Лабораторная работа 3

Шифрование гаммированием

Пологов Владислав Александрович

Содержание

# Цель работы

Реализовать алгоритм шифрования гаммированием конечной гаммой.

# Описание реализации

Для реализации алгоритмов использовались средства языка Python.

Были реализованы как шифратор, так и дешифратор реализуемого алгоритма. (рис. -fig. 1)

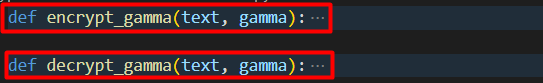


Figure 1: Функции шифратора и дешифратора

# Реализация

## Шифрование гаммированием

Гаммирование - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, то.е. псевдослучайной последовательности (ПСП) с выходов генератора G. Псевдослучайная последовательность является детерминированной, т.е. известен алгоритм её формирования. (рис. -fig. 2)

где — i-й член последовательности псведослучайных чисел, — ключевые параметры.

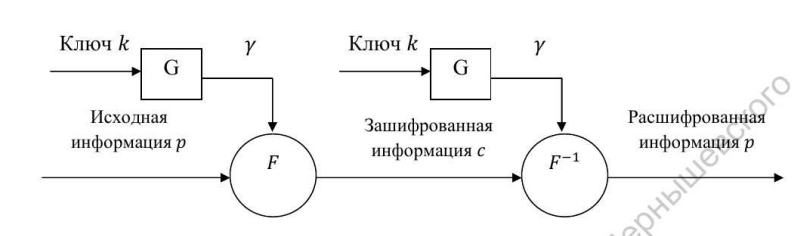


Figure 2: Гаммирование

## Условия достижения максимальной длины периода m

ПСП является периодической. Знание периода гаммы суещственно облегчает криптоанализ. Максимальная длина периода равна m. Для её достижения необходимо удовлетворить следующим условиям:

1. b и m - взаимно простые числа;
2. a - 1 делится на любой простой делитель числа m;
3. a - 1 кратно 4, если m кратно 4.

## Код реализации шифрования гаммированием

Для реализации были использованы функции получения алфавита и продления ключа до длины исходной строки из предыдущих лабораторных. (рис. -fig. 3)

## Код реализации шифрования гаммированием

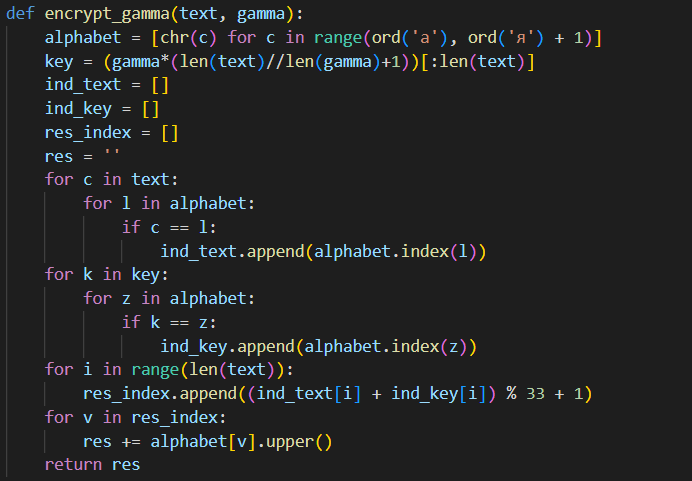


Figure 3: Код шифрования гаммированием

## Код дешифратора

Дешифрация отличается лишь формулой получения индекса элемента. (рис. -fig. 4)

## Код дешифратора

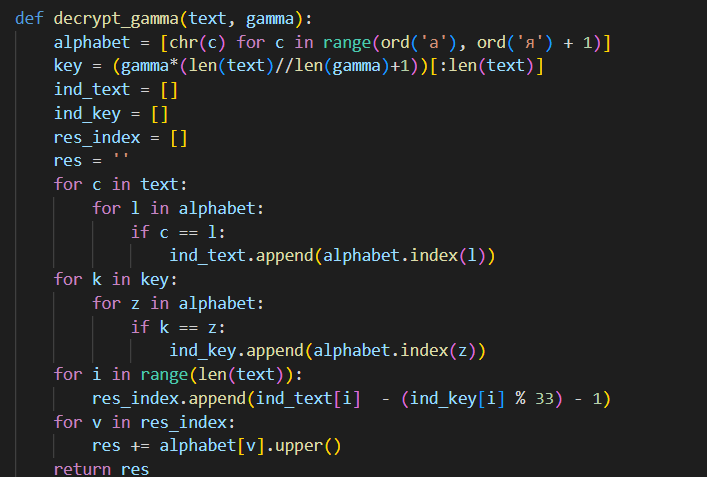


Figure 4: Код дешифратора

# Вывод

* Реализовали алгоритм шифрования гаммированием конечной гаммой.
* Узнали алгоритм формирования псевдослучайной последовательноати.