

Математические основы защиты информации и информационной безопасности. Лабораторная работа №3

Шифрование гаммированием

Студент: Лесков Данила Валерьевич НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
3.1	Шифрование гаммированием	7
4	Выполнение лабораторной работы	9
4.1	Описание реализации метода шифрования	9
4.2	Листинг	10
4.3	Полученные результаты	12
5	Выводы	13
	Список литературы	14

List of Figures

4.1	Схема однократного использования	9
4.2	Результаты шифрования гаммированием	12

List of Tables

1 Цель работы

Ознакомиться с шифрованием гаммированием на примере гаммирования конечной гаммой.

2 Задание

1. Реализовать алгоритм шифрования гаммированием конечной гаммой.

3 Теоретическое введение

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле.

3.1 Шифрование гаммированием

При шифровании гаммированием формируется m - разрядная случайная последовательность. Пусть k - передаваемое сообщение

$$k = k_1 k_2 \dots k_i \dots k_m,$$

а p - последовательность, которая является ключом:

$$p = p_1 p_2 \dots p_i \dots p_m,$$

тогда i -ый символ криптограммы будет равен:

$$c_i = p_i \oplus k_i,$$

где \oplus - операция побитового сложения XOR [1]. В результате криптограмму можно записать следующим образом:

$$C = c_1 c_2 \dots c_i \dots c_m$$

Более подробно о шифровании гаммированием: [2]

4 Выполнение лабораторной работы

В рамках данной лабораторной работы был описан алгоритм шифрования гаммированием с конечной гаммой.

4.1 Описание реализации метода шифрования

В данной работе применяется схема однократного использования (рис. 4.1). К элементам ключа и исходного сообщения применяется побитовое сложение XOR, в результате чего формируется зашифрованное сообщение:

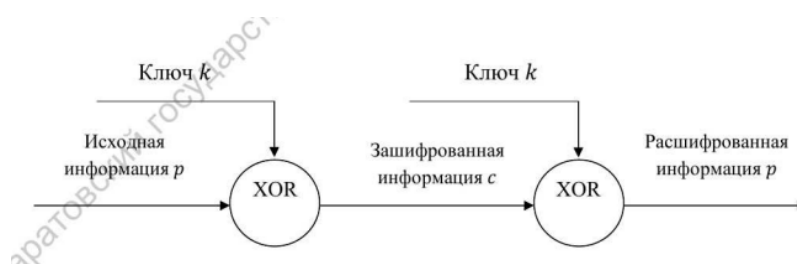


Figure 4.1: Схема однократного использования

Для того, чтобы применить операцию побитового сложения, необходимо, чтобы ключ и исходное сообщение были одной длины. Для достижения данной цели, ключ растягивается до тех пор, пока не сравняется длиной с исходным сообщением следующим образом: пусть сообщение будет

SECURITY,

длина 'm' которого равна 12, тогда ключ растягивается следующим образом:

$$KEY \rightarrow KEYKEYKE$$

Таким образом, к сообщению и ключу одинаковой длины можно применить операцию побитового сложения XOR.

4.2 Листинг

Код приведенной ниже программы реализован на языке python.

```
alphabet = 'абвгдеёжзийклмнопрстуфхцчщъыьэюя'
ignore_symbols = '!@#$%^&*(){}[]<>./" '

def get_indexes(text):
    indexes = []
    for letter in text:
        try:
            indexes.append(alphabet.index(letter) + 1)
        except ValueError:
            indexes.append(ignore_symbols.index(letter) + 10000)
    return indexes

def format_gamma(gamma, message_length):
    new_gamma = ""
    for i in range(message_length):
        new_gamma += gamma[i % len(gamma)]
    return new_gamma
```

```

def encrypt(message_indexes, gamma_indexes):
    indexes = []
    for ix, item in enumerate(message_indexes):
        if message_indexes[ix] > 10000 or gamma_indexes[ix] > 10000:
            result = item
            indexes.append(result)
            continue
        result = (message_indexes[ix] + gamma_indexes[ix]) % len(alphabet)
        indexes.append(result)
    return indexes

def to_text(indexes):
    text = ""
    for index in indexes:
        if index > 10000:
            text += ignore_symbols[index - 10000]
            continue
        text += alphabet[index - 1]
    return text

if __name__ == '__main__':
    message = input("Введите сообщение: ")
    gamma = input("Введите ключ (гамма): ")
    new_gamma = format_gamma(gamma, len(message))
    print("\nПреобразование {} -> {}".format(gamma.upper(), new_gamma.upper()))
    message_indexes = get_indexes(message)

```

```

print("\nВаше сообщение:\n{ } ({})".format(message.upper(), message_indexes))
    gamma_indexes = get_indexes(new_gamma)
print("\nВаша гамма:\n{ } ({})".format(gamma.upper(), gamma_indexes))
encrypted_message_indexes = encrypt(message_indexes, gamma_indexes)
    encrypted_message = to_text(encrypted_message_indexes)
print("\nЗашифрованное сообщение:\n{ } ({})"
    .format(encrypted_message.upper(), encrypted_message_indexes))

```

4.3 Полученные результаты

При запуске программы пользователю предлагается ввести сообщение, которое необходимо зашифровать, и ключ. После этого, если ключ и сообщения разной длины, из ключа исключаются лишние символы или добавляются в конец новые. Знаки препинания и пробелы, в свою очередь, игнорируются и остаются в неизменном виде. Для удобства, они нумеруются начиная с индекса 10000. В результате выполнения пользователь получает зашифрованное сообщение (рис. 4.2).

```

Введите сообщение: БЕЗОПАСНОСТЬ
Введите ключ (гамма): БЕЗОПАСНОСТЬ

Преобразование БЕЗОПАСНОСТЬ -> БЕЗОПАСНОСТЬБЕЗОПАСНОСТЬ

Ваше сообщение:
ШИФРОВАНИЕ ГАММИРОВАНИЕМ ([26, 10, 22, 18, 16, 3, 1, 15, 10, 6, 10020, 4, 1, 14, 14, 10, 18, 16, 3, 1, 15, 10, 6, 14])

Ваша гамма:
БЕЗОПАСНОСТЬ ([2, 6, 9, 16, 17, 1, 19, 15, 16, 19, 20, 30, 2, 6, 9, 16, 17, 1, 19, 15, 16, 19, 20, 30])

Зашифрованное сообщение:
ЪЮЗЛЯГТЬШЧ АВТКШЕПФЮЗЫШ ([28, 16, 31, 1, 0, 4, 20, 30, 26, 25, 10020, 1, 3, 20, 23, 26, 2, 17, 22, 16, 31, 29, 26, 11])

Process finished with exit code 0

```

Figure 4.2: Результаты шифрования гаммированием

5 Выводы

В ходе выполнения данной лабораторной работы было выполнено ознакомление с шифрованием гаммированием на шифрования гаммированием с конечной гаммой.

В результате проделанной работы был программно реализован этот метод шифрования.

Как итог, поставленные цели и задачи были успешно достигнуты.

Список литературы

1. Исключающее «или» [Электронный ресурс]. Википедия, 2021. URL: https://ru.wikipedia.org/wiki/Исключающее_«или».
2. Шифр табличной маршрутной перестановки [Электронный ресурс]. Википедия, 2020. URL: <https://ru.wikipedia.org/wiki/Таммирование>.