Основы информационной безопасности

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

Демидова Екатерина Алексеевна

Содержание

Список иллюстраций

1 Цель работы

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

2 Задание

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. 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.

3 Теоретические сведения

Гаммиирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст[1]:. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных.

4 Выполнение лабораторной работы

Создадим функции: `key_gen` – отвечает за генерацию случайного ключа(составляется выбором из букв кириллицы больших и малых, символов, цифр), `encryption` – принимает на вход текст и ключ, а затем осуществляет посимвольное сложение по модулю 2:

```
def key_gen(text):
    alph = [chr(i) for i in range(1040,1104)] + [chr(i) for i in range(33,64)]
    key = "".join([random.choice(alph) for i in range(len(text))])
    return key


def encryption(text, key):
    return "".join([chr(ord(key[i])^ord(text[i])) for i in range(len(key))])
```

Сначала зашифруем два сообщения:

```
P1 = "ВЗападныйФилиалБанка"
P2 = "ВСеверныйФилиалБанка"
key = key_gen(P1)
C1 = encryption(P1, key)
C2 = encryption(P2, key)
```

Опишем случай, когда злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить. Предположим, что одна из телеграмм является шаблоном – т.е. имеет текст фиксированный формат, в который вписываются

значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C1 \oplus C2$ (известен вид обеих шифровок). Тогда зная P1 имеем:

$$C1 \oplus C2 \oplus P1 = P1 \oplus P2 \oplus P1 = P2.$$

Проиллюстрируем этот процесс на практике. Применим наши функции к заданному сообщению. Допустим нам известна часть второго сообщения. В цикле `while` в интерактивном режиме будет отгадывать части сообщений, пока не угадаем их полностью:

```
fragment = "ВСев"

msg2 = fragment
c1, c2 = C1, C2
length = len(msg2)
while length <= len(P1):
    C12 = encryption(C1[:length], C2[:length])
    msg1 = encryption(C12, msg2)
    print("Расшифрованный текст:")
    display(msg1 + c1[length:])
    print("Введите продолжение текста: ")
    msg1 += input()
    length = len(msg1)
    display(msg1 + c1[length:])

    msg1, msg2 = msg2, msg1
    c1, c2 = c2, c1
```

В результате получим(рис. 4.1)

```
...  Собщения
...  'ВЗападныйФилиалБанка'
...  'ВСевернЫйФилиалБанка'
...  Зашифрованные сообщения
...  '1a\x00Ќ\r\x07EfГЊ/\x19\x14\x08#Э\x04Ё\x03Ѓ'
...  '1I\x05Ё\x08sEfГЊ/\x19\x14\x08#Э\x04Ё\x03Ѓ'
...  Расшифрованный текст:
...  'ВЗап\r\x07EfГЊ/\x19\x14\x08#Э\x04Ё\x03Ѓ'
...  Введите продолжение текста:
...  'ВЗападEfГЊ/\x19\x14\x08#Э\x04Ё\x03Ѓ'
...  Расшифрованный текст:
...  'ВСеверEfГЊ/\x19\x14\x08#Э\x04Ё\x03Ѓ'
...  Введите продолжение текста:
...  'ВСевернЫЊ/\x19\x14\x08#Э\x04Ё\x03Ѓ'
...  Расшифрованный текст:
...  'ВЗападныЊ/\x19\x14\x08#Э\x04Ё\x03Ѓ'
...  Введите продолжение текста:
...  'ВЗападныйФилиалЭ\x04Ё\x03Ѓ'
...  Расшифрованный текст:
...  'ВСевернЫйФилиалЭ\x04Ё\x03Ѓ'
...  Введите продолжение текста:
...  'ВСевернЫйФилиалБанка'
...  Расшифрованный текст:
...  'ВЗападныйФилиалБанка'
```

Рис. 4.1: Результаты работы программы

5 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Предположим, что одна из телеграмм является шаблоном – т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C1 \oplus C2$ (известен вид обеих шифровок). Тогда зная P1 имеем:

$$C1 \oplus C2 \oplus P1 = P1 \oplus P2 \oplus P1 = P2.$$

2. Что будет при повторном использовании ключа при шифровании текста?

Текст вернется к исходному виду.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

К обоим текстам применяется один и тот же ключ.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Главным недостатком является повышение уязвимости. Если злоумышленник узнает один из исзодных текстов или даже его часть, то он может узнать и второй текст.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Ключи могут занимать большое количество памяти и долго генерироваться, поэтому использование одного ключа оптимизирует шифрование. Также это упрощает дешифровку.

6 Выводы

В результате выполнения работы были освоены практические навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

Список литературы

1. Ященко В. В. Введение в криптографию. МЦНМО, 2017. 349 с.