

Отчёт по лабораторной работе №3

Аветисян Давид Артурович

12 октября 2024

РУДН, Москва, Россия

Отчет по лабораторной работы №3

- Познакомиться с шифрованием гаммированием.

Запрос текста и пароля у пользователя

- Я решил реализовать шифрование гаммированием на языке Python. Сначала я задал матрицу с русскими буквами, а также реализовал запрос текста и пароля у пользователя. Все буквы в тексте и пароля я сделал заглавными, а затем я отфильтровал текст и пароль, оставив в нём только русские буквы.

```
lab03.py > ...
1  russian_letters = [chr(i) for i in range(ord('А'), ord('Я') + 1)]
2
3  def xor_cipher(text, password):
4      return
5
6  text = input('Введите текст: ').upper()
7  filter_text = ''.join(char for char in text if char in russian_letters)
8  password = input('Введите пароль: ').upper()
9  filter_password = ''.join(char for char in password if char in russian_letters)
10 if len(filter_text) >= len(filter_password):
11     encrypted_xor = xor_cipher(filter_text, filter_password)
12     print("Криптограмма:", encrypted_xor)
```

Рис. 1: Запрос текста и пароля у пользователя

Шифрование гаммированием на языке Python

- Далее я реализовал само шифрование гаммированием. Я задал три матрицы: для текста, для гаммы и для результата. Пароль я увеличил повторением до длины текста, как указано в теории к лабораторной работе №3. Далее я, опираясь на матрицу с русскими буквами, заполнил первые две матрицы значениями, на которых стоят буквы из текста и пароля соответственно. А уже затем я заполнял третью матрицу складывая значения из первой и второй матрицы и находя остаток от деления. После чего я преобразовал каждое значение из третьей матрицы в букву, исходя из матрицы с русскими буквами, и вывел пользователю.

```
lab03.py > ...
1  russian_letters = [chr(i) for i in range(ord('А'), ord('Я') + 1)]
2
3  def xor_cipher(text, password):
4      data = []
5      for char in text:
6          data.append(russian_letters.index(char))
7      key = []
8      repeated_password = (password * (len(text) // len(password) + 1))[:len(text)]
9      for char in repeated_password:
10         key.append(russian_letters.index(char))
11     cryptogram = []
12     for i in range(len(text)):
```

Проверка метода шифрования гаммированием

- Далее я запустил два теста через командную строку. Один тест как в теории к лабораторной работе №3. Второй тест для дополнительной проверки. Шифрование совпало с тестом в лабораторной работе №3, и реализовано верно.

```
C:\Users\yaeda\OneDrive\Рабочий стол\RUDN\Магистратура\МО3ИИБ>py lab03.py
Введите текст: приказ
Введите пароль: гамма
Криптограмма: УСХЧБЛ

C:\Users\yaeda\OneDrive\Рабочий стол\RUDN\Магистратура\МО3ИИБ>py lab03.py
Введите текст: я хочу играть в доту
Введите пароль: с мужиками
Криптограмма: СВВЮЬУДЭЙДЦЛЧЭФ
```

Рис. 3: Проверка метода шифрования гаммированием

- Я реализовал шифрование гаммированием.