Отчёт по лабораторной работе

Лабораторная работа №_08 / Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Габриэль Тьерри

Содержание

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Задание

Два текста кодируются одним ключом (однократное гаммирование).
Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Выполнение лабораторной работы

Определил функцию шифрования и дешифрования

```python
import random
from random import seed
import string

# Функция шифрования
def encryption_function(text, key):
    # Проверка, что ключ и текст имеют одинаковую длину
    if len(key) != len(text):
        return "Same length required for text and key"
    encrypted_result = ""  # Инициализация результата шифрования
    for i in range(len(key)):
        # Побитовая операция XOR между символами текста и ключа
        encrypted_result_symbol = ord(text[i]) ^ ord(key[i])
        encrypted_result += chr(encrypted_result_symbol) # Добавление символа к результату
    return encrypted_result
```

генерируем ключ

```
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"

key = ""
seed(23) # Установка случайного зерна для воспроизводимости
for i in range(len(P1)):
    key+=random.choice(string.ascii_letters + string.digits) # Генерация случайного ключа
print(key) # Вывод сгенерированного ключа
```

```
7X8s51fbLtByHwiUmrCa
```

Вызов зашифрованные сообщения

```
# Зашифровать сообщения P1 и P2 с использованием ключа
encryption_P1 = encryption_function(P1, key)
encryption_P2 = encryption_function(P2, key)

# Вывести зашифрованные сообщения
print(f"Encrypted text message P1: {encryption_P1}")
print(f"Encrypted text message P2: {encryption_P2}")
```

```
Encrypted text message P1: ъЫьуЎЬЧЧѲрЙаѰюї3\@sU
Encrypted text message P2: ХѫЙсЀѱЋЩvaОтѰЧђфЙяѫё
```

Пример обратного шифрования

```
# Расшифровать зашифрованные сообщения, используя те же функции (для демонстрации)
print(f"P1: {encryption_function(encryption_P1, key)}")
print(f"key: {encryption_function(P1, encryption_P1)}")
print(f"P2: {encryption_function(encryption_P2, key)}")
print(f"key: {encryption_function(P2, encryption_P2)}")
```

```
P1: НаВашисходящийот1204
key: 7X8s51fbLtByHwiUmrCa
P2: ВСеверныйфилиалБанка
key: 7X8s51fbLtByHwiUmrCa
```

Выводы

Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.