Защита лабораторной работы №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Бурдина Ксения Павловна

2022 Oct 19th

RUDN University, Moscow, Russian Federation

Результат выполнения лабораторной работы №8

Цель выполнения лабораторной работы

Цель выполнения лабораторной работы

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

Теоретические сведения

Схема шифрования двух различных текстов одним ключом:

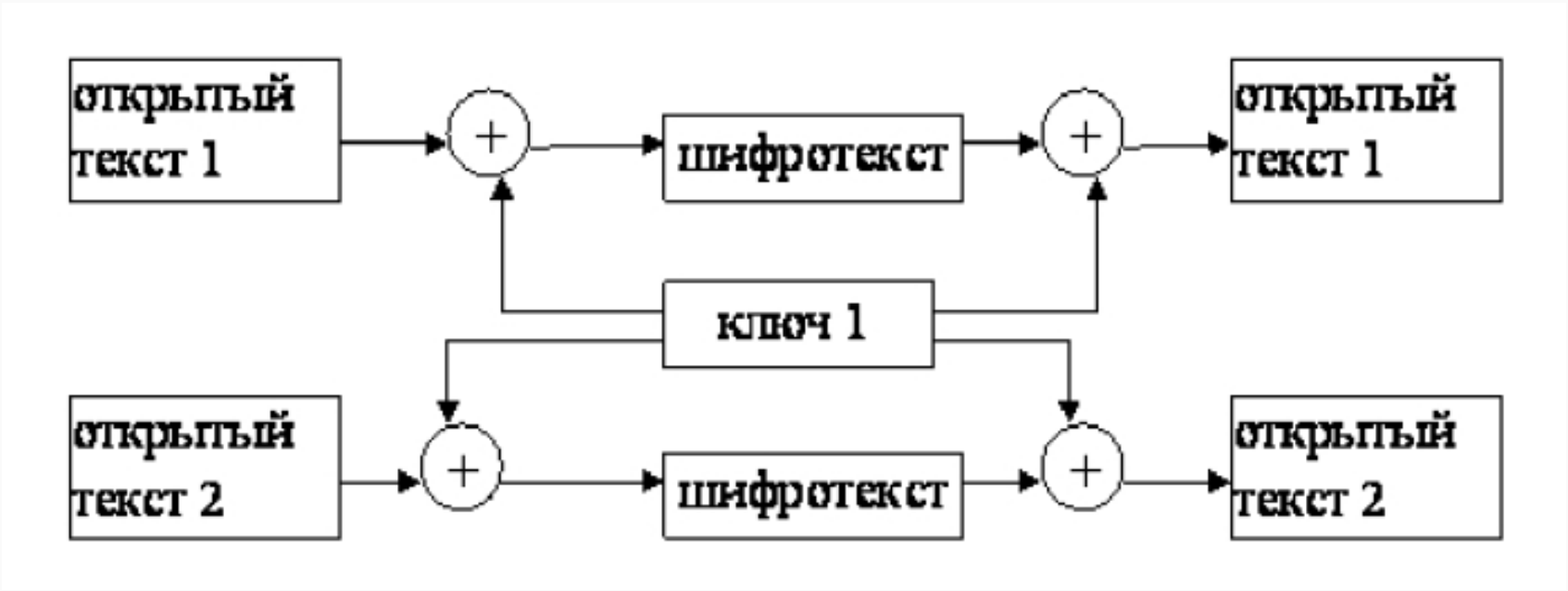

Figure 1: Шифрование двух текстов одним ключом

Шифротексты обеих телеграмм можно найти следующим образом:

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K$$

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Результат выполнения лабораторной работы

Результат выполнения лабораторной работы

Постановка задачи:

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 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. Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Результат выполнения лабораторной работы

Ввод импортов и определение функций, которые будем использовать:

```
import string
import random
```

```
def fun_1(text):
    return ' '.join(hex(ord(i))[2:] for i in text)

def fun_2(size):
    return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))

def fun_3(text1, text2):
    text_1 = [ord(i) for i in text1]
    text_2 = [ord(i) for i in text2]
    return ''.join(chr(a^b) for a, b in zip(text_1, text_2))
```

Figure 2: Ввод импортов и написание функций

Результат выполнения лабораторной работы

Ввод текстов и определение их длины:

```
p1 = "_Звездопад столетия_"
p2 = "Уставший программист"

print(len(p1))
print(len(p2))
```

```
20
20
```

Figure 3: Ввод текстов

Результат выполнения лабораторной работы

Определение шаблонного ключа:

```
key = fun_2(len(p1))
print("Ключ в символьном виде: ", key)
key_16 = fun_1(key)
print("Ключ в шестнадцатиричном виде: ", key_16)
```

```
Ключ в символьном виде:  leXZe5d7I8Jgj2Oj8hys
Ключ в шестнадцатиричном виде:  6c 65 58 5a 65 35 64 37 49 38 4a 67 6a 32 4f 6a 38 68 79 73
```

Figure 4: Определение ключа

Шифрование текстов в символьном и шестнадцатиричном виде по ключу:

```
c1 = fun_3(p1, key)
c2 = fun_3(p2, key)
print("Символьный вид текста 1: ", c1)
print("Символьный вид текста 2: ", c2)

c1_16 = fun_1(c1)
c2_16 = fun_1(c2)
print("Текст 1 в виде шифра: ", c1_16)
print("Текст 2 в виде шифра: ", c2_16)
```

```
Символьный вид текста 1:  3ѲѪѯђЁњЈѹЌjЦШЌѴџѺѐж,
Символьный вид текста 2:  яФКѪїѽќЎiЇЊљљѲѿіЄѐиб
Текст 1 в виде шифра:  33 472 46a 46f 452 401 45a 408 479 40c 6a 426 428 40c 474 45f 47a 450 436 2c
Текст 2 в виде шифра:  44f 424 41a 46a 457 47d 45c 40e 69 407 40a 459 459 472 47f 456 404 450 438 431
```

Figure 5: Шифрование текстов

Результат выполнения лабораторной работы

Расшифровка зашифрованных текстов:

```
decr = fun_3(c1, c2)
print("Расшифрованный текст 1: ", fun_3(decr, p2))
print("Расшифрованный текст 2: ", fun_3(decr, p1))
```

```
Расшифрованный текст 1:  _Звездопад столетия_
Расшифрованный текст 2:  Уставший программист
```

Figure 6: Расшифровка текстов

Выводы

Выводы

1. Изучили теорию по теме однократного гаммирования для кодирования различных исходных текстов одним ключом;
2. Реализовали режим однократного гаммирования на практике, написав программу.