Презентация по лабораторной работе №2

Дисциплина “Математические основы защиты информации и информационной безопасности”

Живцова А.А.

28 сентября 2024

Кафедра теории вероятностей и кибербезопасности, Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Живцова Анна Александровна
- студент кафедры теории вероятностей и кибербезопасности
- Российский университет дружбы народов имени Патриса Лумумбы
- zhivtsova_aa@pfur.ru
- https://github.com/AnnaZhiv

Вводная часть

Актуальность

Шифры перестановки служат примером традиционного симметричного шифрования. Хотя для многих таких шифров существуют методы взлома, изучение этих шифров улучшает понимание концепции симметричного шифрования, а реализация шифров на практике позволяет оценить вычислительную сложность.

Объект и предмет исследования

- Шифрование с помощью маршрутов
- Шифрование с помощью решеток
- Шифр Виженера

Цели и задачи

- Изучить концепцию шифров перестановки
- Реализовать шифрование с помощью маршрутов, шифрование с помощью решеток, и шифрование Виженера.

Материалы и методы

- Язык программирования Python

Результаты

Шифрование с помощью маршрутов

[3]:
```python
# маршрутное шифрование
def crypt1(n, m, text, password):
    min_char, max_char = ord(min(text)), ord(max(text))
    text = text.replace(' ', '')
    cripting_table = np.array(list(text)+[chr(np.random.randint(min_char, max_char)) for i in range(m*n-len(text))]).reshape(
    p = dict(zip(list(password), range(len(password))))
    return ''.join([''.join(cripting_table[:, p[i]]) for i in sorted(p)])
```

[4]:
```python
crypt1(6, 5, 'нельзя недооценивать противника', 'пароль')
```

[4]:
```
'еенпнзоатаьовокннеьвлдирияцтиа'
```

Рис. 1: Рабочий программный код. Шифрование с помощью маршрутов

Шифрование с помощью решеток

```
crypt2(2, 'договор подписали', 'шифр')
```

```
Числовой блок из 4 поворотов
 [[1 2 3 1]
 [3 4 4 2]
 [2 4 4 3]
 [1 3 2 1]]
Выбираем k различных чисел
 [[1. 0. 0. 0.]
 [1. 1. 0. 0.]
 [1. 0. 0. 0.]
 [0. 0. 0. 0.]]
записываем текст через решето, итерация  0
 [['д' '0' '0' '0']
 ['о' 'г' '0' '0']
 ['о' '0' '0' '0']
 ['0' '0' '0' '0']]
записываем текст через решето, итерация  1
 [['д' 'в' 'о' 'р']
 ['о' 'г' 'п' '0']
 ['о' '0' '0' '0']
 ['0' '0' '0' '0']]
записываем текст через решето, итерация  2
 [['д' 'в' 'о' 'р']
 ['о' 'г' 'п' 'о']
 ['о' '0' 'д' 'п']
 ['0' '0' '0' 'и']]
записываем текст через решето, итерация  3
 [['д' 'в' 'о' 'р']
 ['о' 'г' 'п' 'о']
 ['о' 'с' 'д' 'п']
 ['а' 'л' 'и' 'и']]

'вгслропиоплдпоа'
```

Шифр Виженера. Тип 1

```python
# шифр вижнера 1
al = 'a b c d e f g h i j k l m n o p q r s t u v w x y z'.split(' ')
def crypt3(text, password, n):
    min_char, max_char = ord(min(text)), ord(max(text))
    text = text.replace(' ', '')
    text = np.array(list(text)+[chr(np.random.randint(min_char, max_char))
                                for i in range(n*(len(text)//n+1*bool(n%len(text)))-len(text))]).reshape(-1, n)
    return ''.join(['',join([al[(ord(j)+ord(k))%len(al)]
                             for j in t]) for t, k in zip(text, password)])
```

```python
crypt3('how to check this code', 'passw', 5)
```

```
'ipxupotqowxlmwgshisg'
```

Рис. 3: Рабочий программный код. Шифр Виженера. Тип 1

Шифр Виженера. Тип 2

```python
# шифр вижнера 2
al = 'а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я'.split(' ')
def crypt4(text, password):
    password = [password[i%len(password)].lower() for i in range(len(text))]
    return ''.join([al[(al.index(i)+al.index(j))%len(al)] for i, j in zip(text.lower().replace(' ', ''), password)])
```

```python
crypt4('криптография серьезная наука', 'математика')
```

```
'цръфюохшкффягкььчпчалнтшца'
```

Рис. 4: Рабочий программный код. Шифр Виженера. Тип 2