Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Соболевский Денис Андреевич

Содержание

Список иллюстраций

Цель работы

Освоить на практике применение режима однократного гаммирования.

Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Теоретическое введение

- Шифрование — это процесс кодирования информации с целью предотвращения несанкционированного доступа. В случае кражи или утечки зашифрованные данные будут недоступны для прочтения без соответствующего ключа.
- Гаммирование - преобразование исходного (открытого) текста, при котором символы исходного текста складываются (по модулю, равному мощности алфавита) с символами псевдослучайной последовательности, вырабатываемой по определенному правилу.

Выполнение лабораторной работы

1. Импортируем модули.

Рис. 1:

2. Напишем функцию для преобразования данных в шестнадцатеричный формат.

Рис. 2:

3. Напишем функцию для генерации ключа.

Рис. 3:

```
[14]: def encoder(text, key):
          return "".join(chr(a^b) for a, b in zip (text, key))
```

Рис. 4:

```
[17]: msg = "С новым годом, друзья!"
      key = gen_key(len(msg))
      hex_key = toHex(key)
      print("Ключ: ", hex_key)
      enc_text = encoder([ord(i) for i in msg], [ord(i) for i in key])
      hex_text = toHex(enc_text)
      print("Зашифрованное сообщение: ", hex_text)
      decr_text = encoder([ord(i) for i in enc_text], [ord(i) for i in key])
      print("Расшифрованоое сообщение: ", decr_text)

Ключ:  69 64 36 61 6b 7a 30 74 48 61 4a 65 58 39 5a 4a 43 46 32 53 61 62
Зашифрованное сообщение:  448 44 40b 45f 459 431 40c 54 47b 45f 47e 45b 464 15 7a 47e 403 405 405 41f 42e 43
Расшифрованоое сообщение:  С новым годом, друзья!
```

Рис. 5:

4. Реализуем функцию для кодирования и декодирования данных.

5. Закодируем и декодируем сообщение “С Новым годом, друзья!”.

6. Получим ключ, с помощью которого получим сообщение “С Новым годом, коллега”, вместо “С Новым годом, друзья!” при декодировании. Воспользуемся симметричностью кодирования.

```
[18]: new_msg = "С новым годом, коллега"

      key = encoder([ord(i) for i in enc_text], [ord(i) for i in new_msg])
      print("Ключ: ", toHex(key))

Ключ:  69 64 36 61 6b 7a 30 74 48 61 4a 65 58 39 5a 44 3d 3e 3e 2a 1d 473
```

Рис. 6:

Выводы

В данной лабораторной работе было освоено на практике применение режима однократного гаммирования.

Список литературы

[1] https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/shifrovaniye/

[2] https://www.finam.ru/publications/item/gammirovanie-20230628-2028/