Отчёт по лабораторной работе №3

Шифрование Гаммированием

Студент: Гонсалес Ананина Луис Антонио, 1032175329

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 Цель работы

Цель данной лабораторной работы- изучить теорию и реализовать алгоритм шифрования гаммированием с конечной гаммой.

# 2 Теоретические сведения

Шифры гаммирования (аддитивные шифры) являются самыми эффективными с точки зрения стойкости и скорости преобразований. Для зашифрования и дешифрования используются элементарные арифметические операции – открытое/зашифрованное сообщение и гамма, представленные в числовом виде, складываются друг с другом по модулю (mod). Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например, 5+10 mod 4 = 15 mod 4 = 3).

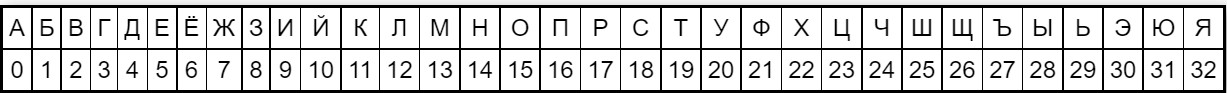
В шифрах гаммирования может использоваться сложение по модулю N (общий случай) и по модулю 2 (частный случай, ориентированный на программно-аппаратную реализацию).

Сложение по модулю N. В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы:

​ Ci = (Pi + Ki) mod N

​ Pi = (Ci + N - Ki) mod N

где Pi, Ci - i-ый символ открытого и шифрованного сообщения; N - количество символов в алфавите; Кi - i-ый символ гаммы (ключа).



Таблица

Например, для шифрования используется русский алфавит (N = 33), открытое сообщение – «АБРАМОВ», гамма – «ЖУРИХИН». При замене символов на числа буква А будет представлена как 0, Б – 1, …, Я – 32. Результат шифрования показан в следующей таблице [1].



Таблица2

# 3 Выполнение работы



Код



Код1



Код2

# 4 Выводы

В итоге в данной лабораторной работы я изучил теорию и реализовал алгоритм шифрования гаммированием с конечной гаммой.

# Список литературы

1. Шифры гаммирования [Электронный ресурс]. Википедия, 2021. URL: <https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema6>.