**Федеральное государственное автономное образовательное учреждение высшего образования**

**«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ»**

**(РУДН)**

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 № 1032205641

Сатлихана Петрити

(Подпись)

Москва 2024

# Список содержания

[Список содержания 2](#_Toc180324978)

[Список изображений 3](#_Toc180324979)

[Цель работы 4](#_Toc180324980)

[*Последовательность выполнения работы* 4](#_Toc180324981)

[Выводы 5](#_Toc180324982)

# Список изображений

[рис. 1 Код для шифрования и дешифрования сообщений с использованием однократного гаммирования (XOR) 4](#_Toc180324985)

Цель работы  
Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

*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.

Код:



рис. 1 Код для шифрования и дешифрования сообщений с использованием однократного гаммирования (XOR)

 Функция xor\_bytes:

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

 Функция decrypt:

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.

Выводы

В результате выполнения работы я освоила на практике применение режима однократного гаммирования при использовании одного ключа для двух сообщений.