Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

дисциплина: Информационная безопасность

Студент: Койфман Кирилл Дмитриевич Группа: НПИбд-01-21

Цель работы Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Задачи

1. Разобрать теоретическую часть и указание к работе, описанные в файле.
2. Разработать приложение, позволяющее шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 при известном ключе.

---

1 задание

Анализ теоретической части лабораторной работы:

Исходные данные.
Две телеграммы Центра:
P_1 = НаВашисходящийот1204
P_2 = ВСеверныйфилиалБанка
Ключ Центра длиной 20 байт:
K = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой, приведённой на рис. 8.1.

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$\begin{aligned} C_1 &= P_1 \oplus K, \\ C_2 &= P_2 \oplus K. \end{aligned} \tag{8.1}$$

Открытый текст можно найти в соответствии с (8.1), зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства (8.1)

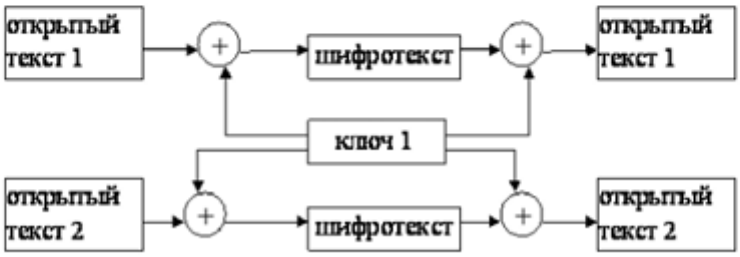

Рис. 8.1. Общая схема шифрования двух различных текстов одним ключом

---

2 задание

Реализация программы, позволяющей шифровать и дешифровать тексты P_1 и P_2 в режиме однократного гаммирования:

```python
import random
import string

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

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

def encrypt(inputText_1, inputText_2):
  text_1 = [ord(i) for i in inputText_1]
  text_2 = [ord(i) for i in inputText_2]
  return ''.join(chr (a^b) for a, b in zip(text_1, text_2))
```

```python
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
print("Source text P1: ", P1)
print("Source text P2: ", P2)

key = generateKey(len(P1))
hexKey = generateHexKey(key)
print("\nKey: ", key)
print("Hex key: ", hexKey)

C1 = encrypt(P1, key)
C2 = encrypt(P2, key)
print("\nEncrypted text P1: ", C1)
print("Encrypted text P2: ", C2)

decrypt = encrypt(C1, C2)
print("\nDecrypted text P1: ", encrypt(decrypt, P2))
print("Decrypted text P2: ", encrypt(decrypt, P1))
```

```
Source text P1:  НаВашисходящийот1204
Source text P2:  ВСеверныйфилиалБанка

Key:  TeOKkAGPxtQt7V7EnR74
Hex key:  54 65 4f 4b 6b 41 47 50 78 74 51 74 37 56 37 45 6e 52 37 34

Encrypted text P1:  щзѝфУѻIEцрOнЦѮЉЇ_`□□
Encrypted text P2:  цфѲѻўЁѲЛсањяЦАЌеўѮЍЄ

Decrypted text P1:  НаВашисходящийот1204
Decrypted text P2:  ВСеверныйфилиалБанка
```

Спасибо за внимание!