Лабораторная работа №8

Лукьянова Ирина Владимировна, НФИбд-02-19

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.[1]

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

2 Теоретические сведения

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 Выполнение лабораторной работы

Добавляем необходимые библиотеки и создаем функцию генерации ключа. Затем создаем функцию перевода в 16 строку и переводим ключ, с помощью этой функции(рис. 3.1)

Figure 3.1: Код

Создаем функцию сложения по модулю 2 (XOR) для нее нам нужна еще одна функция, которая переводит наши символы в числа.(рис. 3.2)

```
[9]: def f3(t,k): #XOR
         a = []
         for (i,j) in zip(t,k):
             a.append(chr(i^j))
         return a

     def for16(a): #превращаем символы в числа
         f = []
         for i in a:
             f.append(ord(i))
         return f

[10]: C1 = f3(for16(P1), for16(key))
      np.array(C1)

[10]: array(['Ю', 'j', 'ь', 'È', 'Й', 'э', 'a', 'Ў', 'ц', 'ќ', 'Оу', 'Ц', 'ш',
             'ъ', 'ш', 'a', 'd', 'y', 'D', 'q'], dtype='<U1')

[11]: C2 = f3(for16(P2), for16(key))
      np.array(C2)

[11]: array(['ж', 'щ', 'ѓ', 'Ђ', 'Ў', 'е', 'ь', 'Оу', 'j', 'Ъ', 'Ц', 'ѓ', 'ш',
             'Ш', 'э', 'Ъ', 'ю', 'Ў', 'ю', 'v'], dtype='<U1')
```

Figure 3.2: Код 2

В итоге получаем следующие данные: (рис. 3.3)

```
[13]: print("Открытый текст:\nP1 = ", P1, "\nP2 = ", P2)
      print("Ключ: ", ''.join(key))
      print("Ключ в 16: ", ' '.join(key16))
      print("Шифр:\nC1 = ", ''.join(C1), "\nC2 = ", ''.join(C2))

      Открытый текст:
      P1 =  НаВашисходящийот1204
      P2 =  ВСеверныйфилиалБанка
      Ключ:  yhH0Euq3ah7FpPvrUKtE
      Ключ в 16:  79 68 48 30 45 75 71 33 61 68 37 46 70 50 76 72 55 4b 74 45
      Шифр:
      C1 =  ЮjњЁЙэаЎцќОуЦшъшadyDq
      C2 =  жщѓЂЎеьОуjЪЦѓшШэЪюЎюv
```

Figure 3.3: Вывод данных

Далее мы используем уже написанные функции для того, чтобы расшифровать текст без ключа: (рис. 3.4)

```
[14]: C = f3(for16(C1), for16(C2))
      np.array(C2)

[14]: array(['ж', 'щ', 'ѓ', 'Ђ', 'Ў', 'е', 'ь', 'Оу', 'j', 'Ъ', 'Ц', 'ѓ', 'ш',
             'Ш', 'э', 'Ъ', 'ю', 'Ў', 'ю', 'v'], dtype='<U1')

[15]: p_1 = f3(for16(C), for16(P2))
      np.array(p_1)

[15]: array(['Н', 'а', 'В', 'а', 'ш', 'и', 'с', 'х', 'о', 'д', 'я', 'щ', 'и',
             'й', 'о', 'т', '1', '2', '0', '4'], dtype='<U1')

[16]: p_2 = f3(for16(C), for16(P1))
      np.array(p_2)

[16]: array(['В', 'С', 'е', 'в', 'е', 'р', 'н', 'ы', 'й', 'ф', 'и', 'л', 'и',
             'а', 'л', 'Б', 'а', 'н', 'к', 'а'], dtype='<U1')

[17]: print("C1 XOR C2: ", ''.join(C))
      print("P1 = C1 XOR C2 XOR P2: ", ''.join(p_1))
      print("P2 = C1 XOR C2 XOR P1: ", ''.join(p_2))

      C1 XOR C2:  '}x|pwr     SЁЦЊЄ
      P1 = C1 XOR C2 XOR P2:  НаВашисходящийот1204
      P2 = C1 XOR C2 XOR P1:  ВСеверныйфилиалБанка
```

Figure 3.4: Вывод данных

Для этого мы используем сложение по модулю 2 между шифротекстами, далее повторяем операцию с одним из открытых текстов. В итоге получаем второй расшифрованный текст. Данные операции также действуют и для второго текста, что я и демонстрирую на рисунке (рис. 3.4).

4 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа? Сложить по модулю 2 оба шифротекста и известный второй текст. В результате получим расшифрованный первый текст, аналогично и для второго текста.

2. Что будет при повторном использовании ключа при шифровании текста? Если оба текста зашифрованы одним ключом, то злоумышленнику легче их взломать.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? Оба открытхих текста шифруются одним ключом.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов. Большая вероятность взлома.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов. Используется всего один ключ, что, к сожалению, является больше недостатком, чем преимуществом.

5 Выводы

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

6 Список литературы

1. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом. / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 7 с.
2. Руководство по оформлению Markdown.