# Презентация по лабораторной работе №1

Дисциплина “Математические основы защиты информации и информационной безопасности”

Живцова А.А.

05 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 простой замены (подстановки) являются наиболее простыми в реализации, поэтому хорошо подходят для начала изучения методов шифрования. Разбирая уязвимости шифров простой замены можно сформулировать идеи для их улучшениия, прослеживая эволюцию методов шифрования.

# Объект и предмет исследования

- Шифр простой замены подстановки
- Шифр Цезаря
- Шифр Атбаш

# Цели и задачи

- Изучить концепцию шифров простой замены
- Реализовать шифрацию и дешифрацию шифра Цезаря и шифра Атабаш

# Материалы и методы

- Язык программирования Python

# Результаты

# Шифр Цезаря и шифр Атбаш

```python
alphabet = 'а б в г д е ё 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(' ')
alphabet_atbash = 'а б в г д е ё 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(' ') + [' ']
alphabet_lat = '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(' ')
alphabet_atbash_lat = '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 cript(alphabet, k, string):
    return ''.join([alphabet[(alphabet.index(letter.lower()) + k + len(alphabet))%len(alphabet)] for letter in string])

print(cript(alphabet_lat, -3, 'YHQLYLGLYLFL'))
print(cript(alphabet_lat, 3, 'venividivici'))
print(cript(alphabet_atbash_lat, len(alphabet), 'YHQL YLGL YLFL'))
print(cript(alphabet_atbash_lat, len(alphabet), 'veni vidi vici'))
```

```
venividivici
yhqlylglylfl
dnwrfdrmrfdrlr
aktofaojofaoio
```

**Рис. 1:** Рабочий программный код. Шифрация и дешифрация шифра Цезаря и шифра Атабаш