Отчёт по лабораторной работе №8

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

Волков Тимофей Евгеньевич

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 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. 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).

Функции (fig. 2.1):

hex_ — перевод в шестнадцатиричную систему.

gen_key — генерирует рандомный ключ.

encrypt — шифрует текст.

decrypt — дешифрует тескт.

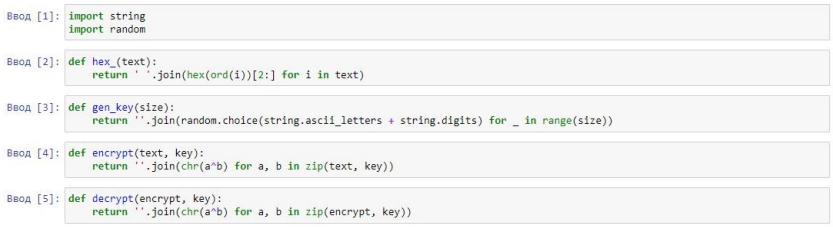

Figure 2.1: Функции

Ввод [9]:
```
P1 = 'НаВашисходящийот1204'
P2 = 'ВСеверныйфилиалБанка'

key = gen_key(len(P1))
hex_key = hex_(P1)

print("Ключ: ", hex_key)

P1_encrypt = encrypt([ord(i) for i in P1], [ord(i) for i in key])
P1_hex_encrypt = hex_(P1_encrypt)

P2_encrypt = encrypt([ord(i) for i in P2], [ord(i) for i in key])
P2_hex_encrypt = hex_(P2_encrypt)

print("Зашифрованное сообщение C1: ", P1_hex_encrypt)

print("Зашифрованное сообщение C2: ", P2_hex_encrypt)

C = encrypt([ord(i) for i in P1_encrypt], [ord(i) for i in P2_encrypt])

P1_decrypt = decrypt([ord(i) for i in C], [ord(i) for i in P2])

print("Расшифрованное сообщение P1: ", P1_decrypt)

P2_decrypt = decrypt([ord(i) for i in C], [ord(i) for i in P1])

print("Расшифрованное сообщение P2: ", P2_decrypt)
```

```
Ключ:  41d 430 412 430 448 438 441 445 43e 434 44f 449 438 439 43e 442 31 32 30 34
Зашифрованное сообщение C1:  45c 445 46a 440 471 475 430 40b 473 446 427 40a 47d 440 47f 418 43 68 5e 7a
Зашифрованное сообщение C2:  453 454 44d 442 40c 40d 44c 405 474 436 450 478 47d 449 47a 44b 442 467 454 47e
Расшифрованное сообщение P1:  НаВашисходящийот1204
Расшифрованное сообщение P2:  ВСеверныйфилиалБанка
```

Figure 2.2: Вывод результата

3 Выводы

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

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 декодировать первый текст используя полученное значение и известный второй текст.

2. Что будет при повторном использовании ключа при шифровании текста?
   Оба текста, шифрованные одним ключем будут подвержены риску взлома.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?
   Шифруем оба текста одним ключем.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.
   Подверженость риску взлома.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.
   Используется меньше ключей.