

Лабораторная работа №7

Алибаева Данагуль ¹

2021 Moscow, Russia

¹RUDN University, Moscow, Russian Federation

Цель выполнения лабораторной работы

Освоить на практике применение режима однократного гаммирования.

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста

Результаты выполнения лабораторной работы

1. Успешное создание приложения.

```
from operator import xor
string = input("Open text: ")
key = input("Key: ")

def gamming(a,b):
    c = []
    for a,b in zip(a,b):
        c.append(chr(xor(ord(a), ord(b))))
    text = ''.join(c)
    return text

d = gamming(string, key)
print(" ")
print("Encrypted message: ", bytes(d, "UTF-8").hex())
```

Open text: с Новым годом, друзья!
Key: Желаю большого счастья

Encrypted message: 37d095260e7cd1ab0dd09e08727c000fd09200750773760e03d1ae

Figure 1: Разработка приложения

Освоила на практике применение режима однократного гаммирования.

Спасибо за внимание!