Лабораторная работа №3

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования шифрование гаммированием конечной гаммой.

# 2 Теоретическое введение

**Гаммирование** - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, то есть псевдослучайной последовательности (ПСП) с выходов генератора G. ПСП по своим статистическим свойствам неотличима от случайной последовательности, но является детерминированной, то есть известен алгоритм ее формирования. Чаще всего в качестве функции F берется операция поразрядного сложения по модулю два или по модулю N (N - число букв алфавита открытого текста).

Простейший генератор ПСП можно представить рекуррентным соотношением:

где - i-й член последовательности псевдослучайных чисел, - ключевые параметры. Отметим, что ПСП является периодической.

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

Более подробно см. в [1].

# 3 Выполнение лабораторной работы

Списки word и gamma содержат шифруемое слово и гамму соответственно. Список alphabet заполняем буквами русского алфавита без “ё”. Далее сравниваем размерности word и gamma и если количество букв в word больше количества букв в gamma, то в список gamma\_new записываем подряд gamma столько раз, сколько оно целиком входит по количеству букв в word, а затем оставшуюся часть gamma, чтобы сравнять размерности. Если же количество букв в word меньше количества букв в gamma, то в gamma\_new из gamma записывается столько букв, сколько их содержится в word. Затем в списки number\_word и number\_gamma\_new записываем номера соответствующих букв из нашего алфавита. i-я буква зашифрованного слова получается по формуле: , поскольку в нашем алфавите без “ё” 32 буквы. Наконец, выводим результат на экран.

Код программы (рис. 1).



Рис. 1: Реализация шифрования гаммированием

# 4 Выводы

В ходе выполнения данной лабораторной работы было реализовано шифрование гаммированием конечной гаммой на языке программирования Python.

# Список литературы

1. Шифры гаммирования [Электронный ресурс]. URL: <https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema6>.