Презентация к лабораторной работе 7

Элементы криптографии. Однократное гаммирование

Саттарова В.В.

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Саттарова Вита Викторовна
- студент НФИбд-02-20, 1032201655
- Российский университет дружбы народов

Вводная часть

Актуальность и прагматика

- Практические навыки применения шифрования позволяют обеспечить лучшую безопасность информации в системе

Цели

- Изучить основы криптографии.
- Освоить на практике применение режима однократного гаммирования.

Задачи

- Выполнить все пункты, указанные в методических рекомендациях к лабораторной работе.
- Выполняя задания, познакомиться с основами криптографии.
- Выполняя задания, изучить однократное гаммирование.
- Написать отчёт, проанализировав результаты, полученные в ходе выполнения лабораторной работы.

Контекст и его изменение

Ввод [16]:
```
import random as rd
```

Ввод [17]:
```
# строка
message = "С Новым Годом, друзья!"
```

Ввод [18]:
```
# перевод в 16
def hex_string(mes):
    return " ".join([hex(ord(elem))[2:] for elem in mes])
```

Ввод [19]:
```
# ключ
def make_key(mes):
    base = "abcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчшщъыьэюя0123456789"
    return "".join([rd.choice(base) for i in range(len(mes))])
```

Ввод [20]:
```
# кодирование
def coding(mes, key):
    return "".join(chr(ord(mes[i]) ^ ord(key[i])) for i in range(len(mes)))
```

Рис. 1: Функции

Порт и контекст

Ввод [30]:
```
main_key = make_key(message)
encoded = coding(message, main_key)
decoded = coding(encoded, main_key)
```

Ввод [31]:
```
print(message)
print(main_key)
print(encoded)
print(decoded)
```

```
С Новым Годом, друзья!
хлъвтарк0хбоьбвqа5ві8ы
dЛ̄p{|КУц□ёрНВхрЎ□Хў̄Х
С Новым Годом, друзья!
```

Ввод [36]:
```
# пример с неверным ключом
new_key = make_key(message)
coding(encoded, new_key)
```

Out[36]:
```
'ёЗ̲0еькы9ы\x0сиЊ\x1aV]VoЌ0\x18@T'
```

Ввод [37]:
```
coding(message, encoded)
```

Out[37]:
```
'хлъвтарк0хбоьбвqа5ві8ы'
```

Результаты

Результаты

- Изучены основы криптографии.
- Освоено на практике применение режима однократного гаммирования.
- Написан отчёт к лабораторной работе.