Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Афтаева К.В.

21 октября 2023

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Афтаева Ксения Васильевна
- студент группы НПИбд-01-20
- Российский университет дружбы народов им. Патриса Лумумбы
- 1032201739@pfur.ru
- https://github.com/KVAftaeva/study_2023-2024_infosec

Вводная часть

Актуальность

- Криптография – это важнейший инструмент кибербезопасности, она обеспечивает дополнительный уровень защиты, позволяет сохранить конфиденциальность данных и предотвращает их перехват киберпреступниками

Объект и предмет исследования

- Принцип однократного гаммирования

Цели и задачи

1. Изучить принцип однократного гаммирования
2. Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования

Материалы и методы

- Однократное гаммирование

Выполнение работы

Функция кодирования

```
def encrypt(text, gamma):
    textLen = len(text)
    gammaLen = len(gamma)

    keyText = []
    for i in range(textLen // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(textLen % gammaLen):
        keyText.append(gamma[i])

    code = []
    for i in range(textLen):
        code.append(alphabeth[(alphabeth.index(text[i]) + alphabeth.index(keyText[i])) % 73])

    return(print(*code,sep=''))
```

Функция декодирования

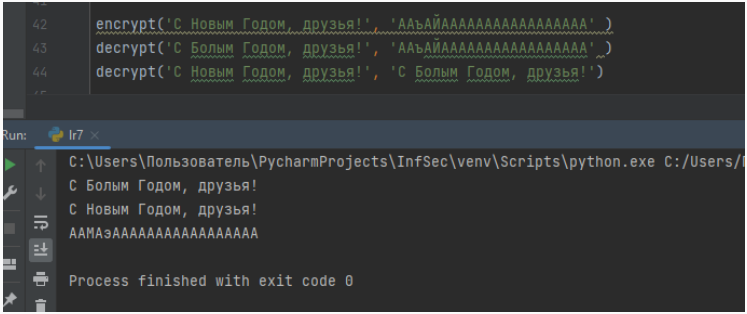
```
def decrypt(code, gamma):
    codeLen = len(code)
    gammaLen = len(gamma)

    keyText = []
    for i in range(codeLen // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(codeLen % gammaLen):
        keyText.append(gamma[i])

    text = []
    for i in range(codeLen):
        text.append(alphabeth[(alphabeth.index(code[i]) - alphabeth.index(keyText[i]) + 73) % 73])

    return(print(*text,sep=''))
```

Работа программы



Результаты

Результат

1. Изучен принцип однократного гаммирования
2. Разработано приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования

Вывод

Вывод

Я освоила на практике применение режима однократного гаммирования. Разработала приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.