

Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Каримов Зуфар НПИ-01-18

Содержание

1	Цель работы	3
2	Последовательность выполнения работы	4
3	Контрольные вопросы	6
4	Выводы	8

1 Цель работы

Освоить на практике применение режима однократного гаммирования

2 Последовательность выполнения работы

1. Блок функции для расчетов. (рис. 2.1)

```
Ввод [18]: import string
import random

Ввод [19]: def function1(text):
            return ''.join(hex(ord(i))[2:] for i in text)

            def function2(size):
                return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))

            def function3(text, key):
                return ''.join(chr(a^b) for a,b in zip(text, key))

            def function4(text, encrypt):
                return ''.join(chr(a^b) for a,b in zip(text, encrypt))
```

Figure 2.1: Блок функции для расчетов

2. Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. 2.2)

```
Ввод [20]: message = 'С новым Годом, друзья!'
key = function2(len(message))
hex_key = function1(key)
print("Используем ключ: ", key)
print("Ключ в шестнадцатичном виде: ", hex_key)
encrypt = function3([ord(i) for i in message], [ord(i) for i in key])
hex_encrypt = function1(encrypt)
print("Зашифрованное сообщение: ", hex_encrypt)
decrypt = function3([ord(i) for i in encrypt], [ord(i) for i in key])
print("Расшифрованное сообщение: ", decrypt)

Используем ключ:  zDgLIqM1zYRg6zxGluve19
Ключ в шестнадцатичном виде:  7a 44 67 4c 57 71 4d 31 7a 79 52 67 36 7a 78 47 4e 75 76 65 49 39
Зашифрованное сообщение:  45b 64 45a 472 465 43a 471 11 469 447 466 459 48a 56 58 473 48e 436 441 429 486 18
Расшифрованное сообщение:  С новым Годом, друзья!
```

Figure 2.2: Получение шифротекста

3. Определил ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (рис. 2.3)

```
Ввод [23]: compute_key = function4([ord(i) for i in message], [ord(i) for i in encrypt])
decrypt_compute_key = function3([ord(i) for i in encrypt], [ord(i) for i in key])
print("Исходный ключ: ", key)
print("Вариант прочтения открытого текста: ", decrypt_compute_key)

Исходный ключ: zDgLMqH1zyRg6zXGhuveI9
Вариант прочтения открытого текста: С новым Годом, друзья!
```

Figure 2.3: Прочтение открытого текста

3 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование—метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гаммапоследовательностью и используется для зашифровывания и расшифровывания данных.

2. Перечислите недостатки однократного гаммирования.

Ключ одного размера с сообщением, на один ключ используется только один текст.

3. Перечислите преимущества однократного гаммирования.

Простота и криптостойкость.

4. Почему длина открытого текста должна совпадать с длиной ключа?

Каждый символ текста попарно складывается с символом ключа.

5. Какая операция используется в режиме однократного гаммирования, назовите её особенности?

Сложение по модулю 2. Особенность в симметричности—операция при повторном применении дает исходный результат.

6. Как по открытому тексту и ключу получить шифротекст?

Сложить по модулю 2 каждый символ открытого текста и ключа.

7. Как по открытому тексту и шифротексту получить ключ?

Сложить по модулю 2 каждый символ открытого текста и шифротекста.

8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?

- полная случайность ключа;
- равенство длин ключа и открытого текста;
- однократное использование ключа.

4 Выводы

Освоил на практике применение режима однократного гаммирования.