

Презентация №8

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

Аскеров А.Э.

22 мая 2024

Российский университет дружбы народов, Москва, Россия

Вступление

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

Выполнение лабораторной работы

Выполнение лабораторной работы

```
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
щСЭвэшюЖчш74рйщУ1ЕА4
```

Рис. 1: Работа алгоритма взлома ключа

Выполнение лабораторной работы

```
... Введите гамму(на русском языке! Да и пробелы тоже нельзя! Короче, только символы из dictцСЭвэшоЖчш74рйщУ1ЕА4
Числа текста [47, 1, 35, 1, 26, 10, 19, 23, 16, 5, 32, 27, 10, 11, 16, 20, 66, 67, 75, 69]
числа гаммы [27, 51, 41, 3, 31, 26, 32, 40, 25, 26, 72, 69, 18, 11, 27, 53, 66, 38, 33, 69]
1
29
21
57
30
33
63
Числа зашифрованного текста [74, 52, 1, 4, 57, 36, 51, 63, 41, 31, 29, 21, 28, 22, 43, 73, 57, 30, 33, 63]
Зашифрованный текст: 9TagЧГСЭЗэуьфЙ8ЧьАЭ
Расшифрованный текст НаВашисходящийот1204
```

Рис. 2: Работа алгоритма шифрования и дешифровки

Заключение

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