**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

Факультет физико-математических и естественных наук

Кафедра информационных технологий

ОТЧЕТ по лабораторной работе 8

### ТЕМА «Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом»

**по дисциплине «Информационная безопасность»**

### Выполнил:

Студент группы НПИбд-02-21

Студенческий билет № 1032205421

Стeлина Петрити

# Список содержания

Список содержания.

Список изображений Цель работы.

*Последовательность выполнения работы*

Выводы

# Список изображений

рис. 1 Код для шифрования и дешифрования сообщений)

## Цель работы

Ознакомиться с практическим использованием метода одноразового шифрования с помощью гаммирования, закодировав несколько исходных текстов с использованием одного ключа.

## Последовательность выполнения работы

1. Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.Определить вид шифротекста при известном ключе и известном открытом тексте.

Задача состоит в том, чтобы разработать приложение, которое будет шифровать и дешифровать тексты с использованием однократного гаммирования, а затем попытаться прочитать тексты без знания ключа.



рис. 1 Код для шифрования и дешифрования сообщений

### Функция xorbytes:

Выполняет операцию XOR для каждого байта текста и ключа. Если текст длиннее ключа, ключ повторяется.

### Функция decryption:

Использует ту же операцию XOR для расшифровки сообщения с известным ключом.

### Шифрование:

Для двух исходных сообщений P1 и P2, шифротексты c1 и c2 вычисляются через XOR с ключом.

### Атака:

Вычисляется P1⊕P2, чтобы показать, как можно восстановить одно сообщение, если известно другое.

## Вывод

В ходе выполнения работы я приобрела практические навыки использования режима одноразового гаммирования с применением одного ключа для кодирования двух сообщений.