Лабораторная работа 3

Шифрование гаммированием

Греков Максим Сергеевич

Содержание

# Цель работы

* Ознакомиться с шифрованием гаммированием.
* Исследовать стойкость шифров, основанных на процедуре гаммирования.
* Реализовать алгоритм шифрования гаммированием конечной гаммой.

# Описание метода

**Гаммирование** – метод последовательного симметричного шифрования, суть которого состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой. (рис. 1)

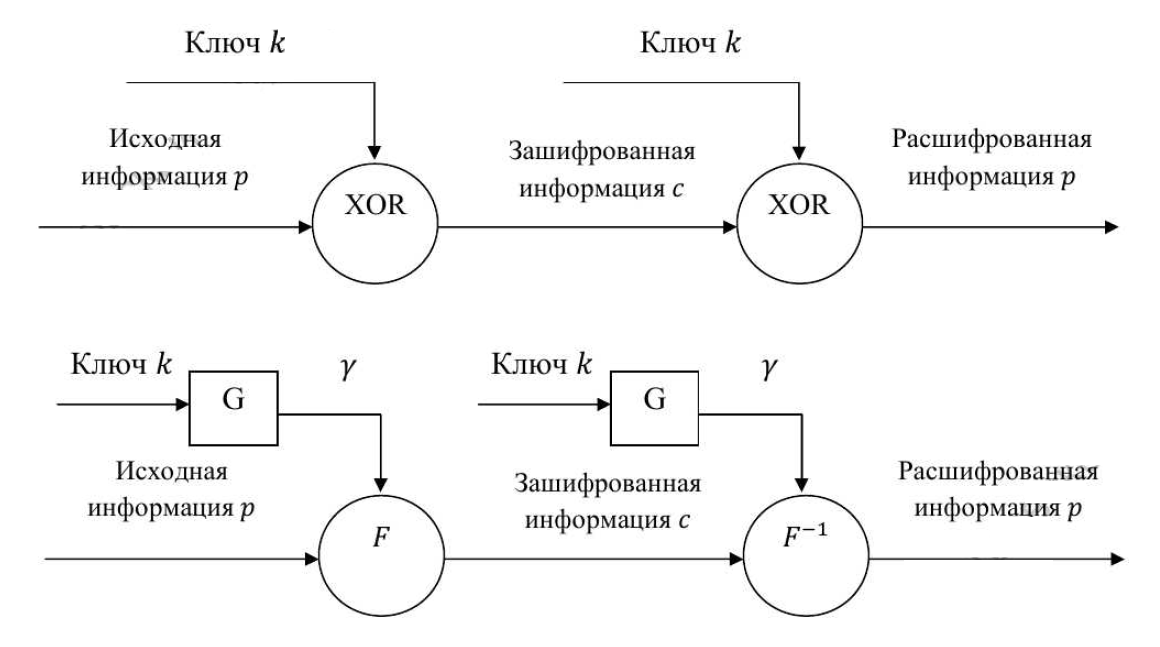


Figure 1: Гаммирование

## Стойкость

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.

## Пример шифрования

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). (рис. 2) Получаем:

Криптограмма: *«УСХЧБЛ» (« 20 18 22 24 02 12»)*.

# Реализация

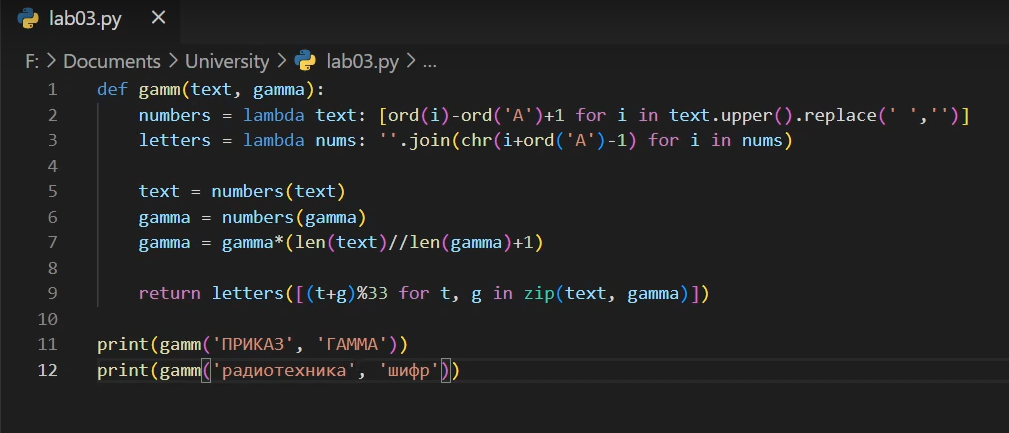


Figure 2: Реализация на Python

* Результат 1: *УСХЧБЛ*
* Результат 2: *ИЙЩЩЖЫЪЕЕСЯС*

# Вывод

* Ознакомились с шифрованием гаммированием.
* Исследовали стойкость шифров, основанных на процедуре гаммирования.
* Реализовали алгоритм шифрования гаммированием конечной гаммой.