Презентация по лабораторной работе № 8

Информационная безопасность

Адебайо Р. А.

27.10.2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Адебайо Ридвануллахи Айофе
- студент группы НКНбд-01-20
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов
- Страничка на GitHub
- Страничка на LinkedIn

Цель лабораторной работы

Цель лабораторной 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.

Порядок выполнения работы(1)

Определить функцию шифрования и дешифрования

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

```python
def cipher_text_function(text, key):
    #condition to check if the key and text have the same length
    if len(key) != len(text):
        return "Key and text must have the same length"
    cipher_text = ""
    for i in range (len(key)):
        cipher_text_symbol=ord(text[i]) ^ ord(key[i])
        cipher_text+=chr(cipher_text_symbol)
    return cipher_text
```


Рис. 1: Функция шифрования

Порядок выполнения работы(2)

Определить вид шифротексты и ключа

In [4]:
```
P1="НаВашисходящийот1204"
P2="ВСеверныйфилиалБанка"
```

In [5]:
```
key=""
seed(23)
for i in range(len(P1)):
    key += random.choice(string.ascii_letters + string.digits)
print(key)
```

```
7X8s51fbLtByHwiUmrCa
```

Рис. 2: создание ключа той же длины, что и открытый текст

Вызов функции шифрования.

In [6]:

```
1 cipher_P1 = cipher_text_function(P1, key)
2 cipher_P2 = cipher_text_function(P2, key)
3 print(f"Encoded P1: {cipher_P1}")
4 print(f"Encoded P2: {cipher_P2}")
5
```

```
Encoded P1: ЬЩЬуѿЉЧЧѲрЙаΨюї3\@sU
Encoded P2: Х◊ЙісЄѱЋЩvaѺтΨчЋфЙя◊ё
```

Рис. 3: получение шифротекста

Пример обратного шифрования

```
n [7]:
1 print(f"P1: {cipher_text_function(cipher_P1, key)}")

P1: НаВашисходящийот1204

n [8]:
1 print(f"Key: {cipher_text_function(P1, cipher_P1)}")

Key: 7X8s51fbLtByHwiUmrCa

[10]:
1 print(f"P2: {cipher_text_function(cipher_P2, key)}")
2 print(f"Key: {cipher_text_function(P2, cipher_P2)}")

P2: ВСеверныйфилиалБанка
Key: 7X8s51fbLtByHwiUmrCa
```


Рис. 4: обратный шифрование

Вывод

Вывод

В ходе выполнения данной лабораторной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.