

Отчет по лабораторной работе №8

Дисциплина: Информационная безопасность

Выполнила: Афтаева Ксения Васильевна

Содержание

1	Цель работы	5
2	Задачи	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	11
	Список литературы	12

Список иллюстраций

4.1	Пример работы программы	10
-----	-----------------------------------	----

Список таблиц

1 Цель работы

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

2 Задачи

1. Изучить принцип одноразового гаммирования для кодирования двух исходных текстов одним ключом.
2. Разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме одноразового гаммирования.

3 Теоретическое введение

Шифрование гаммированием – это метод шифрования, который основан на использовании гаммы [1].

Гамма шифра – это псевдослучайная последовательность, выработанная по определенному алгоритму для шифрования открытых данных и дешифрования зашифрованных данных. Она играет роль ключа в одноразовой система шифрования. Строго говоря, она не удовлетворяет ни требованию случайности, так как используется детерминированный алгоритм для ее выработки, ни требованию бесконечной длины, так как все псевдослучайные последовательности имеют конечный период. Тем не менее, при правильно выбранном алгоритме генерации гаммы шифра можно получить метод шифрования с хорошей практической стойкостью, достаточной для решения реальных задач защиты информации [2].

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста[3].

4 Выполнение лабораторной работы

1. Разработала приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования (код выполнен на языке программирования Python):

```
alphabeth = ['A', 'Б', 'В', 'Г', 'Д', 'Е', 'Ё', 'Ж', 'З', 'И', 'Й', 'К',  
             'Л', 'М', 'Н', 'О', 'П', 'Р', 'С', 'Т', 'У', 'Ф', 'Х', 'Ц',  
             'Ч', 'Ш', 'Щ', 'Ъ', 'Ы', 'Ь', 'Э', 'Ю', 'Я', 'а', 'б', 'в',  
             'г', 'д', 'е', 'ё', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н',  
             'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ',  
             'ъ', 'ы', 'ь', 'э', 'ю', 'я', '.,', '!', '?', ' ']
```

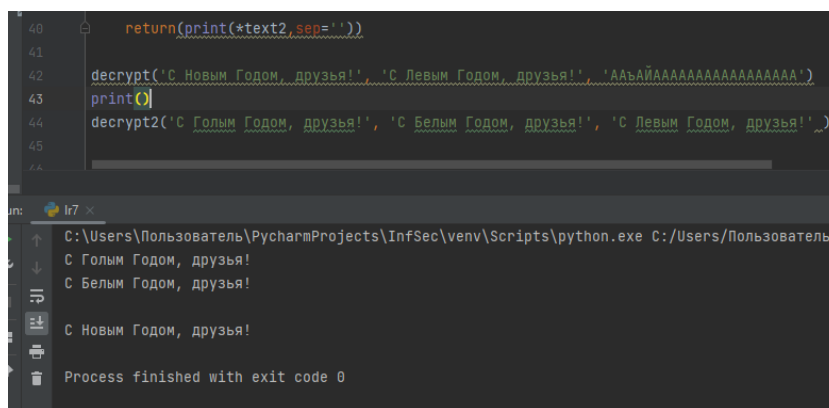
```
def decrypt(text1, text2, gamma):  
    text1Len = len(text1)  
    text2Len = len(text2)  
    gammaLen = len(gamma)  
  
    keyText = []  
    for i in range(text1Len // gammaLen):  
        for symb in gamma:  
            keyText.append(symb)  
    for i in range(text1Len % gammaLen):  
        keyText.append(gamma[i])
```


'С Левым Годом, друзья!')

Первая функция (decrypt) определяет вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе. Задаем алфавит из заглавных, строчных букв русского алфавита, !, ?, ., , и пробела. На вход поступает два открытых текста, в виде массива символов, и ключ — гамму. Анализируем длину текста, «растягиваем» гамму до нужного размера и выполняем посимвольное сложение. Функция выводит два шифротекста.

Вторая функция (decrypt2) позволяет злоумышленнику прочитать оба текста, не зная ключа и не стремясь его определить. Если у злоумышленника есть оба шифротекста и один из открытых текстов, достаточно сложить по модулю 2 оба шифротекста и открытый текст, и получим второй открытый текст, не зная ключа.

В качестве примера работаю с фразой из предыдущей лабораторной работы и ее вариациями. Вызвала первую функцию, передав ей 2 открытых текста и гамму, с помощью которой ее нужно зашифровать (рис. 4.1). Получила два зашифрованных текста (рис. 4.1). Затем два полученных зашифрованных текста передаю во вторую функцию (рис. 4.1). Туда же передаю один из открытых текстов (рис. 4.1). На выход получаю второй открытый текст (рис. 4.1).



```
40     return(print(*text2, sep=''))
41
42     decrypt('С Новым Годом, друзья!', 'С Левым Годом, друзья!', 'АААААААААААААААААААА')
43     print()
44     decrypt2('С Голым Годом, друзья!', 'С Белым Годом, друзья!', 'С Левым Годом, друзья!')
45
46
```

Terminal Output:

```
C:\Users\Пользователь\PycharmProjects\InfSec\venv\Scripts\python.exe C:/Users/Пользователь/
С Голым Годом, друзья!
С Белым Годом, друзья!
С Новым Годом, друзья!
Process finished with exit code 0
```

Рис. 4.1: Пример работы программы

5 Выводы

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. Разработала приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования.

Список литературы

1. Шифрование гаммированием: простыми словами о защите информации [Электронный ресурс]. 2023. URL: <https://nauchniestati.ru/spravka/shifrovanie-gammirovaniem/>.
2. Шифрование методом гаммирования [Электронный ресурс]. 2018. URL: https://studopedia.ru/20_116311_shifrovanie-metodom-gammirovaniya.html.
3. Лабораторная работа №7. Элементы криптографии. однократное гаммирование. [Электронный ресурс]. 2023. URL: https://esystem.rudn.ru/pluginfile.php/2090352/mod_resource/content/2/007-lab_crypto-gamma.pdf.