Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование.

Казакова Виктория Алексеевна

Содержание

Список иллюстраций

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

3 Ход работы

1. Импорт необходимых модулей, создание функций для перевода данных в 16ричный формат, функции для ключа и функцию кодирования и декодирования (рис. 3.1).

```
import string
import random

def text(t):
  return "".join(hex(ord(i))[2:] for i in t)

def get_key(size):
  return "".join(random.choice(string.ascii_letters + string.digits) for _ in range(size))

def coder(t, key):
  return "".join(chr(a ^ b) for a, b in zip(t, key))
```

Рис. 3.1: Подготовка необходимых функций

2. Прописываю основной код, в котором используются все написанные ранее функции (рис.@fig:002).

```
message = "С новым годом, друзья!"
key1 = get_key(len(message))
key2 = text(key1)
print("Ключ: ", key2)
text1 = coder([ord(i) for i in message], [ord(i) for i in key1])
text2 = text(text1)
print("Зашифрованное сообщение: ", text2)
text3 = coder([ord(i) for i in text1], [ord(i) for i in key1])
print("Расшифрованное сообщение: ", text3)
```

Рис. 3.2: Кодирование и декодирование строки

3. Результат работы программы: (3.3).

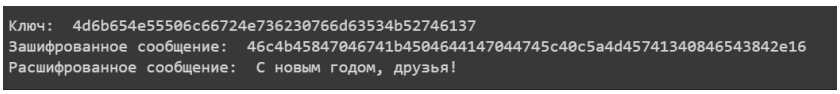

Рис. 3.3: Результат

4 Выводы

В ходе работы было освоено на практике применение режима однократного гаммирования.

5 Список литературы

1. [Методический материал] [https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/co
   lab_crypto-gamma.pdf]
2. [Сайт для поиска команд] [https://www.ibm.com/]
3. [Google Colab] [https://colab.research.google.com/?hl=ru]