Лабораторная работа №2

Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна

26 сентября 2023

Российский университет дружбы народов, Москва, Россия

НПМмд-02-23

Шифры перестановки

Цель лабораторной работы

Изучить шифры перестановки.

Задачи лабораторной работы

1. Реализовать маршрутное шифрование.
2. Реализовать шифрование с помощью решёток.
3. Реализовать шифрование таблицей Виженера.

Ход лабораторной работы

Маршрутное шифрование

Реализуем маршрутное шифрование.

Маршрутное шифрование

```
# ввод данных
message = input("Введите сообщение: ").replace(' ', '')
password = input("Введите пароль: ")
m = len(message)
n = len(password)
message += ((m % n)*n - m) * message[-1]
main_table = list()

#формирование таблицы
for i in range(m % n):
    main_table.append(list(message[(i*n): ((i+1)*n)]))

# Выбор порядка столбцов
sort_password = sorted(list(password))
list_index = list()
for i in sort_password:
    list_index.append(password.find(i))

# Шифрование сообщения
coded_message = ''
for i in list_index:
    for j in range(len(main_table)):
        coded_message += main_table[j][i]
print("Зашифрованное сообщение:", coded_message)
```

Шифрование с помощью решёток

Реализуем шифрование с помощью решёток.

```
# ввод данных
k = int(input('Введите число k: '))
message = input("Введите сообщение: ").replace(' ', '')
password = input("Введите пароль длины k^2 без повторяющихся букв: ")
m = len(message)
message += (k**2 - m) * message[-1]

#формирование решётки
l = np.arange(k**2).reshape(k, k) + 1
table = np.hstack([np.vstack([l, np.rot90(l)]), np.vstack([np.rot90(l, k=3), np.rot90(l, k=2)])])
for i in range(k**2):
    r_index = np.random.randint(4)
    a = np.where(table == (i+1))[0][r_index]
    b = np.where(table == (i+1))[1][r_index]
    table[a][b] = 0

table1 = table; table2 = np.rot90(table, k=3); table3 = np.rot90(table, k=2); table4 = np.rot90(table)
index_1 = np.where(table1 == 0); index_2 = np.where(table2 == 0); index_3 = np.where(table3 == 0);
index_4 = np.where(table4 == 0)
index = np.hstack([index_1, index_2, index_3, index_4])
coded_table = np.empty((2*k, 2*k), dtype="object")

# Шифрование сообщения
for i in range(4):
    for j in range(k**2):
        coded_table[index[0][(k**2)*i + j]][index[1][(k**2)*i + j]] = message[(k**2)*i + j]
sort_password = sorted(list(password))
list_index = list()
for i in sort_password:
    list_index.append(password.find(i))
coded_message = ''
for i in list_index:
    for j in range(len(coded_table)):
        coded_message += coded_table[j][i]
print("Зашифрованное сообщение:", coded_message)
```

Таблица Виженера

Реализуем шифрование таблицей Виженера.

Таблица Виженера

```
# ввод данных
alpha = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя'
message = input("Введите сообщение: ").replace(' ', '')
password = input("Введите пароль: ")

#уравнивание пароля с сообщением
i = 0
while len(message) != len(password):
    password += password[i]
    i += 1

# Шифрование сообщения
coded_message = ''
for i in range(m):
    ch1 = message[i]
    ch2 = password[i]
    ch3 = alpha[(alpha.index(ch1) + alpha.index(ch2)) % n]
    coded_message += ch3
print("Зашифрованное сообщение:",coded_message)
```

Выводы

Изучила шифры перестановки на примере маршрутного шифрования, шифрования с помощью решёток и шифрования таблицей Виженера.