Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Дорофеева А.Т.

21 октября 2023

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Дорофеева Алёна Тимофеевна
- студент группы НПИбд-01-20
- Российский университет дружбы народов им. Патриса Лумумбы
- 1032201392@pfur.ru
- https://github.com/DorofeevaAT/study_2022-2023_infosec

Вводная часть

Актуальность

- Криптография – это важнейший инструмент кибербезопасности, она обеспечивает дополнительный уровень защиты, позволяет сохранить конфиденциальность данных и предотвращает их перехват киберпреступниками

Объект и предмет исследования

- Принцип однократного гаммирования

Цели и задачи

1. Изучить принцип однократного гаммирования
2. Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования

Материалы и методы

- Однократное гаммирование

Выполнение работы

Функция кодирования

```python
# Функция для шифрования текста
def encrypt(text, gamma):
    result = ""
    gamma_index = 0

    for char in text:
        if char in alphabet:
            char_index = alphabet[char]
            gamma_char = gamma[gamma_index]
            gamma_index = (gamma_index + 1) % len(gamma)
            gamma_index = gamma_index if gamma_char in alphabet else 0
            gamma_index = 0 if gamma_char not in alphabet else gamma_index
            char_index = (char_index + alphabet[gamma_char]) % 33
            result += alphabet_reversed[char_index]
        else:
            result += char  # Если символ не из алфавита, оставляем без изменений

    return result
```

Функция декодирования

```python
# Функция для дешифрования текста
def decrypt(text, gamma):
    result = ""
    gamma_index = 0

    for char in text:
        if char in alphabet:
            char_index = alphabet[char]
            gamma_char = gamma[gamma_index]
            gamma_index = (gamma_index + 1) % len(gamma)
            gamma_index = gamma_index if gamma_char in alphabet else 0
            gamma_index = 0 if gamma_char not in alphabet else gamma_index
            char_index = (char_index - alphabet[gamma_char]) % 33
            result += alphabet_reversed[char_index]
        else:
            result += char  # Если символ не из алфавита, оставляем без изменений

    return result

encrypted_text = encrypt(text, gamma)
decrypted_text = decrypt(encrypted_text, gamma)
```

Работа программы

```
Введите гамму (на русском языке без пробелов): привет
Введите текст для шифрования: этобаза
Зашифрованный текст: ндшдёыр
Расшифрованный текст: этобаза
```

Результаты

Результат

1. Изучен принцип однократного гаммирования
2. Разработано приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования

Вывод

Вывод

Я освоила на практике применение режима однократного гаммирования. Разработала приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.