Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Импортирую библиотеки:

```
import numpy as np
import operator as op
import sys
```

Подаю на вход сообщение:

```
s = "С Новым Годом, друзья!"
```

1. Определю вид шифротекста при известном ключе и известном открытом тексте.
   Функция получает на вход строку, переводит ее в шестнадцатеричную систему счисления. Затем в программе рандомно генерируется ключ. При помощи ключа получаю зашифрованное сообщение в шестнадцатеричной системе счисления. Затем перевожу это сообщение в строковый вид.

```
def encryption(text):
    print("Открытый текст: ", text)

    new_text = []
    for i in text:
        new_text.append(i.encode("cp1251").hex())
    print("\nОткрытый текст в 16-ой системе: ", new_text)

    r = np.random.randint(0, 255, len(text))
    key = [hex(i)[2:] for i in r]

    new_key = []
    for i in key:
            new_key.append(i.encode("cp1251").hex().upper())
    print("\nКлюч в 16-ой системе: ", key)

    xor_text = []
    for i in range(len(new_text)):
        xor_text.append("{:02x}".format(int(key[i], 16) ^ int(new_text[i], 16)))
    print("\nШифротекст в 16-ой системе: ", xor_text)

    en_text = bytearray.fromhex("".join(xor_text)).decode("cp1251")
    print("\nШифротекст: ", en_text)

    return key, xor_text, en_text
```

Результат работы функции:

```
Открытый текст:  С Новым Годом, друзья!

Открытый текст в 16-ой системе:  ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20',
'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']

Ключ в 16-ой системе:  ['9b', 'd5', 'e6', '59', 'c7', '68', 'b1', 'b3', '68', 'e9', '15', '26', '3a', '7e', '66', '68', '9
2', '0', 'df', 'df', 'c5', '11']

Шифротекст в 16-ой системе:  ['4a', 'f5', '2b', 'b7', '25', '93', '5d', '93', 'ab', '07', 'f1', 'c8', 'd6', '52', '46', '8
c', '62', 'f3', '38', '23', '3a', '30']

Шифротекст:  Jx+·%“]“«⍰cИЦRFЊby8#:0
Открытый текст:  С Новым Годом, друзья!

Шифротекст:  Jx+·%“]“«⍰cИЦRFЊby8#:0
```

2. Определю ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. Функция нахождения ключа получает на вход две строки: открытый текст и зашифрованный. Затем она преобразует строки в шестнадцатеричный формат и
выполняет операцию XOR для нахождения ключа.

```python
def find_key(text, en_text):
    print("Открытый текст: ", text)
    print("\nШифротекст: ", en_text)

    new_text = []
    for i in text:
        new_text.append(i.encode("cp1251").hex())
    print("\nОткрытый текст в 16-ой системе: ", new_text)

    tmp_text = []
    for i in en_text:
        tmp_text.append(i.encode("cp1251").hex())
    print("\nШифротекст текст в 16-ой системе: ", tmp_text)

    xor_text = [hex(int(k,16)^int(t,16))[2:] for (k,t) in zip(new_text, tmp_text)]
    print("\nНайденный ключ в 16-ой системе: ", xor_text)
    return xor_text
```

Результат работы функции:

```
Открытый текст в 16-ой системе:  ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20',
'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']

Шифротекст текст в 16-ой системе:  ['4a', 'f5', '2b', 'b7', '25', '93', '5d', '93', 'ab', '07', 'f1', 'c8', 'd6', '52', '4
6', '8c', '62', 'f3', '38', '23', '3a', '30']

Найденный ключ в 16-ой системе:  ['9b', 'd5', 'e6', '59', 'c7', '68', 'b1', 'b3', '68', 'e9', '15', '26', '3a', '7e', '66',
'68', '92', '0', 'df', 'df', 'c5', '11']
Ключ найден верно
```

Проверка:

```python
if k == key:
    print("Ключ найден верно")
else:
    print("Ключ найден неверно")
```

Ответы на контрольные вопросы

1. Поясните смысл однократного гаммирования.
Гаммирование – выполнение операции XOR между элементами гаммы и элементами подлежащего сокрытию текста. Если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и

подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

2. Перечислите недостатки однократного гаммирования.
   Абсолютная стойкость шифра доказана только для случая, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.

3. Перечислите преимущества однократного гаммирования.
   Во-первых, такой способ симметричен, т.е. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение. Во-вторых, шифрование и расшифрование может быть выполнено одной и той же программой. Наконец, Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.

4. Почему длина открытого текста должна совпадать с длиной ключа?
   Если ключ короче текста, то операция XOR будет применена не ко всем элементам и конец сообщения будет не закодирован. Если ключ будет длиннее, то появится неоднозначность декодирования.

5. Какая операция используется в режиме однократного гаммирования, назовите её особенности?
   Наложение гаммы по сути представляет собой выполнение побитовой операции сложения по модулю 2, т.е. мы должны сложить каждый элемент гаммы с соответствующим элементом ключа. Данная операция является симметричной, так как прибавление одной и той же величины по модулю 2 восстанавливает исходное значение

6. Как по открытому тексту и ключу получить шифротекст?
   В таком случае задача сводится к правилу:
   $C_i = P_i \oplus K_i$, т.е. мы поэлементно получаем символы зашифрованного сообщения, применяя операцию исключающего или к соответствующим элементам ключа и открытого текста.

7. Как по открытому тексту и шифротексту получить ключ?
   Подобная задача решается путем применения операции исключающего или к последовательностям символов зашифрованного и открытого сообщений:

   $$K_i = P_i \oplus C_i.$$

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

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

Вывод

В ходе данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

Список литературы

- Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №7