Презентация №8

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

Аскеров А.Э.

22 мая 2024

Российский университет дружбы народов, Москва, Россия

Вступление

Цель работы

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

Выполнение лабораторной работы

Выполнение лабораторной работы

```python
def vzlom(P1, P2):
    code = []
    for i in range(20):
        code.append(alphabeth[(alphabeth.index(P1[i]) + alphabeth.index(P2[i]))  % len(alphabeth)])
    #получили известные символы в шаблоне
    print(code)
    print(code[16], " и ", code[19])
    p3 = "".join(code)
    print(p3)

vzlom(P1, P2)
```

```
[4]
['щ', 'С', 'З', 'в', 'э', 'ш', 'ю', 'Ж', 'ч', 'ш', '7', '4', 'р', 'й', 'щ', 'У', '1', 'Е', 'А', '4']
1  и  4
щСЗвэшюЖчш74рйщУ1ЕА4
```

Рис. 1: Работа алгоритма взлома ключа

Выполнение лабораторной работы

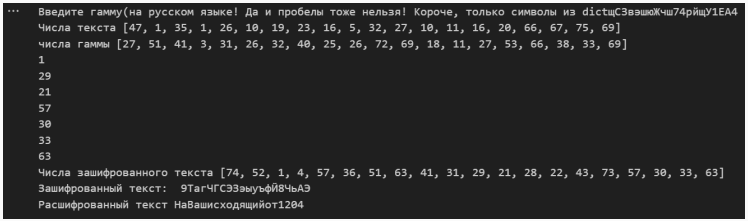

Рис. 2: Работа алгоритма шифрования и дешифровки

Заключение

Заключение

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.