Отчет по лабораторной работе №7

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.

2 Задачи

1. Изучить принцип однократного гаммирования.
2. Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного 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 данные в режиме однократного гаммирования (код выполнен на языке программирования Python):

```
alphabeth = ['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', '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 encrypt(text, gamma):
    textLen = len(text)
    gammaLen = len(gamma)

    keyText = []
    for i in range(textLen // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(textLen % gammaLen):
        keyText.append(gamma[i])
```

```
    code = []
    for i in range(textLen):
        code.append(alphabeth[(alphabeth.index(text[i])
        + alphabeth.index(keyText[i])) % 73])

    return(print(*code,sep=''))

def decrypt(code, gamma):
    codeLen = len(code)
    gammaLen = len(gamma)

    keyText = []
    for i in range(codeLen // gammaLen):
        for symb in gamma:
            keyText.append(symb)
    for i in range(codeLen % gammaLen):
        keyText.append(gamma[i])

    text = []
    for i in range(codeLen):
        text.append(alphabeth[(alphabeth.index(code[i])
        - alphabeth.index(keyText[i]) + 73) % 73])

    return(print(*text,sep=''))

encrypt('С Новым Годом, друзья!', 'ААъАЙАААААААААААААААА' )
decrypt('С Болым Годом, друзья!', 'ААъАЙАААААААААААААААА' )
decrypt('С Новым Годом, друзья!', 'С Болым Годом, друзья!')
```

В качестве примера зашифруем текст “С Новым Годом, друзья!” (рис. 4.1). Затем

полученный результат пробуем расшифровать тем же ключом (рис. 4.1). Видим, что все успешно расшифровалось (рис. 4.1). Затем определяем ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис. 4.1). Для этого используем функцию дешифровки, передавая ей исходный текст и то, что получилось в зашифрованном варианте (рис. 4.1). Получаем ключ.

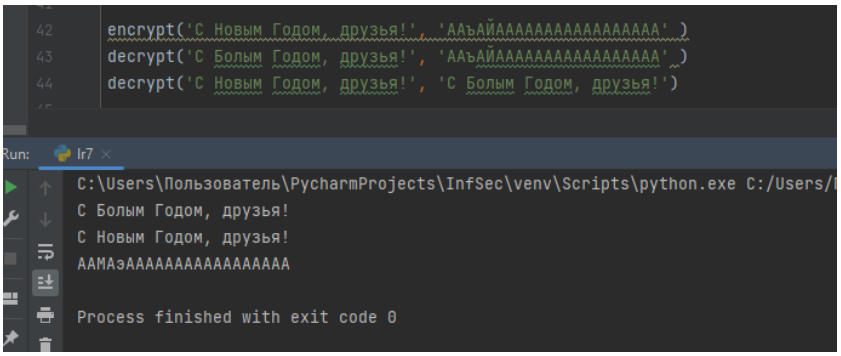

Рис. 4.1: Пример работы программы

5 Выводы

Я освоила на практике применение режима однократного гаммирования. Разработала приложение, позволяющее шифровать и дешифровать данные 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.