Презентация к лабораторной работе 7

Информационная безопасность компьютерных сетей

Еленга Невлора Люглеш.

21 октября 2023

Докладчик

:::::::::::::: {.columns align=center} ::: {.column width="70%"}

- Еленга Невлора Люглеш
- Студент 4-го курса
- Группа НКНбд-01-20
- Российский университет дружбы народов
- 1032205073
- https://github.com/Newlora501

Актуальность

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Шифрование в режиме однократного гаммирования – это один из методов симметричного шифрования, который используется для защиты информации от несанкционированного доступа.

Шифрование в режиме однократного гаммирования – это метод симметричного шифрования, в котором побитово складывается (по модулю 2) открытый текст с ключом-гаммой.

Ключ-гамма – это случайный битовый набор, который используется только для зашифрования одного сообщения и должен быть равен или более длинным, чем сам текст. Ключ-гамма порождается с помощью генератора случайных чисел и не должен быть известен злоумышленнику.

Как это работает?

Для шифрования в режиме однократного гаммирования мы используем операцию побитового XOR (исключающее ИЛИ), которая имеет следующую таблицу истинности:

a	b	a XOR b
0	0	0
0	1	1
1	0	1
1	1	0

Рис.1.1

Цели и задачи

- Освоить на практике применение режима одно кратного гаммирования .

- Описание программы

- Запуск программы

Материалы и методы

- Python

- Библотека Numpy

Результаты

```
Ввод [36]: raw = "С Новым Годом, друзья!"

Ввод [37]: key1 = gen_key(raw)

Ввод [38]: ct = Crypt(raw, key1)

Open Text: С Новым Годом, друзья!
Hex Open Text:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff
21
Key:  22 eb 31 7d 8e 9b e3 b1 26 71 91 7a 0 94 b1 fa 19 35 38 da b0 b1
Hex Crypted Text:  f3 cb fc 93 6c 60 0f 91 e5 9f 75 94 ec b8 91 1e e9 c6 df 26
4f 90
Crypted Text:уль“l`▯‘eцu”мё‘▯ийя&Oђ

Ввод [39]: dct = Crypt(ct, key1)

Open Text: уль“l`▯‘eцu”мё‘▯ийя&Oђ
Hex Open Text:  f3 cb fc 93 6c 60 0f 91 e5 9f 75 94 ec b8 91 1e e9 c6 df 26 4f
90
Key:  22 eb 31 7d 8e 9b e3 b1 26 71 91 7a 0 94 b1 fa 19 35 38 da b0 b1
Hex Crypted Text:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc
ff 21
Crypted Text:С Новым Годом, друзья!

Ввод [ ]:
```

Рис. 1.1.

```
Ввод [41]: key2 = find_key(raw, ct)

Open Text: С Новым Годом, друзья!
Crypted Text: уль“l`▯‘eцu”мё‘▯ийя&Oђ
Hex Open Text:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
Hex Crypted Text:  f3 cb fc 93 6c 60 0f 91 e5 9f 75 94 ec b8 91 1e e9 c6 df 26 4f 90
key  22 eb 31 7d 8e 9b e3 b1 26 71 91 7a 0 94 b1 fa 19 35 38 da b0 b1

Ввод [43]: key3 = find_key("С Новым Годом, друзья!", ct)

Open Text: С Новым Годом, друзья!
Crypted Text: уль“l`▯‘eцu”мё‘▯ийя&Oђ
Hex Open Text:  d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
Hex Crypted Text:  f3 cb fc 93 6c 60 0f 91 e5 9f 75 94 ec b8 91 1e e9 c6 df 26 4f 90
key  22 eb 31 7d 8e 9b e3 b1 26 71 91 7a 0 94 b1 fa 19 35 38 da b0 b1
```

Рис.1.2