Презентация по лабораторной работе №3

Дисциплина “Математические основы защиты информации и информационной безопасности”

Живцова А.А.

09 октября 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

Известно, что простейшей и наиболее надежной хемой шифрования является схема однократного использования. Однако в данной схеме длина ключа совпадает с длиной передаваемых данных, что затруднительно. Отсюда вытекает идея гаммирования.

Объект и предмет исследования

- Шифрование с помощью гаммирования конечной гаммой

Цели и задачи

- Изучить алгоритм шифрования гаммированием
- Реализовать шифрование с помощью конечной гаммы

Материалы и методы

- Язык программирования Python

Результаты

Результаты

```
def gamma(text, gamma, mod, al):
    return ''.join([al[(al.index(text[i]) + al.index(gamma[i%len(gamma)]))%mod] for i in range(len(text))])
```

```
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_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(' ')
gamma('приказ', 'гамма', 33, alphabet)
```

```
'трхчак'
```

Рис. 1: Рабочий программный код