Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе №3

Шифрование гаммированием

Лубышева Ярослава Михайловна

Содержание

1 Цель работы **5**

2 Задание **6**

3 Выполнение лабораторной работы **7**

4 Выводы **9**

5 Список литературы **10**

List of Figures

3.1 Программная реализация алгоритма шифрования гаммированием конечной гаммой 7
3.2 Результаты работы алгоритма шифрования гаммированием конечной гаммой 8

List of Tables

1 Цель работы

Выполнить задание к лабораторной работе № 3 [1].

2 Задание

1) Изучить метод шифрования гаммированием.
2) Реализовать программно алгоритм шифрования гаммированием конечной гаммой.

3 Выполнение лабораторной работы

Для реализации алгоритма шифрования гаммированием конечной гаммой была написана программа на языке программирования Python (fig. 3.1).

```python
# алфавит
alphabet = ['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']
```

```python
# Алгоритм шифрования гаммированием конечной гаммой
# gamma - гамма-шифр
# mes - сообщение для шифрования
# modul - модуль (mod) для операции побитового сложения
def gamma_encryption(gamma, mes, modul):
  mes = list(mes.lower())
  gamma = list(gamma.lower())

  # сделаем, чтобы гамма-шифр gamma дублировался на всю длину сообщения mes
  gamma *= len(mes)//len(gamma) + 1
  gamma = gamma[:len(mes)]

  cryptogram = ""

  for let_gamma, let_mes in zip(gamma, mes):
    # если обе буквы находятся в алфавите
    if let_gamma in alphabet and let_mes in alphabet:
      # находим индекс каждой и вычисляем индекс буквы криптограммы по формуле
      ind_let_gamma = alphabet.index(let_gamma)
      ind_let_mes = alphabet.index(let_mes)
      ind_let_crypt = (ind_let_mes+1 + ind_let_gamma+1) % modul - 1
      # запоминаем букву
      cryptogram += ''.join(alphabet[ind_let_crypt])

  print("Криптограмма: ", cryptogram)
```

Figure 3.1: Программная реализация алгоритма шифрования гаммированием конечной гаммой

Результаты работы алгоритма представлены на рисунке ниже (fig. 3.2).

```
gamma = "ГАММА"
mes = "ПРИКАЗ"
modul = 33
gamma_encryption(gamma, mes, modul)
```

```
Криптограмма:  усхчбл
```

Figure 3.2: Результаты работы алгоритма шифрования гаммированием конечной гаммой

4 Выводы

Выполнено задание к лабораторной работе № 3.

5 Список литературы

1. Методические материалы курса