# Элементы криптографии. Однократное гаммирование

Краснова Диана Владимировна

21 октября, 2023, Москва, Россия

## 1 Цели и задачи

### 1.1 Цель лабораторной работы

Изучение алгоритма шифрования гаммированием

## 2 Выполнение лабораторной работы

### 2.1 Гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

### 2.2 Гаммирование

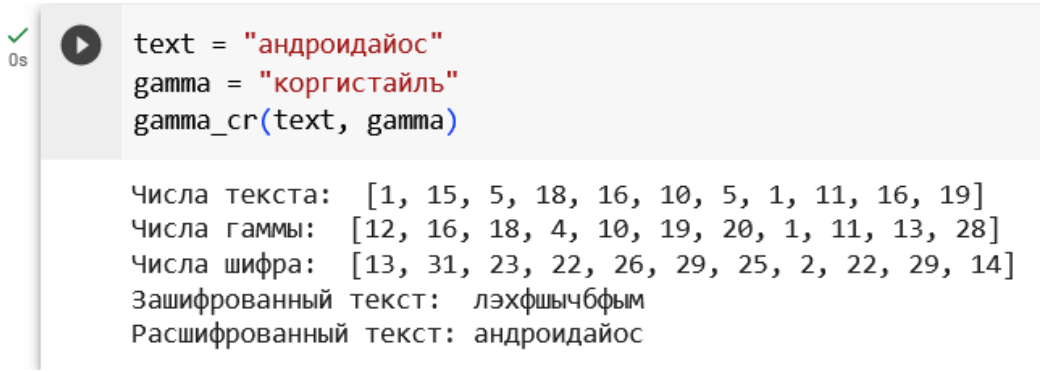
Наложение (или снятие) гаммы на блок сообщения в рассматриваемом нами стандарте реализуется с помощью операции побитного сложения по модулю 2 (XOR). То есть при шифровании сообщений каждый блок открытого сообщения ксорится с блоком криптографической гаммы, длина которого должна соответствовать длине блоков открытого сообщения. При этом, если размер блока исходного текста меньше, чем размер блока гаммы, блок гаммы обрезается до размера блока исходного текста (выполняется процедура усечения гаммы).

### 2.3 Формула

В аддитивных шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются. Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

$$Ci = (Ti + Gi) mod N$$

## 2.4 Пример работы программы



```
text = "андроидайос"
gamma = "коргистайль"
gamma_cr(text, gamma)
```

```
Числа текста:  [1, 15, 5, 18, 16, 10, 5, 1, 11, 16, 19]
Числа гаммы:  [12, 16, 18, 4, 10, 19, 20, 1, 11, 13, 28]
Числа шифра:  [13, 31, 23, 22, 26, 29, 25, 2, 22, 29, 14]
Зашифрованный текст:  лэхфшычбфым
Расшифрованный текст: андроидайос
```

*Работа алгоритма гаммирования*

# 3 Выводы

## 3.1 Результаты выполнения лабораторной работы

Изучили алгоритм шифрования с помощью гаммирования