Лабораторная №8

Основы информационной безопасности

Жибицкая Е.Д.

Российский университет дружбы народов, Москва, Россия

Цель

Цель работы

- Освоение на практике применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Ход работы

Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Реализация

Для выполнения данной лабораторной работы воспользуемся программой, написанной в предыдущей лабораторной работе №7. Зашифруем исходные сообщения, предварительно сгенерировав ключ.

```
import random
import string
def key_generation(text):
  key = ''
  for i in range(len(text)):
    key += random.choice(string.ascii_letters + string.digits)
  return key

def encryption(text, key):
    n_text = ''
    for i in range(len(text)):
      n_text += chr(ord(text[i]) ^ ord(key[i]))
    return n_text

P1 = 'НаВашисходящийот1204'
key = key_generation(P1)
en_P1 = encryption(P1, key)
de_P1 = encryption(en_P1, key)

P2 = 'ВСеверныйфилиалБанка'
en_P2 = encryption(P2, key)
de_P2 = encryption(en_P2, key)
```

Рис. 1: Сообщения 1 и 2

Реализация

```
print("Открытый текст: ", P1, "\nКлюч: ", key, "\nШифротекст: ", en_P1, "\nИсходный текст: ", de_P1)
print("Открытый текст: ", P2 ,"\nКлюч: ", key ,"\nШифротекст: ", en_P2 ,"\nИсходный текст: ", de_P2)

encr = encryption(en_P1, en_P2)
print("Расшифровка P1, зная P2: ", encryption(P2, encr))
print("Расшифровка P2, зная P1: ", encryption(P1, encr))
```

Рис. 2: Расшифровка сообщений

Затем сгенерируем шифротекст, посмотрим на вывод программы. Также выполним задание и расшифруем сообщение 1 за счет сообщения 2 и наоборот(для этого также используем сложение по модулю 2).

Результат

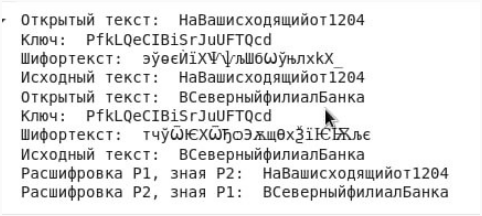

Рис. 3: Вывод программы

Выводы

Вывод

- В ходе работы было произведено повторное знакомство с элементами криптографии, произведена шифровка и дешифровка даннных с помощью ключа, расшифровка сообщений, закодированных одним ключом без ключа, зная только сообщения