

Защита лабораторной работы №8

Информационная безопасность

Данзанова С. З.

2024

Российский университет дружбы народов, Москва, Россия

Докладчик

- Данзанова Саяна Зоригтоевна
- Студентка группы НПИбд-01-21
- Студ. билет 1032217624
- Российский университет дружбы народов

Цель лабораторной работы

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

Теоретическая справка (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 0B B2 70 54

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии с так называемой «схемой шифрования двух различных текстов одним ключом».

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$C1 = P1 \oplus K, C2 = P2 \oplus K \quad (8.1)$$

Теоретическая справка (3)

Открытый текст можно найти в соответствии с (8.1), зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства (8.1) складываются по модулю 2. Тогда с учётом свойства операции XOR

$$1 \oplus 1 = 0, 1 \oplus 0 = 1 \quad (8.2)$$

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 $P1$ и учитывая (8.2), имеем:

$$C1 \oplus C2 \oplus P1 = P1 \oplus P2 \oplus P1 = P2 \quad (8.3)$$

Теоретическая справка (4)

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 (8.3) 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.

Задача лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитав 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.

Решение задачи лабораторной работы

Для решения задачи написан программный код:

```
✓ [31] # Импорт библиотек
      import random
      import string

✓ [19] # Функция сложения двух строк по модулю
      def xor_text_f(text1, text2):
          if len(text1) != len(text2): return "Ошибка: тексты разной длины"
          xor_text = ''
          for i in range(len(text1)):
              xor_text_symbol = ord(text1[i]) ^ ord(text2[i])
              xor_text += chr(xor_text_symbol)
          return xor_text

✓ [32] P1 = "НаВашисходящийот1204"
      P2 = "ВСеверныйфилиалБанка"

      print("Исходный текст P1:", P1)
      print("Исходный текст P2:", P2)
```

➡ Исходный текст P1: НаВашисходящийот1204
Исходный текст P2: ВСеверныйфилиалБанка

Рис. 1: Программный код приложения, реализующего режим однократного

Решение задачи лабораторной работы

```
✓ [33] random.seed(20)
0 сек. key = ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(len(P1)))
print("Ключ:", key)

➡ Ключ: 5URYX45jqR025g3uk5kb

✓ [34] C1 = xor_text_f(P1, key)
0 сек. C2 = xor_text_f(P2, key)

print("Зашифрованный текст C1:", C1)
print("Зашифрованный текст C2:", C2)

➡ Зашифрованный текст C1: ШернАКВЯЯАёоййизз[V
Зашифрованный текст C2: ЧVажяVJСшЖVльйїїжкoJёђ

✓ [35] P1_xor_P2 = xor_text_f(C1, C2)
0 сек. print("Результат сложения исходных текстов P1 и P2:", P1_xor_P2)

➡ Результат сложения исходных текстов P1 и P2: 00'0}x|00pwr 0SÉЦЬЄ
```

Рис. 2: Программный код приложения, реализующего режим однократного гаммирования)

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

Список литературы. Библиография

[0] Методические материалы курса