Лабораторная работа №3

Математические основы защиты информации и информационной безопасности

Леонтьева К. А., НПМмд-02-23

9 октября 2023

Российский университет дружбы народов

Москва, Россия

Цель лабораторной работы

1) Реализовать на языке программирования шифрование гаммированием конечной гаммой

Задачи лабораторной работы

1) Изучить теоретическую часть лабораторной работы по методичке
2) Написать соответствующую программу

Гаммирование - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, то есть псевдослучайной последовательности (ПСП) с выходов генератора G. Чаще всего в качестве функции F берется операция поразрядного сложения по модулю два или по модулю N (N - число букв алфавита открытого текста).

Простейший генератор ПСП можно представить рекуррентным соотношением:

$$\gamma_i = (a\gamma_{i-1} + b)mod(m), i = 1, ..., m,$$

где γ_i - i-й член последовательности псевдослучайных чисел, a, γ_0, b - ключевые параметры.

Ход выполнения лабораторной работы

- Реализуем шифрование гаммированием с конечной гаммой

```
import numpy as np
import math
```

```
word = 'приказ'
gamma = 'гамма'
word = list(word.replace(" ", ""))
gamma = list(gamma)

alphabet = []
for i in range(1072,1104):
    alphabet.append(chr(i))
```

```
gamma_new = []

if len(word) > len (gamma):
    for i in range(math.floor(len(word)/len(gamma))):
        gamma_new.append(gamma)
    sum(gamma_new, [])
    for j in range(len(word)%len(gamma)):
        gamma_new.append(list(gamma[j]))

if len(word) < len (gamma):
    for g in range(len(word)):
        gamma_new.append(list(gamma[g]))

gamma_new = sum(gamma_new,[])
```

Figure 1: Рис.1: Шифрование гаммированием

Ход выполнения лабораторной работы

```
number_word = []
number_gamma_new = []
for i in range(len(word)):
    number_word.append(alphabet.index(word[i])+1)
    number_gamma_new.append(alphabet.index(gamma_new[i])+1)
```

```
chipher = []
for i in range(len(word)):
    k = (number_word[i] + number_gamma_new[i])%32
    chipher.append(alphabet[k-1])
```

```
print(''.join(chipher))
```

```
усхчбл
```

Figure 2: Рис.2: Шифрование гаммированием

Вывод

- В ходе выполнения данной лабораторной работы было реализовано шифрование гаммированием конечной гаммой на языке программирования Python