

Отчёт по лабораторной работе №8

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Контрольные вопросы	9
4	Выводы	10
	Список литературы	11

Список иллюстраций

2.1 Вывод программы	8
-------------------------------	---

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом [1].

2 Выполнение лабораторной работы

Постановка задания: два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочесть оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочесть оба текста, не зная ключа и не стремясь его определить.

Создаем функцию, генерирующую ключ из ascii-символов и цифр, и функцию, кодирующую исходный текст по ключу. На вход функция принимает текст и ключ. Переводит ключ в 16-ричную ИС, далее использует XOR, переводит из 16-ричной ИС. Возвращает шифротекст.

```
import random
import string

def generate_key(length: int):
    return random.sample(string.ascii_letters + string.digits, length)

def encrypt(text: str, key: list = None):
    if not key:
```

```

    key = generate_key(length=len(text))

text_16 = [ord(char) for char in text]
key = [ord(el) for el in key]

print(f"Ключ шифрования:", ' '.join(str(s) for s in key))
print(f"Исходный текст:", text)

encrypted_text = []
for i in range(len(text)):
    encrypted_text.append(text_16[i] ^ key[i])

ciphertext = ''.join([chr(i) for i in encrypted_text])
print(f'Шифротекст: {ciphertext}\n\n')

return ciphertext

```

Задаем два текста. Генерируем ключ. Зашифровываем оба текста по одному ключу. Зашифровываем первый шифротекст по второму шифротексту. Используем один из текстов в качестве ключа дешифровки.

```

p1 = 'НаВашисходящийот1204'
p2 = 'ВСеверныйфилиалБанка'
key = generate_key(20)

c1 = encrypt(p1, key=key)
c2 = encrypt(p2, key=key)

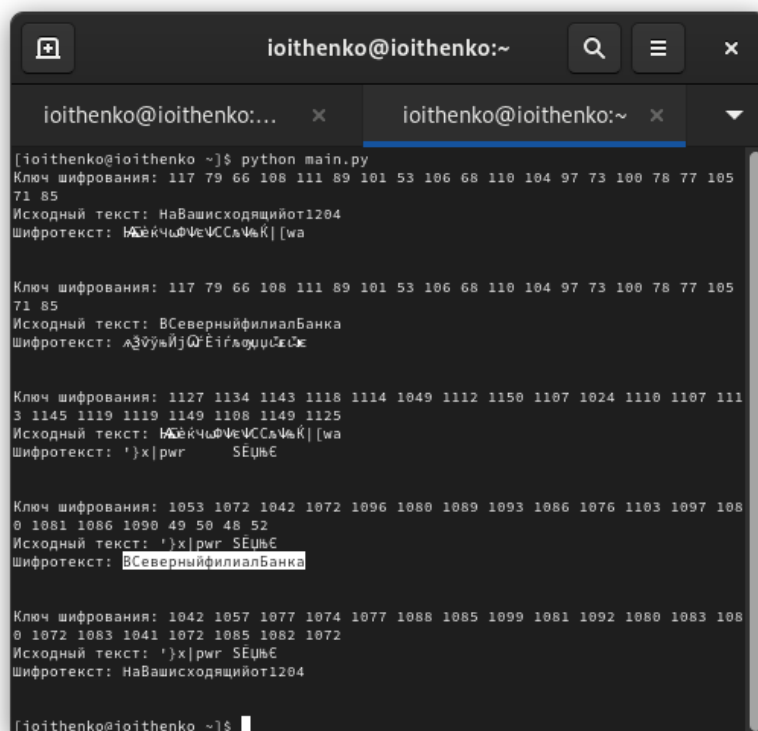
c1_c2 = encrypt(c1, key=c2)

```

encrypt(c1_c2, p1)

encrypt(c1_c2, p2)

Компилируем программу (рис. 2.1).



```
[ioithenko@ioithenko ~]$ python main.py
Ключ шифрования: 117 79 66 108 111 89 101 53 106 68 110 104 97 73 100 78 77 105
71 85
Исходный текст: НаВашисходящийот1204
Шифротекст: hXkKчФVеVCCsV%K| [wa

Ключ шифрования: 117 79 66 108 111 89 101 53 106 68 110 104 97 73 100 78 77 105
71 85
Исходный текст: ВСеверныйфилиалБанка
Шифротекст: A3vUyИjQFEiГoиuиeCя

Ключ шифрования: 1127 1134 1143 1118 1114 1049 1112 1150 1107 1024 1110 1107 111
3 1145 1119 1119 1149 1108 1149 1125
Исходный текст: hXkKчФVеVCCsV%K| [wa
Шифротекст: '>х|рwг SEцЬЕ

Ключ шифрования: 1053 1072 1042 1072 1096 1080 1089 1093 1086 1076 1103 1097 108
0 1081 1086 1090 49 50 48 52
Исходный текст: '>х|рwг SEцЬЕ
Шифротекст: ВСеверныйфилиалБанка

Ключ шифрования: 1042 1057 1077 1074 1077 1088 1085 1099 1081 1092 1080 1083 108
0 1072 1083 1041 1072 1085 1082 1072
Исходный текст: '>х|рwг SEцЬЕ
Шифротекст: НаВашисходящийот1204

[ioithenko@ioithenko ~]$
```

Рис. 2.1: Вывод программы

3 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа? Нужно применить XOR для двух шифротекстов, а к полученному результату применить XOR с ключом, равным известному открытому тексту. Тогда результатом будет второй открытый текст
2. Что будет при повторном использовании ключа при шифровании текста? Шифрование будет небезопасным, т.к. с помощью шифротекстов и одного открытого текста можно дешифровать другой текст
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? Каждый текст шифруется однократным гаммированием отдельно с использованием этого ключа
4. Перечислите недостатки шифрования одним ключом двух открытых текстов. Главный недостаток - можно дешифровать открытый текст без знания ключа.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов. Т.к. ключей используется меньше, то тратится меньше памяти на хранение и передачу ключей.

4 Выводы

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

Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.