Информационная безопасность

Презентация к лабораторной работе № 7

Мерич Дорук Каймакджыоглу.

21/10/2023

Информация

Докладчик

- Мерич Дорук Каймакджыоглу
- Студент
- НКНбд-01-20
- Российский университет дружбы народов
- 1032204917
- https://github.com/dorukme123

Объект и предмет исследования

- № 7. Элементы криптографии. Однократное гаммирование

```python
if __name__ == "__main__":
    import string
    text = input("Enter the text you want to encrypt: ")
    key = generate_random_key(text)
    encrypted_text = encrypt(text, key)

    print(f"Original Text: {text}")
    print(f"Encrypted Text: {encrypted_text}")
    print(f"Key: {key}")

    decrypted_text = decrypt(encrypted_text, key)
    print(f"Decrypted Text: {decrypted_text}")
```

Цели и задачи

- Освоить на практике применение режима однократного гаммирования.

```python
def generate_random_key(text):
    key = ''.join(random.choice(string.ascii_letters) for _ in range(len(text)))
    return key

def encrypt(text, key):
    encrypted_text = ''.join(chr(ord(text[i]) ^ ord(key[i])) for i in range(len(text)))
    return encrypted_text

def decrypt(encrypted_text, key):
    decrypted_text = ''.join(chr(ord(encrypted_text[i]) ^ ord(key[i])) for i in range(len(encrypted_text)))
    return decrypted_text
```

- 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.

Материалы и методы

- LaTex

- Процессор **pandoc** для входного формата Markdown

- Результирующие форматы
  - **pdf**

  - **docx**

- Автоматизация процесса создания: **Makefile**

Результаты

- Я освоил на практике применение режима однократного гаммирования.

```
Enter the text you want to encrypt: штирлиц - вы герой!
Original Text: штирлиц - вы герой!
Encrypted Text: IзьЃёмMX`рчPMѧЛийђV
Key: NutCjQZxMPukmTSxcbw
Decrypted Text: штирлиц - вы герой!
PS C:\Users\Meric>
Enter the text you want to encrypt: штирлиц - вы болван!
Original Text: штирлиц - вы болван!
Encrypted Text: ИÈывґèJRkMŸиVѧѲючЧЄѾ`
Key: PBsrhhNrFmDsvVEuuTCA
Decrypted Text: штирлиц - вы болван!
PS C:\Users\Meric>
```

Итог работы

- Получено **pdf** из report.md

- Получено **docx** из report.md

- Получено **html** из presentation.md
- Получено **pdf** из presentation.md
- Получено **docx** из presentation.md
- Запись отчета выложен в youtube.com
- Запись презентация выложен в youtube.com

- Запись отчета выложен в rutube.com
- Запись презентация выложен в rutube.com
- Работа выложена в респоситории в github.com
- CHANGELOG.md создано
- Версия на работе создано