Отчет по лабораторной работе №8

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

Смородова Дарья Владимировна

2022 Oct 29th

Содержание

List of Tables

List of Figures

1 Цель работы

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

2 Задание 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 P_1 и P_2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C_1 и C_2 обоих текстов P_1 и P_2 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 Теоретическое введение[1]

Исходные данные: Две телеграммы Центра: P1 = НаВашисходящийот1204 P2 = ВСеверныйфилиалБанка Ключ Центра длиной 20 байт: K = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54 Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой ниже.

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K$$

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR:

$$1 \oplus 0 = 1, 1 \oplus 1 = 0$$

получаем:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст

[1] Методические материалы к лабораторной работе

фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C_1 \oplus C_2$ (известен вид обеих шифровок). Тогда зная P_1 и учитывая формулу выше, имеем:

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$

Таким образом, злоумышленник получает возможность определить те символы сообщения P_2, которые находятся на позициях известного шаблона сообщения P_1. В соответствии с логикой сообщения P_2, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения P_2. Затем вновь используется последняя формула с подстановкой вместо P_1 полученных на предыдущем шаге новых символов сообщения P_2. И так далее.

Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

4 Выполнение лабораторной работы

1. Напишем на Python функцию шифрования (рис. 4.1):

Ввод [12]:
```
import numpy as np
def cript(s1, s2):
    print("Строка 1 в 10 сс: ", s1)
    array1 = []
    for i in s1:
        array1.append(i.encode('cp1251').hex())
    print("Строка 1 в 16 сс: ", *array1)
    array2 = []
    print("Строка 2 в 10 сс: ", s2)
    for i in s2:
        array2.append(i.encode('cp1251').hex())
    print("Строка 2 в 16 сс: ", *array2)

    key = np.random.randint(0,255,len(s1))
    key_16 = [hex(i)[2:] for i in key]
    print ("Ключ в 16 сс: ", *key_16)
    array3 = []
    for i in range(len(array1)):
        array3.append("{:02x}".format(int(array1[i], 16) ^ int(key_16[i], 16)))
    print("Зашифрованный текст строки 1 в 16 сс:", *array3)
    array4 = []
    for i in range(len(array2)):
        array4.append("{:02x}".format(int(array2[i], 16) ^ int(key_16[i], 16)))
    print("Зашифрованный текст строки 2 в 16 сс:", *array4)

    text1 = bytearray.fromhex(''.join(array3)).decode('cp1251')
    print("Зашифрованный текст строки 1: ", text1)
    text2 = bytearray.fromhex(''.join(array4)).decode('cp1251')
    print("Зашифрованный текст строки 2: ", text2)
    return key_16, text1, text2
```

Figure 4.1: Функция шифрования данных

2. Посмотрим работу данной функции (рис. 4.2):

Ввод [24]:
```
s1 = "НаВашисходящийот1204"
s2 = "ВСеверныйфилиалБанка"
key, text1, text2 = cript(s1, s2)
```

```
Строка 1 в 10 сс:  НаВашисходящийот1204
Строка 1 в 16 сс:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
Строка 2 в 10 сс:  ВСеверныйфилиалБанка
Строка 2 в 16 сс:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
Ключ в 16 сс:  85 25 6a c d8 3f a5 f 8e d3 92 31 4 12 49 8c d4 5e bb e6
Зашифрованный текст строки 1 в 16 сс: 48 c5 a8 ec 20 d7 54 fa 60 37 6d c8 ec fb a7 7e e5 6c 8b d2
Зашифрованный текст строки 2 в 16 сс: 47 f4 8f ee 3d cf 48 f4 67 27 7a da ec f2 a2 4d 34 b3 51 06
Зашифрованный текст строки 1:  НЕЁм ЧТъ`7mИмы§~c1‹T
Зашифрованный текст строки 2:  GфЦо=ПНфg'zЪмтўM4iQ
```

Figure 4.2: Результат работы функции, шифрующей данные

3. Напишем функцию дешифровки, которая возвращает вторую строку, получив на вход первую строку и обе защифрованные строки (рис. 4.3):

Ввод [16]:
```
def foundtext(text1, text2, new_text):
    print("Текст: ", new_text)
    print("Зашифрованный текст строки 1: ", text1)
    print("Зашифрованный текст строки 2: ", text2)
    text1_16 = []
    for i in text1:
        text1_16.append(i.encode('cp1251').hex())
    print ("Текст строки 1 в 16 сс: ", *text1_16)
    text2_16 = []
    for i in text2:
        text2_16.append(i.encode('cp1251').hex())
    print ("Текст строки 2 в 16 сс: ", *text2_16)

    array1 = []
    for i in new_text:
        array1.append(i.encode('cp1251').hex())
    print("Текст в 16 сс: ", *array1)

    array2 = []
    array3 = []
    for i in range(len(array1)):
        array2.append("{:02x}".format(int(text1_16[i], 16) ^ int(text2_16[i], 16)))
        array3.append("{:02x}".format(int(array2[i], 16) ^ int(array1[i], 16)))

    print("Текст 2 в 16 сс: ", *array3)
    text_2 = bytearray.fromhex(''.join(array3)).decode('cp1251')
    print("Текст 2: ", text_2)
    return text_2
```

Figure 4.3: Функция, дешифрующая данные

4. Посмторим на результаты функции дешифрования(рис. 4.4):

Ввод [25]:
```
t2 = foundtext(text1, text2, s1)
```
```
Текст:  НаВашисходящийот1204
Зашифрованный текст строки 1:  нЕЁм ЧТъ`7тИмы$~e1‹Т
Зашифрованный текст строки 2:  GфЦо=ПНфg'zЪмтўМ4iQ
Текст строки 1 в 16 сс:  48 c5 a8 ec 20 d7 54 fa 60 37 6d c8 ec fb a7 7e e5 6c 8b d2
Текст строки 2 в 16 сс:  47 f4 8f ee 3d cf 48 f4 67 27 7a da ec f2 a2 4d 34 b3 51 06
Текст в 16 сс:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
Текст 2 в 16 сс:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
Текст 2:  ВСеверныйфилиалБанка
```

Ввод [26]:
```
t1 = foundtext(text1, text2, s2)
```
```
Текст:  ВСеверныйфилиалБанка
Зашифрованный текст строки 1:  нЕЁм ЧТъ`7тИмы$~e1‹Т
Зашифрованный текст строки 2:  GфЦо=ПНфg'zЪмтўМ4iQ
Текст строки 1 в 16 сс:  48 c5 a8 ec 20 d7 54 fa 60 37 6d c8 ec fb a7 7e e5 6c 8b d2
Текст строки 2 в 16 сс:  47 f4 8f ee 3d cf 48 f4 67 27 7a da ec f2 a2 4d 34 b3 51 06
Текст в 16 сс:  c2 d1 e5 e2 e5 f0 ed fb e9 f4 e8 eb e8 e0 eb c1 e0 ed ea e0
Текст 2 в 16 сс:  cd e0 c2 e0 f8 e8 f1 f5 ee e4 ff f9 e8 e9 ee f2 31 32 30 34
Текст 2:  НаВашисходящийот1204
```

Figure 4.4: Результат работы функции, дешифрующей данные

5 Контрольные вопросы

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

   Чтобы определить один из текстов, зная другой, необходимо вопсользоваться следующей формулой: $C_1 \oplus C_2 \oplus + P_1 = P_1 \oplus P_2 \oplus + P_1 = P_2$, где C_1 и C_2 - шифротексты. Т.е. ключ в данной формуле не используется.

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

   При повторном использовании ключа при шифровании текста получим исходное сообщение.

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

   Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по следующей формуле:

   $$C_1 = P_1 \oplus + K$$

   $$C_2 = P_2 \oplus + K,$$

   где C_i - шифротексты, P_i - открытые тексты, K - единый ключ шифровки

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Во-первых, имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа. Во-вторых, зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения P_2, которые находятся на позициях известного шаблона сообщения P_1.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

   Такой подход помогает упростить процесс шифрования и дешифровки. Также, при отправке сообщений между 2-я компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

6 Выводы

В ходе выполнения данной лабораторной работы, мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

7 Список литературы

1. Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН”