Защита лабораторной работы №7. Элементы криптографии. Однократное гаммирование

Бурдина Ксения Павловна

2022 Oct 19th

RUDN University, Moscow, Russian Federation

Результат выполнения лабораторной работы №7

Цель выполнения лабораторной работы

Цель выполнения лабораторной работы

Освоение на практике применения режима однократного гаммирования.

Теоретические сведения

Теоретические сведения

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Схема однократного гаммирования:

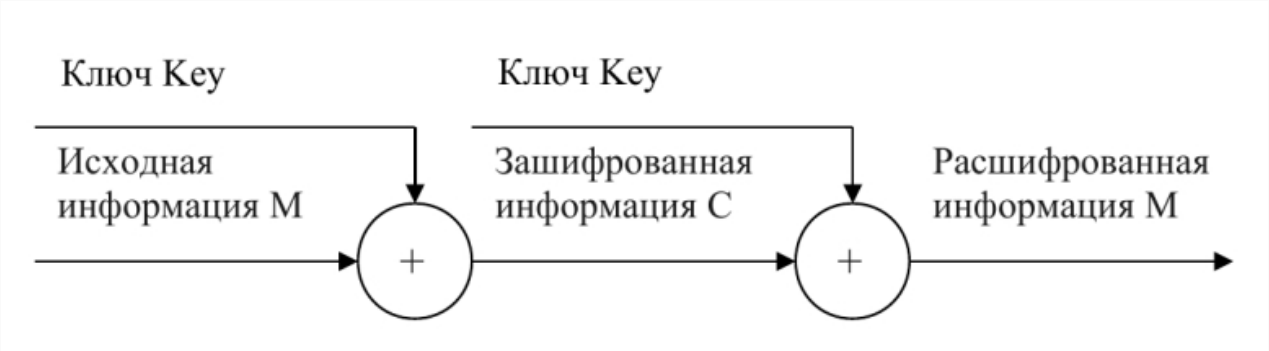

Figure 1: Однократное гаммирование

Теоретические сведения

Задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила:

$$C_i = P_i \oplus K_i$$

Задача нахождения ключа решается так, что обе части равенства необходимо сложить по модулю 2 с P_i:

$$C_i \oplus P_i = P_i \oplus K_i \oplus P_i = K_i$$

$$K_i = C_i \oplus P_i$$

Результат выполнения лабораторной работы

Результат выполнения лабораторной работы

Постановка задачи:

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

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.

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(text, key):
    return ''.join(chr(a^b) for a, b in zip(text, key))

def fun_4(text, encr):
    return ''.join(chr(a^b) for a, b in zip(text, encr))
```

Figure 2: Ввод импортов и написание функций

Результат выполнения лабораторной работы

Листинг и вывод программы для пункта 1:

```
message = 'С Новым Годом, друзья!'
print("Исходное сообщение: ", message)

key = fun_2(len(message))
key_16 = fun_1(key)
print("Сгенерированный ключ: ", key)
print("Ключ в шестнадцатиричном виде: ", key_16)

encr = fun_3([ord(i) for i in message], [ord(i) for i in key])
encr_16 = fun_1(encr)
print("Текст в зашифрованном виде: ", encr_16)
decr = fun_3([ord(i) for i in encr], [ord(i) for i in key])
print("Расшифрованное сообщение: ", decr)
```

```
Исходное сообщение:  С Новым Годом, друзья!
Сгенерированный ключ:  kBs1gtkXKjvGD1MxT7Wwuh
Ключ в шестнадцатиричном виде:  6b 42 73 31 67 74 6b 58 4b 6a 76 47 44 31 4d 78 54 37 57 77 75 68
Текст в зашифрованном виде:  44a 62 46e 40f 455 43f 457 78 458 454 442 479 478 1d 6d 44c 414 474 460 43b 43a 49
Расшифрованное сообщение:  С Новым Годом, друзья!
```

Figure 3: Листинг и вывод задания 1

Результат выполнения лабораторной работы

Листинг и вывод программы для пункта 2:

```
ident_key = fun_4([ord(i) for i in message], [ord(i) for i in encr])
decr_ident_key = fun_3([ord(i) for i in encr], [ord(i) for i in key])
print("Подобранный ключ: ", ident_key)
print("Вариант прочтения открытого текста: ", decr_ident_key)
```

```
Подобранный ключ:  kBs1gtkXKjvGD1MxT7Wwuh
Вариант прочтения открытого текста:  С Новым Годом, друзья!
```

Figure 4: Листинг и вывод задания 2

Выводы

Выводы

1. Изучили теорию по теме однократного гаммирования;
2. Реализовали режим однократного гаммирования на практике, написав программу.