Отчет по лабораторной работе 3

По предмету мат. основы защиты информации

Студент: Дидусь Кирилл Валерьевич, 1132223499
Группа: НПМмд-02-22
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва, 2022

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Целью данной лабораторной работы является ознакомление с шифрованием гаммированием, а так же реализация шифрования гаммирования конечной гаммой.

2 Задание

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. Например, в поле Галуа суммирование принимает вид операции «исключающее ИЛИ (XOR)» [1].

В криптографии простой шифр XOR является разновидностью аддитивного шифра, алгоритма шифрования, который работает в соответствии с принципами [2]:

$$A \oplus 0 = A,$$
$$A \oplus A = 0,$$
$$A \oplus B = B \oplus A,$$
$$(A \oplus B) \oplus C = A \oplus (B \oplus C),$$
$$(B \oplus A) \oplus A = B \oplus 0 = B,$$

Рис. 3.1: Рис. 1.Принципы алгоритма шифрования гаммированием

где $\oplus$ обозначает операцию исключающей дизъюнкции (XOR). Эта операция иногда называется сложением по модулю 2 (или вычитанием, что идентично). С

помощью данной логики строка текста может быть зашифрована путем применения побитового оператора XOR к каждому символу с использованием заданного ключа. Для расшифровки результата достаточно повторно применить функцию XOR с ключом, чтобы снять шифр [2].

Шифры гаммирования (аддитивные шифры) являются самыми эффективными с точки зрения стойкости и скорости преобразований (процедур зашифрования и дешифрования). По стойкости данные шифры относятся к классу совершенных. Для зашифрования и дешифрования используются элементарные арифметические операции – открытое/зашифрованное сообщение и гамма, представленные в числовом виде, складываются друг с другом по модулю (mod) [3].

Пусть символам исходного алфавита соответствуют числа от 0 (А) до 32 (Я). Если обозначить число, соответствующее исходному символу, x, а символу ключа – k, то можно записать правило гаммирования следующим образом: $z = x + k \pmod N$, где z – закодированный символ, N - количество символов в алфавите, а сложение по модулю N - операция, аналогичная обычному сложению, с тем отличием, что если обычное суммирование дает результат, больший или равный N, то значением суммы считается остаток от деления его на N [4].

4 Выполнение лабораторной работы

Примечание: комментарии по коду представлены на скриншотах к каждому из проделанных заданий.

4.1 Шифрование гаммированием

В соответствии с заданием, была написана программа для шифрования гаммированием. Программный код представлен в качестве листинга в конце отчета.

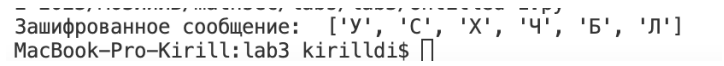

Рис. 4.1: Рис. 2. Результат шифрования сообщений с использованием гаммирования конечной гаммой

5 Библиография

1. Википедия. Гаммирование [Электронный ресурс]. Википедия, свободная энциклопедия, 2022. URL: https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5 (дата обращения: 14.11.2022).

2. Wikipedia. XOR cipher [Электронный ресурс]. Wikipedia, free Encyclopedia, 2022. URL: https://en.wikipedia.org/wiki/XOR_cipher (дата обращения: 14.11.2022).

3. Викторович А.В. 6.1 Шифры гаммирования [Электронный ресурс].Учебная и научная деятельность Анисимова Владимира Викторовича, 2021. URL: https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema6 (дата обращения: 14.11.2022).

4. Интерактивная система обучения. Методы шифрования с закрытым ключом [Электронный ресурс]. Электроника для всех, 2017. URL: https://emkelektron.webnode.com/news/metody-shifrovaniya-zamenoj-podstanovkoj/ (дата обращения: 14.11.2022).

6 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомился с шифрованием гаммированием, а так же мне удалось реализовать алгоритм шифрования конечной гаммой на языке программирования Python.

7 Листинг программы

```
alfabet = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЪЭЮЯ"

# Функция переводящяя строку в последовательность из алфавитного номера букв сооб
def to_number(msg):
    number_arr = []
    for char in msg:
        number_arr.append(alfabet.index(char)+1)
    return number_arr

# Функция переводящяя последовательность из алфавитного номера букв сообщения в с
def to_letters(num_arr):
    letter_arr = []
    for num in num_arr:
        letter_arr.append(alfabet[num-1])
    return letter_arr

# Функция выполняющая шифрование
def encrypt_gamma(msg,key,m):
    code = []
    i = 0
    for num in msg:
        if i == len(key):
```

```
            i = 0
        code.append((num + key[i])%m)
        i += 1
    return to_letters(code)

# вызов функций
a = to_number("ПРИКАЗ") # сообщение
b = to_number("ГАММА") # ключ
m = 33
print("Зашифрованное сообщение: ",encrypt_gamma(a,b,m))
```