Отчет по лабораторной работе №8

Дисциплина: Основы информационной безопасности

Иванов Сергей Владимирович

Содержание

Список иллюстраций

1 Цель работы

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

2 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 P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

3 Выполнение лабораторной работы

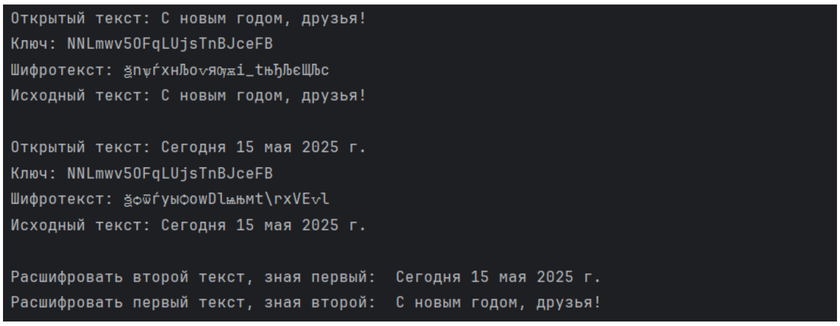
Я выполнял работу на языке программирования Python, используя функции, реализованные в лабораторной работе №7.

Используя функцию для генерации ключа, генерирую ключ, затем шифрую два разных текста одним и тем же ключом (рис. 1).

```python
text1 = 'С новым годом, друзья!'
text2 = 'Сегодня 15 мая 2025 г.'

key = generate_key(text1)
en_crypt = en_de_crypt(text1, key)
de_crypt = en_de_crypt(en_crypt, key)

en_crypt_text2 = en_de_crypt(text2, key)
de_crypt_text2 = en_de_crypt(en_crypt_text2, key)

print("Открытый текст:", text1, "\nКлюч:", key, "\nШифротекст:", en_crypt, "\nИсходный текст:", de_crypt, "\n")
print("Открытый текст:", text2, "\nКлюч:", key, "\nШифротекст:", en_crypt_text2, "\nИсходный текст:", de_crypt_text2, "\n")

r = en_de_crypt(en_crypt_text2, en_crypt)
print('Расшифровать второй текст, зная первый: ', en_de_crypt(text1, r))
print('Расшифровать первый текст, зная второй: ', en_de_crypt(text2, r))
```

Рис. 3.1: Шифрование двух текстов

Расшифровываю оба текста сначала с помощью одного ключа, затем предполагаю, что мне неизвестен ключ, но извествен один из текстов и уже расшифровываю второй, зная шифротексты и первый текст (рис. 2).



```
Открытый текст: С новым годом, друзья!
Ключ: NNLmwv5OFqLUjsTnBJceFB
Шифротекст: ѯnψѓxнЉovяѹѫi_tћЂЉєЩЉc
Исходный текст: С новым годом, друзья!

Открытый текст: Сегодня 15 мая 2025 г.
Ключ: NNLmwv5OFqLUjsTnBJceFB
Шифротекст: ѯѻѿѓyыѻowDlѩњмt\rxVEѵl
Исходный текст: Сегодня 15 мая 2025 г.

Расшифровать второй текст, зная первый:  Сегодня 15 мая 2025 г.
Расшифровать первый текст, зная второй:  С новым годом, друзья!
```

Рис. 3.2: Результат работы программы

Листинг программы 1

```
import random
import string

# генерация ключа
def generate_key(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key

# шифрование и дешифрование текста
def en_de_crypt(text, key):
    new_text = ''
    for i in range(len(text)):
        new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
    return new_text

# функция для нахождения возможных ключей
def find_keys(text, fragment):
    possible_keys = []
    for i in range(len(text) - len(fragment) + 1):
        possible_key = ''
        for j in range(len(fragment)):
            possible_key += chr(ord(text[i + j]) ^ ord(fragment[j]))
        possible_keys.append(possible_key)
    return possible_keys
```

```
text1 = 'С новым годом, друзья!'
text2 = 'Сегодня 15 мая 2025 г.'

key = generate_key(text1)
en_crypt = en_de_crypt(text1, key)
de_crypt = en_de_crypt(en_crypt, key)

en_crypt_text2 = en_de_crypt(text2, key)
de_crypt_text2 = en_de_crypt(en_crypt_text2, key)

print("Открытый текст:", text1, "\nКлюч:", key, "\nШифротекст:", en_crypt, "\nИсх
print("Открытый текст:", text2, "\nКлюч:", key, "\nШифротекст:", en_crypt_text2,

r = en_de_crypt(en_crypt_text2, en_crypt)
print('Расшифровать второй текст, зная первый: ', en_de_crypt(text1, r))
print('Расшифровать первый текст, зная второй: ', en_de_crypt(text2, r))
```

4 Ответы на контрольные вопросы

1. Как, зная один из текстов (P_1 или P_2), определить другой, не зная при этом ключа? - Для определения другого текста (P_2) можно просто взять зашифрованные тексты $C_1 \oplus C_2$, далее применить XOR к ним и к известному тексту: $C_1 \oplus C_2 \oplus P_1 = P_2$.

2. Что будет при повторном использовании ключа при шифровании текста? - При повторном использовании ключа мы получим дешифрованный текст.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? - Режим шифрования однократного гаммирования одним ключом двух открытых текстов осуществляется путем XOR-ирования каждого бита первого текста с соответствующим битом ключа или второго текста.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов - Недостатки шифрования одним ключом двух открытых текстов включают возможность раскрытия ключа или текстов при известном открытом тексте.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов - Преимущества шифрования одним ключом двух открытых текстов включают использование одного ключа для зашифрования нескольких сообщений без необходимости создания нового ключа и выделения на него памяти.

5 Выводы

В ходе лабораторной работы были освоины на практике навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.