# Отчёт по лабораторной работе №7

**Элементы криптографии. Однократное гаммирование**

Волков Тимофей Евгеньевич

# Содержание

**1 Цель работы** **5**

**2 Теоретическое описание** **6**

**3 Выполнение лабораторной работы** **8**

**4 Выводы** **10**

**5 Контрольные вопросы** **11**

# List of Tables

# List of Figures

3.1 Функции . . . . . 8
3.2 Задание 1 . . . . . 9
3.3 Задание 2 . . . . . 9

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Теоретическое описание

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» является простой, но надёжной схемой шифрования данных.

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

К. Шеннон доказал абсолютную стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.

Необходимые и достаточные условия абсолютной стойкости шифра: – полная случайность ключа; – равенство длин ключа и открытого текста; – однократное использование ключа.

# 3 Выполнение лабораторной работы

Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Функции (fig. 3.1):

hex_ — перевод в шестнадцатиричную систему.

gen_key — генерирует рандомный ключ.

encrypt — шифрует текст.

decrypt — дешифрует тескт.

compute_key — создает ключ на основе текста и шифротекста.

```
Ввод [1]: import string
          import random

Ввод [2]: def hex_(text):
              return ' '.join(hex(ord(i))[2:] for i in text)

Ввод [3]: def gen_key(size):
              return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))

Ввод [4]: def encrypt(text, key):
              return ''.join(chr(a^b) for a, b in zip(text, key))

Ввод [5]: def decrypt(encrypt, key):
              return ''.join(chr(a^b) for a, b in zip(encrypt, key))

Ввод [6]: def compute_key(text, encrypt):
              return ''.join(chr(a^b) for a, b in zip(text, encrypt))
```

Figure 3.1: Функции

1. Определить вид шифротекста при известном ключе и известном открытом тексте (fig. 3.2).


Figure 3.2: Задание 1

2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (fig. 3.3).


Figure 3.3: Задание 2

# 4 Выводы

Освоил на практике применение режима однократного гаммирования.

# 5 Контрольные вопросы

1. Поясните смысл однократного гаммирования.
   Гаммирование — 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.

2. Перечислите недостатки однократного гаммирования.
   Ключ одного размера с сообщением, на один ключ используется только один текст.

3. Перечислите преимущества однократного гаммирования.
   Простота, криптостойкость.

4. Почему длина открытого текста должна совпадать с длиной ключа?
   Каждый символ текста попарно складывается с символом ключа.

5. Какая операция используется в режиме однократного гаммирования, назовите её особенности?
   Используется сложение по модулю 2.

6. Как по открытому тексту и ключу получить шифротекст?
   Сложить по модулю 2 каждый символ открытого текста и ключа.

7. Как по открытому тексту и шифротексту получить ключ?
   Сложить по модулю 2 каждый символ открытого текста и шифротекста.

8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

   – полная случайность ключа; – равенство длин ключа и открытого текста; – однократное использование ключа.