Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Липатникова М.С. группа НФИбд-02-19

Содержание

List of Figures

1 Цель работы

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

2 Выполнение лабораторной работы

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 P1 и P2 в режиме однократного гаммирования (fig. 2.1). Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить(fig. 2.2).

Создала 3 функции: - одна генерирует ключ из ASCII-кодов по количеству букв в сообщении; - вторая делает шифрование в режиме однократного гаммирования: сначала каждая буква текста и ключа изменяется на число из таблицы символов Unicode, представляющее его позицию, потом это число переводится в 16-ную систему. Далее текст возводится в степень ключа - это зашифрованное сообщение; - в третьей функции по двум шифротекстам и тексту-шаблону мы находим позиции, а потом дешифровываем второе сообщение.

```
Ввод [1]:  import random
           import string
```

```
Ввод [2]:  def key_gen(text):
               simb = string.ascii_letters + string.digits
               return ''.join(random.choice(simb) for i in range(len(text)))
           def gamm(text, key):
               text_cypher = [hex(ord(i))[2:] for i in text]
               key_cypher = [hex(ord(i))[2:] for i in key]
               print("Текст в 16-ной системе: ", text_cypher, '\nКлюч в 16-ной системе: ', key_cypher)
               return ''.join(chr(int(a, 16)^int(b, 16)) for a,b in zip (text_cypher, key_cypher))
```

```
Ввод [3]:  text1 = "НаВашисходящийот1204"
           text2 = "ВСеверныйфилиалБанка"
           key = key_gen(text1)
           cypher1 = gamm(text1, key)
           cypher2 = gamm(text2, key)
           print()
           print("Зашифрованный текст1: ", cypher1,'\nКлюч: ', key)
           print("Зашифрованный текст2: ", cypher2,'\nКлюч: ', key)

           Текст в 16-ной системе:  ['41d', '430', '412', '430', '448', '438', '441', '445', '43e', '434', '44f', '449', '438', '439',
           '43e', '442', '31', '32', '30', '34']
           Ключ в 16-ной системе:  ['58', '33', '52', '48', '33', '7a', '66', '77', '34', '6b', '74', '6f', '4b', '7a', '53', '48', '52
           ', '70', '76', '5a']
           Текст в 16-ной системе:  ['412', '421', '435', '432', '435', '440', '43d', '44b', '439', '444', '438', '43b', '438', '430',
           '43b', '411', '430', '43d', '43a', '430']
           Ключ в 16-ной системе:  ['58', '33', '52', '48', '33', '7a', '66', '77', '34', '6b', '74', '6f', '4b', '7a', '53', '48', '52
           ', '70', '76', '5a']

           Зашифрованный текст1:  хЃрѹѻтЧвЊџлЦѳуѭЊcBFn
           Ключ:  X3RH3zfw4ktoKzSHRpvZ
           Зашифрованный текст2:  ъВѧѺІкћмЍЯьєѳъѨљѢэьѪ
           Ключ:  X3RH3zfw4ktoKzSHRpvZ
```

Figure 2.1: Программа

```
Ввод [4]:  def f_tt(cypher1, cypher2, text1):
               tcypher1 = [hex(ord(i))[2:] for i in cypher1]
               tcypher2 = [hex(ord(i))[2:] for i in cypher2]
               print("Шифротекст1 в 16-ной системе: ", tcypher1, '\nШифротекст2 в 16-ной системе: ', tcypher2)
               ttext1 = [hex(ord(i))[2:] for i in text1]
               k = ''.join(chr(int(a, 16)^int(b, 16)) for a,b in zip (tcypher1, tcypher2))
               k = [hex(ord(i))[2:] for i in k]
               P2 = ''.join(chr(int(a, 16)^int(b, 16)) for a,b in zip (k, ttext1))
               return P2
```

```
Ввод [5]:  P2 = f_tt(cypher1, cypher2, text1)
           print()
           print('Текст2: ', P2)

           Шифротекст1 в 16-ной системе:  ['445', '403', '440', '478', '47b', '442', '427', '432', '40a', '45f', '43b', '426', '473', '
           443', '46d', '40a', '63', '42', '46', '6e']
           Шифротекст2 в 16-ной системе:  ['44a', '412', '467', '47a', '406', '43a', '45b', '43c', '40d', '42f', '44c', '454', '473', '
           44a', '468', '459', '462', '44d', '44c', '46a']

           Текст2:  ВСеверныйфилиалБанка
```

```
Ввод [6]:  P1 = f_tt(cypher1, cypher2, text2)
           print()
           print('Текст1: ', P1)

           Шифротекст1 в 16-ной системе:  ['445', '403', '440', '478', '47b', '442', '427', '432', '40a', '45f', '43b', '426', '473', '
           443', '46d', '40a', '63', '42', '46', '6e']
           Шифротекст2 в 16-ной системе:  ['44a', '412', '467', '47a', '406', '43a', '45b', '43c', '40d', '42f', '44c', '454', '473', '
           44a', '468', '459', '462', '44d', '44c', '46a']

           Текст1:  НаВашисходящийот1204
```

Figure 2.2: Программа

3 Вывод

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

4 Список литературы

1. Теоретические материалы курса.