Лабораторная работа №2

Математические основы защиты информации и информационной безопасности

Назарьин Артем Игоревич

Содержание

List of Figures

1 Цель работы

Реализовать шифрование перестановками, шифрование с помощью решеток и таблицы Виженера.

2 Выполнение лабораторной работы

2.1 Выполнение задания

Реализую маршрутное шифрование перестановками (рис. -fig. 2.1 , -fig. 2.2)

```python
#столбцовая перестановка
def stolb_encryption(input_text, key):
    #Удаляем символы-разделители из ключа и переводим его в список символов
    key = [c for c in key if c.isalpha()]
    #Удаляем все символы-разделители из исходного текста
    input_text = ''.join([c for c in input_text if c.isalpha()])
    #Определяем количество столбцов на основе длины ключа
    num_columns = len(key)
    #Вычисляем количество строк в таблице с зашифрованным текстом
    num_rows = len(input_text) // num_columns
    if len(input_text) % num_columns != 0:
        num_rows += 1

    #Заполняем таблицу с шифротекстом пустыми символами
    table = [[''] * num_columns for _ in range(num_rows)]

    #Заполняем таблицу с исходным текстом по столбцам
    index = 0
    for col in range(num_columns):
        for row in range(num_rows):
            if index < len(input_text):
                table[row][col] = input_text[index]
                index += 1

    #Создаем список, содержащий индексы столбцов после перестановки
    column_order = [key.index(c) for c in sorted(key)]
```

Figure 2.1: Маршрутное шифрование, часть 1

```python
    #Создаем список, содержащий индексы столбцов после перестановки
    column_order = [key.index(c) for c in sorted(key)]

    #Шифруем текст, объединяя символы в каждом столбце в порядке перестановки столбцов
    ciphertext = ''
    for col in column_order:
        for row in range(num_rows):
            ciphertext += table[row][col]

    return ciphertext

input_text = 'this message is secret'
key = 'super'
ciphertext = stolb_encryption(input_text, key)
print(ciphertext)
```

```
ssecageiretthismess
```

Figure 2.2: Маршрутное шифрование, часть 2

Реализую шифрование с помощью таблицы Виженера. (рис. -fig. 2.3 , -fig. 2.4)

Исходный текст: криптография серьезная наука; пароль – математика. Итоговый результат частично не совпал с примером из задания, поскольку в задании была представлена таблица с неполным алфавитом.

```
[ ] #Таблица Виженера
    #шифрование
    def vigenere_encrypt(input_text, key):
        #Преобразуем текст и ключ в верхний регистр
        input_text = input_text.upper()
        key = key.upper()

        #Создаем шифрованный текст
        ciphertext = ''
        for i in range(len(input_text)):
            char = input_text[i]
            if char.isalpha():
                #вычисляем смещение для текущего символа
                shift = ord(key[i % len(key)]) - ord('A')
                #шифруем символ
                encrypted_char = chr((ord(char) - ord('A') + shift) % 32 + ord('A'))
                ciphertext += encrypted_char
            else:
                ciphertext += char

        return ciphertext
```

Figure 2.3: Шифрование с помощью таблицы Виженера, часть 1

```
    #дешифрование
    def vigenere_decrypt(ciphertext, key):
        #Преобразуем текст и ключ в верхний регистр
        ciphertext = ciphertext.upper()
        key = key.upper()

        #Создаем дешифрованный текст
        input_text = ""
        for i in range(len(ciphertext)):
            char = ciphertext[i]
            if char.isalpha():
                #Вычисляем смещение для текущего символа
                shift = ord(key[i % len(key)]) - ord('A')
                #Расшифровываем символ
                decrypted_char = chr((ord(char) - ord('A') - shift) % 32 + ord('A'))
                input_text += decrypted_char
            else:
                input_text += char

        return input_text
```

```
[ ] input_text = 'криптография серьезная наука'
    key = 'математика'

    ciphertext = vigenere_encrypt(input_text, key)
    print('Зашифрованный текст:', ciphertext)

    decrypted_text = vigenere_decrypt(ciphertext, key)
    print('Расшифрованный текст:', decrypted_text)

    Зашифрованный текст: ЦРЪФЮОХШКФФЯ ЦСРОНСНМЯ ТМУЬИ
    Расшифрованный текст: КРИПТОГРАФИЯ СЕРЬЕЗНАЯ НАУКА
```

Figure 2.4: Шифрование с помощью таблицы Виженера, часть 2

3 Выводы

Я реализовал шифрование перестановками и шифрование с помощью таблицы Виженера.