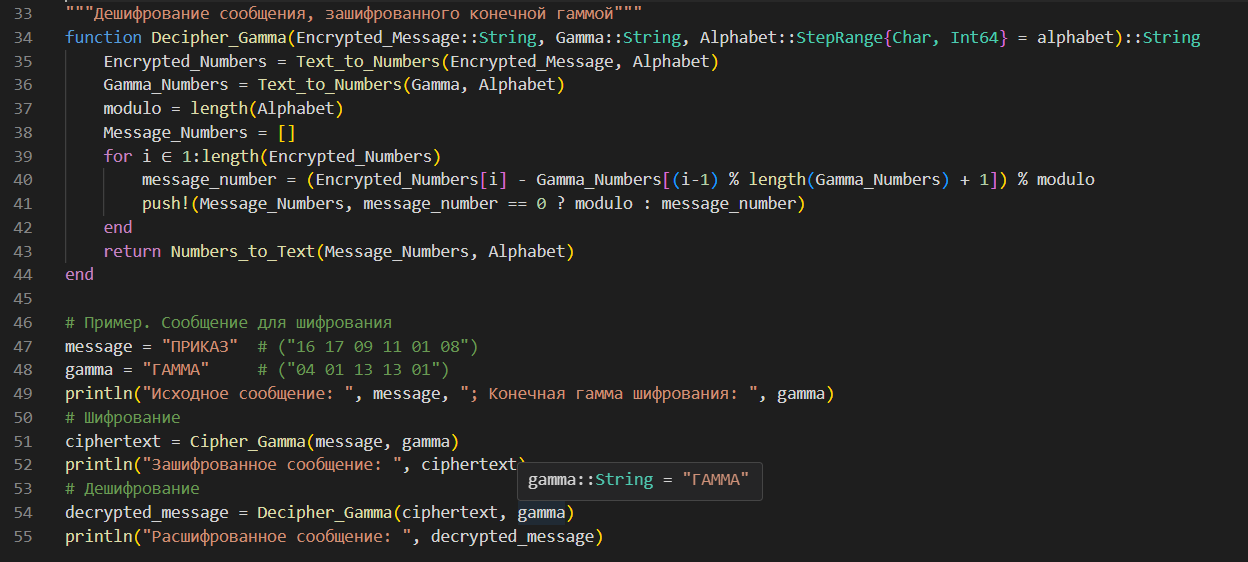
Криптограмма: “УСХЧБЛ” (“20 18 22 24 02 12”).

# 3 Выполнение лабораторной работы

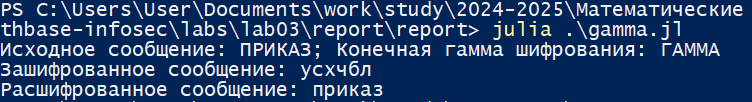
Следуя указаниям [1], реализуем алгоритм шифрования гаммированием конечной гаммой и его расшифрование на Julia ([??,??]), в результате получим следующий вывод ([??]).



Код реализации алгоритма шифрования конечной гаммой на Julia



Код реализации алгоритма дешифрования сообщения, зашифрованного конечной гаммой на Julia



Результат кода реализации алгоритма шифрования конечной гаммой на Julia

# 4 Выводы

В ходе выполнения лабораторной работы я изучил работу алгоритма шифрования гаммированием конечной гаммой, а также реализовал его программно.

# Список литературы

1. Лабораторная работа № 3. Шифрование гаммированием [Электронный ресурс]. Саратовский государственный университет имени Н.Г. Чернышевского, 2024.