Отчёт по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Морозов Михаил Евгеньевич

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	9
Сп	исок литературы	10

Список иллюстраций

3.1	Код. Часть 1	7
3.2	Код. Часть 2	8
3.3	Код. Часть 3	8
3.4	Получили "С новым годом, друзья!"	8

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Теоретическое введение

Гаммирование, или Шифр ХОR, — метод симметричного шифрования, заключающийся в "наложении" последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гаммапоследовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле. Например, в поле Галуа суммирование принимает вид операции "исключающее ИЛИ (ХОR)". [1]

3 Выполнение лабораторной работы

Напишем функции на python и зададим переменные. (рис. 3.1)

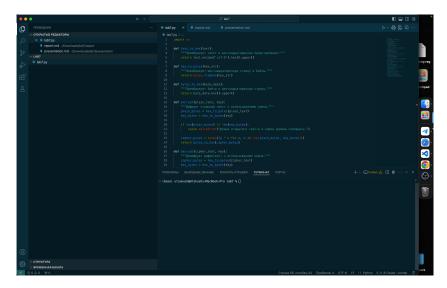


Рис. 3.1: Код. Часть 1

Напишем функции на python и зададим переменные. (рис. 3.2)

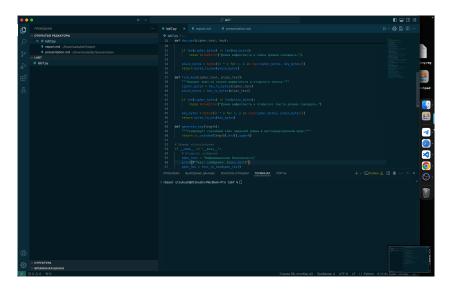


Рис. 3.2: Код. Часть 2

Напишем функции на python и зададим переменные. (рис. 3.3)

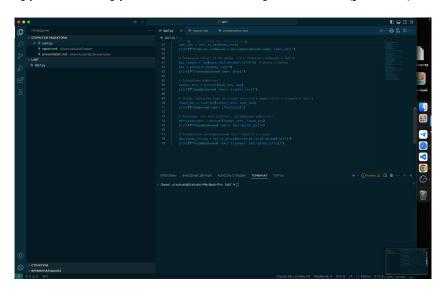


Рис. 3.3: Код. Часть 3

Применим написанные функции для создания ключа, шифрования текста и дешифрования. (рис. 3.4)

```
• (base) utsukush@Utskushs-MacBook-Pro lab7 % /opt/anaconda3/bin/python /Users/utsukush/Desktop/lab7/lab7.py
Текст сообщения: С Новым Годом, друзья!
Открытое сообщение выестнавдатеричном виде: DbA1200090008ED082D188D08C208D093D08ED08D4D08ED08C2C200084D180D183D087D18CD18F21
Стенерированный ключ: 2000592204EA3SC3645D2A40C206C4EB1F7406F2E8F8401EZ13A5C64315F7306FF5E38421D189H77
Замиформальный ключ: 2000592204EA3SC3645D2A40C206C4EB1F7406F2E8F8401EZ13A5C64315F7306FF5E38421D189H7
Замиформальный ключ: 200059204EA3SC465D2A40F206FC4EB17406F75E38F75E3862B1991A1ED06
Рассиформальный текст: D6A12000900008ED002D18ED08C200093D08ED08AD08ED08C2C20008AD18013SD087018CD18F21
Рассиформальный текст: D6A12000900008ED002D18ED08C200093D08ED08AD08ED08C2C20008AD18013SD087018CD18F21
Рассиформальный текст: (Строжа): С Новым Годом, друзья!

( base) utsukush@Utskushs-MacBook-Pro lab7 %
```

Рис. 3.4: Получили "С новым годом, друзья!"

4 Выводы

Освоили на практике применение режима однократного гаммирования.

Список литературы

1. Гаммирование [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: https://en.wikipedia.org/wiki/XOR_cipher.