Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Губина О. В.

28 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Губина Ольга Вячеславовна
- студент(-ка) уч. группы НПИбд-01-20
- Российский университет дружбы народов
- 1032201737@pfur.ru
- https://github.com/ovgubina

Вводная часть

Актуальность

- Необходимость знания шифрования на проктике для обеспечения информационной безопасности.

Объект и предмет исследования

- Симметричное шифрование, гаммирование.

Цели и задачи

- Освоить на практике применение режима однократного гаммирования.
- Написать программу осуществляющую шифровние.

Материалы и методы

- Язык программирования Python

Процесс выполнения работы

Создание сообщениий для кодирования и ключа

```
import string # импортируем библиотеки для работы
import random

# задаем сообщения, которые мы хотим закодировать
message_1 = "Хочу плакать(" # P1
message_2 = "Божи поможи((" # P2

key = '' # ключ K пока неизвестен, т.к не подобран

# создаем ключ для кодирования обоих сообщений
for i in range(len(message_1)):
  key = key + random.choice(string.ascii_letters + string.digits)
print("Ключ:", key)
```

Функция кодирования

```
# функция кодирования/декодирования текста по ключу
def encryption(text, key):
  en_text = ''
  for i in range(len(key)):
    en_text_symbol_xor = ord(text[i]) ^ ord(key[i])
    en_text = en_text + chr(en_text_symbol_xor)
  return en_text
```

Шифрование сообщений

```
# кодируем сообщения в соответствие с ключом
encrypted_message_1 = encryption(message_1, key) # C1
encrypted_message_2 = encryption(message_2, key) # C2

print("Зашифрованные тексты:", encrypted_message_1, ",", encrypted_message_2)
```

Дешифрование текста

```
# декодируем зашифрованные ранее сообщения
decrypted_message_1 = encryption(encrypted_message_1, key)
decrypted_message_2 = encryption(encrypted_message_2, key)

print("Первое расшифрованное сообщение: ", decrypted_message_1)
print("Второе расшифрованное сообщение: ", decrypted_message_2)
```

```
Ключ: 3oPUlieI2nVsb
Зашифрованные тексты: ЖёЭЖLiўщJўДпJ , ТёA№Liћv Ќj3[J
Первое расшифрованное сообщение:  Хочу плакать(
Второе расшифрованное сообщение:  Божи поможи((
```

Дешифрование без ключа

```
# не знаем ключ

new_key = encryption(encrypted_message_1, encrypted_message_2)
print("Текст для расшифровки:", new_key)

print("Расшифрованный текст 1:", encryption(new_key, message_2))
print("Расшифрованный текст 2:", encryption(new_key, message_1))
```

```
Текст для расшифровки: 4q{zЖ
Расшифрованный текст 1: Хочу плакать(
Расшифрованный текст 2: Божи поможи((
```

Результаты работы

Результаты работы

- Написала программу программу осуществляющую кодирование двух текстов одним ключом (однократное гаммирование).

Вывод

Вывод

Освоила на практике применение режима однократного гаммирования для двух текстов при использовании одного ключа.