Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Афтаева К.В.

25 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 для кодирования двух исходных текстов одним ключом
2. Разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования

Материалы и методы

- Однократное гаммирование

Выполнение работы

Функция кодирования

```python
def decrypt(text1, text2, gamma):
    text1Len = len(text1)
    text2Len = len(text2)
    gammaLen = len(gamma)

    keyText = []
    for i in range(text1Len // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(text1Len % gammaLen):
        keyText.append(gamma[i])

    code1 = []
    code2 = []

    for i in range(text1Len):
        code1.append(alphabeth[(alphabeth.index(text1[i]) + alphabeth.index(keyText[i])) % 71])

    for i in range(text2Len):
        code2.append(alphabeth[(alphabeth.index(text2[i]) + alphabeth.index(keyText[i])) % 71])

    return(print(*code1,sep=''),print(*code2,sep=''))
```

Функция декодирования

```
def decrypt2(code1, code2, text1):
    code1Len = len(code1)
    code2Len = len(code2)
    text1Len = len(text1)

    text2 = []

    for i in range(code1Len):
        text2.append(alphabeth[(alphabeth.index(code1[i]) - (alphabeth.index(code2[i]) - alphabeth.index(text1[i]))) % 71])

    return(print(*text2,sep=''))
```

Работа программы

```
decrypt('С Новым Годом, друзья!', 'С Левым Годом, друзья!', 'ААъАЙАААААААААААААААА')
print()
decrypt2('С Голым Годом, друзья!', 'С Белым Годом, друзья!', 'С Левым Годом, друзья!')
```

```
Run:  lr7
C:\Users\Пользователь\PycharmProjects\InfSec\venv\Scripts\python.exe C:/Users/Пользователь/PycharmProje
С Голым Годом, друзья!
С Белым Годом, друзья!

С Новым Годом, друзья!

Process finished with exit code 0
```

Результаты

Результат

1. Изучен принцип однократного гаммирования для кодирования двух исходных текстов одним ключом
2. Разработано приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования

Вывод

Вывод

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. Разработала приложение, ппозволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования.