

# Лабораторная работа №3

Шифрование гаммированием

---

Баулин Егор Александрович, НФИмд-02-22

14 октября 2022

Российский университет дружбы народов, Москва, Россия

## Цели и задачи

---

Знакомство с шифрованием гаммированием на примере гаммирования конечной гаммой.

Реализовать алгоритм шифрования гаммированием конечной гаммой.

## Выполнение лабораторной работы

---

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле.

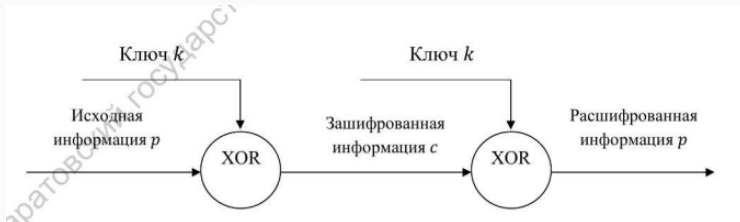


Figure 1: Схема однократного использования

## Полученные результаты

---



Введите сообщение: шифр

Введите ключ (гамма): шифр

Преобразование ШИФР -> ШИФР

Ваше сообщение:

ШИФР ([26, 10, 22, 18])

Ваша гамма:

ШИФР ([26, 10, 22, 18])

Зашифрованное сообщение:

СТЙВ ([19, 20, 11, 3])

## Выводы

---

Таким образом в процессе лабораторной работы изучено и реализовано шифрование гаммирования конечной гаммой.