Защита лабораторной работы №3

Шифрование гаммированием

Бармина Ольга

2024 September 7th

Российский университет дружбы народов, Москва, Россия

Цель выполнения лабораторной работы

- Освоение шифрования гаммированием
- Программная реализация алгоритма ширования гаммированием конечной гаммой

Теоретические сведения

Гаммирование - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, то есть псевдослучайной последовательности (ПСП) с выходом генератора G. Псевдослучайная последовательность по своим статистическим свойствам неотличима от случайной последовательности, но является детерминированной, то есть известен алгоритм ее формирования.

Результат выполнения лабораторной работы

Результат выполнения лабораторной работы

Алгоритм поиска зашифрованного текста на основе принципа формирования шифрования гаммирования:

```
def gen_key(m, pas):
    m = m.lower().replace(' ', '')
    pas = pas.lower().replace(' ', '')
    pas = list(pas)
    if len(m) == len(pas):
        return pas
    else:
        for i in range(len(m)-len(pas)):
            pas.append(pas[i%len(pas)])
    return pas
```

Figure 1: Генерация ключа

Результат выполнения лабораторной работы

Пример шифрования:

```python
def gamma(text, pas):
    alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'
    alphabet = list(alphabet)
    pas = gen_key(text, pas)
    text = list(text)

    res = ''
    for i in range(len(text)):
        c = (ord(text[i]) + ord(pas[i]) - 2*ord('a') + 2) % 31
        res += alphabet[c-1]
    return res
```

```python
gamma('приказ', 'гамма')
```

```
'усхчбл'
```

Figure 2: Реализация шифрования

Выводы

1. Изучили шифрование гаммированием
2. Реализовали алгоритм шифрования гаммированием конечной гаммой на языке Python