

Защита лабораторной З

по предмету мат. основы защиты информации

Дидусь К.В.

Российский университет дружбы народов, Москва, Россия

Информация

- Диудусь Кирилл Валерьевич
- Студент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- 1132223499@rudn.ru
- <https://github.com/kirilldi/>



Введение

Актуальность

- Изучение базовых принципов шифрования
- Важность знания основ шифрования для работы в сфере информационных технологий

Цели и задачи лабораторной

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

- ТУИС РУДН
- Язык программирования Python

Выполнение лабораторной

$$A \oplus 0 = A,$$

$$A \oplus A = 0,$$

$$A \oplus B = B \oplus A,$$

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

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

Figure 1: Рис. 1. шифрование гаммированием

Программная реализация

```
3 # Функция переводящая строку в последовательность из алфавитного номера букв сообщения
4 def to_number(msg):
5     number_arr = []
6     for char in msg:
7         number_arr.append(alfabet.index(char)+1)
8     return number_arr
9
10 # Функция переводящая последовательность из алфавитного номера букв сообщения в строку букв
11 def to_letters(num_arr):
12     letter_arr = []
13     for num in num_arr:
14         letter_arr.append(alfabet[num-1])
15     return letter_arr
16
17 # Функция выполняющая шифрование
18 def encrypt_gamma(msg, key, m):
19     code = []
20     i = 0
21     for num in msg:
22         if i == len(key):
23             i = 0
24         code.append(num + key[i] % m)
25         i += 1
26     return to_letters(code)
```

Figure 2: Рис. 2. Программная реализация шифрования гаммированием

Вывод программы

```
-----, -----, -----, -----, -----, -----, -----  
Зашифрованное сообщение: ['У', 'С', 'Х', 'Ч', 'Б', 'Л']  
MacBook-Pro-Kirill:lab3 kirilldi$ █
```

Figure 3: Рис. 3. Результат шифрования слова ПРИКАЗ с гаммой ГАММА

Вывод

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