

# **Отчёт по лабораторной работе №8**

**Дисциплина: Информационная безопасность**

Евдокимов Иван Андреевич

# Содержание

Техническое оснащение:	5
Цель работы:	6
Постановка задачи	7
Код программы	8
Список литературы	12

# Список иллюстраций

1	шифровка и дишифровка текста . . . . .	10
2	шифровка и дишифровка текста на английском . . . . .	11

## Список таблиц

## Техническое оснащение:

- Персональный компьютер с операционной системой Windows 10;
- OBS Studio, использующийся для записи скринкаста лабораторной работы;
- Приложение Visual Studio Code для редактирования файлов формата *md*, а также для конвертации файлов отчётов и презентаций;

## **Цель работы:**

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

## Постановка задачи

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.

# Код программы

```
# Импортируем модули для генерации случайными символов и для работы с системами с
import random
import string

# Определяем класс для работы с текстовым кодированием
class TextEncoding:

    @staticmethod # Статический метод, который не требует экземпляр класса для в
    def determine_alphabet(text):
        # Определяем, используется ли латиница в шифре. Если используется, возвра
        if text[0] in string.ascii_lowercase:
            return string.ascii_lowercase + string.digits
        else:
            return "абвгдеёжзийклмнопрстуфхцщъыьэюя" + string.digits

    @staticmethod
    def generate_key(size, alphabet):
        # Генерируем случайный ключ того же размера, что и вводимый текст
        return "".join(random.choice(alphabet) for _ in range(size))

    @staticmethod
    def to_hex(coding):
```



```

        # Конвертируем каждый символ в шестнадцатеричное представление и объединяем
        return " ".join(hex(ord(character))[2:] for character in coding)

    @staticmethod
    def encode_string(text, key):
        # Возврат xor каждого символа в тексте с соответствующим символом в ключе
        return "".join(chr(ord(char) ^ ord(key_char)) for char, key_char in zip(text, key))

    @staticmethod
    def xor_texts(ciphertext1, ciphertext2):
        # Возврат xor каждого символа в двух текстах
        return "".join(chr(ord(char1) ^ ord(char2)) for char1, char2 in zip(ciphertext1, ciphertext2))

# Получаем вводимые тексты
plaintext1 = input("Введите первый открытый текст: ")
plaintext2 = input("Введите второй открытый текст: ")

# Определяем, какой алфавит использовать для генерации ключа
alphabet = TextEncoding.determine_alphabet(plaintext1)

# Генерируем ключ
key = TextEncoding.generate_key(len(plaintext1), alphabet)

# Выводим ключ и его шестнадцатеричное представление
print(f"Ключ: {key}", f"Ключ в 16 бит: {TextEncoding.to_hex(key)}", sep='\n')

# Шифруем оба текста и выводим их и их шестнадцатеричные представления
ciphertext1 = TextEncoding.encode_string(plaintext1, key)

```

```

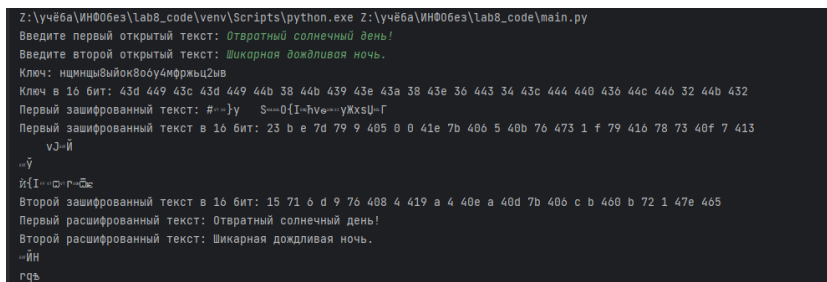
ciphertext2 = TextEncoding.encode_string(plaintext2, key)
print(f"Первый зашифрованный текст: {ciphertext1}", f"Первый зашифрованный текст")
print(f"Второй зашифрованный текст: {ciphertext2}", f"Второй зашифрованный текст")

# Расшифровываем оба текста и выводим их
decrypted_text1 = TextEncoding.encode_string(ciphertext1, key)
decrypted_text2 = TextEncoding.encode_string(ciphertext2, key)
print("Первый расшифрованный текст:", decrypted_text1)
print("Второй расшифрованный текст:", decrypted_text2)

# Выводим результат XOR между двумя зашифрованными текстами
xor_result = TextEncoding.xor_texts(ciphertext1, ciphertext2)
print("Результат XOR двух зашифрованных текстов:", xor_result)

```

вывод запуска программы 1 (шифровка и дешифровка текста).



```

Z:\учеба\ин006ез\lab8_code\venv\Scripts\python.exe Z:\учеба\ин006ез\lab8_code\main.py
Введите первый открытый текст: Отвратный солнечный день!
Введите второй открытый текст: Шикарная дождливая ночь.
Ключ: нщмнщывйок8ооу4мфржц2ув
Ключ в 16 бит: 43d 449 43c 43d 449 44b 38 44b 439 43e 43a 38 43e 3b 443 34 43c 444 44b 43b 44c 44b 32 44b 432
Первый зашифрованный текст: #-}y S==0{I-!ve---yXxsU-Г
Первый зашифрованный текст в 16 бит: 23 b e 7d 79 9 405 0 0 41e 7b 40b 5 40b 7b 473 1 f 79 41b 78 73 40f 7 413
vJ-й
--Û
й{I---о-г-Бж
Второй зашифрованный текст в 16 бит: 15 71 b d 9 7b 408 4 419 a 4 40e a 40d 7b 40b c b 46b b 72 1 47e 4b5
Первый расшифрованный текст: Отвратный солнечный день!
Второй расшифрованный текст: Шикарная дождливая ночь.
--йН
гqъ

```

Рис. 1: шифровка и дешифровка текста

вывод запуска программы 2 на английском (шифровка и дешифровка текста на английском).

```
Z:\y4e6a\ИМ006ea\lab0_code\venv\Scripts\python.exe Z:\y4e6a\ИМ006ea\lab0_code\main.py
Введите первый открытый текст: Disgusting sunny day!
Введите второй открытый текст: A gorgeous rainy night.
Ключ: нБееюоттдоаьктОТЪзг
Ключ в 16 бит: 43c 431 435 431 44e 44e 442 442 444 434 43e 44a 430 432 43a 442 30 442 37 449 44d 433
Первый зашифрованный текст: ojlunlmxBrOмЧеЫаШдW
Первый зашифрованный текст в 16 бит: 478 458 446 456 43b 43d 430 42b 42a 453 41e 439 447 456 42c 49 462 53 428 434 412
Второй зашифрованный текст: SбUуПЧQвЮиYаPяRя
Второй зашифрованный текст в 16 бит: 47d 414 462 45e 43c 429 427 42d 431 447 41e 438 453 453 42c 49 462 59 420 42a 45b
Первый расшифрованный текст: Disgusting sunny day!
Второй расшифрованный текст: A gorgeous rainy night
Результат XOR двух зашифрованных текстов: -I-----
-I
Process finished with exit code 0
```

Рис. 2: шифровка и дишифровка текста на английском

### Выводы:

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

# Список литературы

1. Официальный сайт VirtualBox
2. Материал для выполнения лабораторной
3. Официальный сайт CentOS