

Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Логинов Сергей

НФИбд-01-18

Цель работы

Освоить на практике применение режима однократного гаммирования

Ход работы

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности двух элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы - это сложение ее элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста.

$$C_i = P_i \oplus K_i$$

$$K_i = C_i \oplus P_i$$

Ход работы

```
from itertools import zip_longest
def gamma_cr(text, key):
    shifr = ''
    for (x, y) in zip_longest(text, key):
        if not x:
            break
        shifr += chr((ord(x) ^ ord(y)))
    return shifr
```

Ход работы

```
text1 = 'привет дорогой друг'
```

```
len(text1)|
```

19

```
key1 = '2134frewghjko568445m'
```

```
len(key1)
```

19

```
shifr1 = gamma_cr(text1, key1)  
print(shifr1)
```

ЙψҒІѓаЕуіbsќҒџÈŦŦŸ

```
len(shifr1)
```

19

```
text2 = gamma_cr(shifr1, key1)  
print(text2)
```

привет дорогой друг

Ход работы

```
key3 = gamma_cr(shifr1, 'привет дорогой враг')  
print(key3)
```

2134frehjko56824Fm

```
print(gamma_cr(shifr1, key3))
```

привет дорогой враг

```
key4 = (gamma_cr('Этот текст из 22 симв', 'С Новым Годом, друзья!'))
```

```
print(key4)  
len(key4)
```

ᄀb#|B KR|дIᄀbvtсГ

22

```
print(gamma_cr('Этот текст из 22 симв', key4))
```

С Новым Годом, друзья!

Контрольные вопросы

1. Поясните смысл однократного гаммирования
2. Перечислите недостатки однократного гаммирования
3. Перечислите преимущества однократного гаммирования
4. Почему длина открытого текста должна совпадать с длиной ключа?
5. Какая операция используется в режиме однократного гаммирования, назовите ее особенности?
6. Как по открытому тексту и ключу получить шифротекст?
7. Как по открытому тексту и шифротексту получить ключ?
8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

Вывод

В ходе лабораторной работы получили практическое знакомство с режимом однократного гаммирования