Отчёт по лабораторной работе №3  
Математические основы защиты информации и информационной безопасности

Шифрование гаммированием

Выполнил: Махорин Иван Сергеевич,  
НФИмд-02-21, 1032259380

Содержание

# 1 Цель работы

Изучить шифрование гаммированием и научиться его реализовывать.

# 2 Выполнение лабораторной работы

## 2.1 Реализация шифрования гаммированием

Шифрование гаммированием (или шифр XOR) — это метод симметричного шифрования, при котором открытый текст посимвольно «складывается» с гаммой (ключом), состоящей из случайной последовательности, используя операцию сложения по модулю. Этот процесс выполняется как при шифровании, так и при расшифровке, обеспечивая теоретически абсолютную стойкость, если длина гаммы не меньше длины сообщения.

Выполним реализацию этого шифрования на языке Julia (рис. 1 - рис. 4):

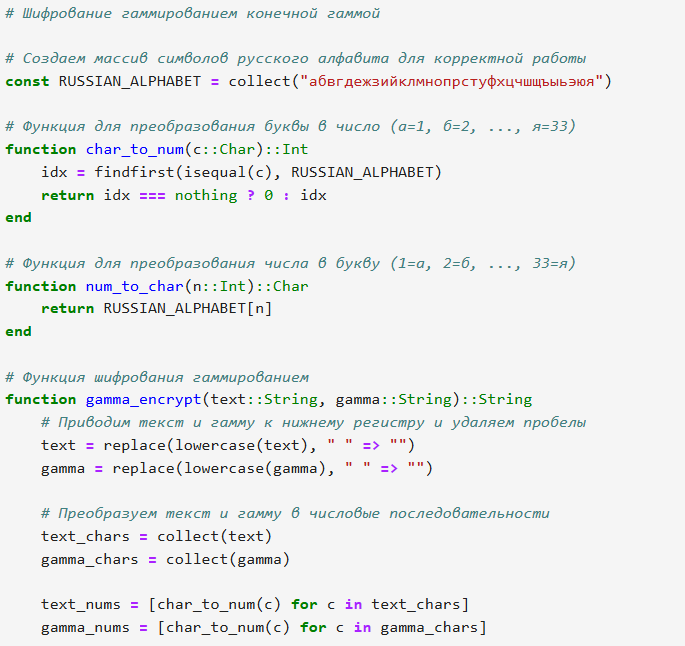


Рис. 1: Реализация шифрования гаммированием

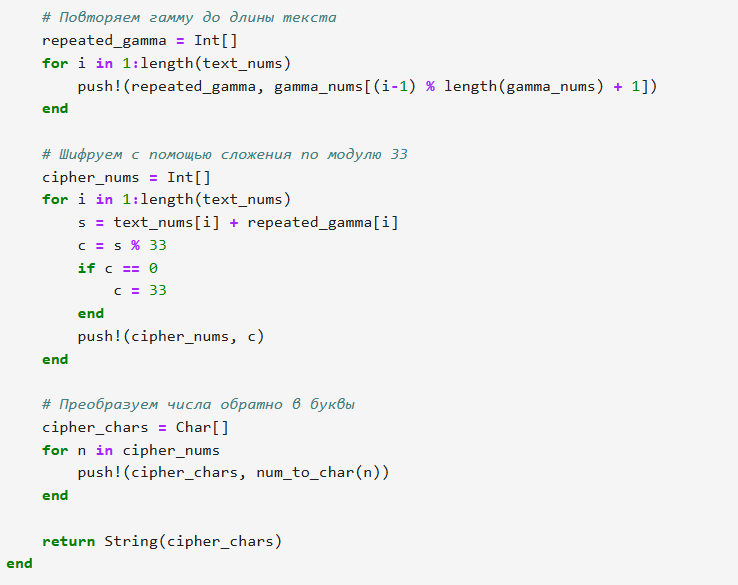


Рис. 2: Реализация шифрования гаммированием



Рис. 3: Реализация шифрования гаммированием

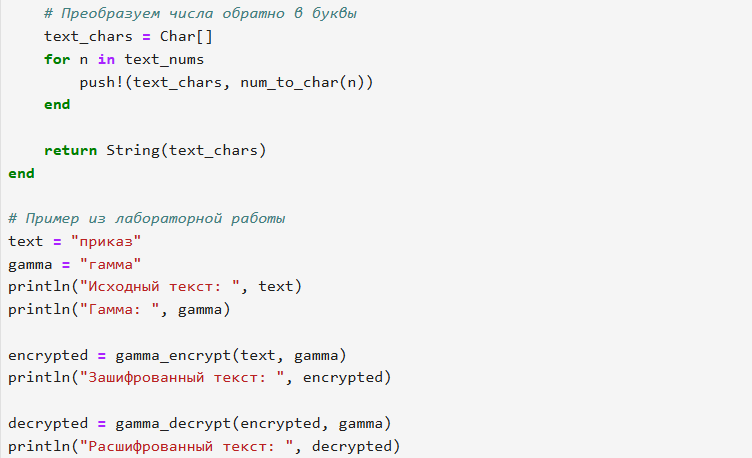


Рис. 4: Реализация шифрования гаммированием

Проверим работу шифрования гаммированием (рис. 5):

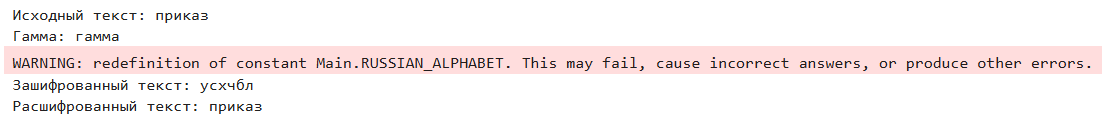


Рис. 5: Проверка

# 3 Список литературы. Библиография

[1] Julia: https://docs.julialang.org/en/v1/