Лабораторная работа №3

Презентация

Миличевич Александра

15 февраля 2025

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель работы

Познакомится с способом шифрования гаммирование

Задание

Задание

1. Реализовать алгоритм шифрования гаммированием конечной гаммой.

Гаммирование — это метод шифрования, который использует псевдослучайную последовательность битов, называемую гаммой, для преобразования открытого текста в зашифрованный. Этот метод обеспечивает высокую степень безопасности, так как каждая битовая позиция открытого текста изменяется в зависимости от соответствующего бита гаммы. Гаммирование часто применяется в криптографии для защиты данных, так как оно позволяет эффективно скрывать информацию от несанкционированного доступа.

Гаммирование находит широкое применение в современных системах шифрования, таких как протоколы передачи данных и защищенные коммуникации, обеспечивая высокий уровень конфиденциальности и защиты информации от несанкционированного доступа.

Выполнение лабораторной работы

Шифрование гаммированием (одноразовый блокнот) на русском языке

Этот код реализует шифрование гаммированием для русского языка, также известное как шифрование с использованием одноразового блокнота.

Функция `gamming_cipher_encrypt_ru(text, gamma)`
Эта функция выполняет шифрование текста с помощью гаммирования.

- **Вход:**
  - `text`: Строка - текст для шифрования (русский язык).
  - `gamma`: Строка - гамма (ключ) для шифрования (русский язык).
- **Выход:** Строка - зашифрованный текст (русский язык).

```python
import random

def gamming_cipher_encrypt(text, gamma):
    """
    Шифрует текст с использованием метода шифрования гаммированием (одноразовый блокнот).
    Args:
        text (str): Текст для шифрования.
        gamma (str): Случайная гамма (ключ).
    Returns:
        str: Зашифрованный текст.
    """
    text = text.upper() # Приводим текст к верхнему регистру
    gamma = gamma.upper() # Приводим гамму к верхнему регистру
    cipher_text = "" # Создаем пустую строку для зашифрованного текста
    for text_char, gamma_char in zip(text, gamma): # Итерируемся по символам текста и гаммы
        if 'A' <= text_char <= 'Z' and 'A' <= gamma_char <= 'Z': # Проверяем, являются ли оба символа буквами латинского алфавита
            text_char_code = ord(text_char) - ord('A') # Получаем числовой код символа текста
            gamma_char_code = ord(gamma_char) - ord('A') # Получаем числовой код символа гаммы
            encrypted_char_code = (text_char_code + gamma_char_code) % 26 # Складываем коды и берём остаток от деления на 26 (алфавит)
            encrypted_char = chr(encrypted_char_code + ord('A')) # Преобразуем число обратно в символ
            cipher_text += encrypted_char # Добавляем зашифрованный символ к результирующей строке
        else:
            cipher_text += text_char # Если символ не буква, то добавляем его без изменений
    return cipher_text # Возвращаем зашифрованный текст
```

Рис. 1: функция гаммирования

Логика работы:

1. Приводит текст и гамму к верхнему регистру.
2. Создает пустую строку для хранения зашифрованного текста.
3. Определяет русский алфавит и его длину.
4. Перебирает символы текста и гаммы параллельно.
5. Для русских букв:
   - Вычисляет индексы букв в алфавите.
   - Складывает индексы, берет остаток от деления на длину алфавита для получения индекса зашифрованного символа.
   - Добавляет зашифрованный символ в результирующую строку.
6. Для остальных символов:
   - Добавляет их в результирующую строку без изменений.

Функция `generate_gamma_ru(length)`

Эта функция генерирует случайную гамму заданной длины.

- **Вход:** `length`: Целое число - длина гаммы.
- **Выход:** Строка - случайная гамма (русский язык).

```python
def generate_gamma(length):
    """
    Генерирует случайную строку букв для гаммы.
    Args:
        length (int): Длина гаммы
    Returns:
        str: Случайная гамма.
    """
    return "".join(random.choice("ABCDEFGHIJKLMNOPQRSTUVWXYZ") for _ in range(length)) # Генерирует случайную строку из букв
```

Рис. 2: функция generate_gamma

Пример использования

1. Задается исходный текст: ПРИВЕТ.
2. Генерируется случайная гамма той же длины.
3. Выполняется шифрование текста с использованием гаммы.
4. Выводится исходный текст, гамма и зашифрованный текст.

```python
# Пример использования:
text = "ПРИВЕТ" # Исходный текст
gamma = generate_gamma(len(text)) # Генерируем гамму той же длины, что и текст
encrypted_text = gamming_cipher_encrypt(text, gamma) # Шифруем текст

print(f"Исходный текст: {text}") # Выводим исходный текст
print(f"Гамма: {gamma}") # Выводим гамму
print(f"Зашифрованный текст: {encrypted_text}") # Выводим зашифрованный текст
```

```
Исходный текст: ПРИВЕТ
Гамма: FIIIVR
Зашифрованный текст: ПРИВЕТ
```

Рис. 3: пример применения

Важные замечания

- Для максимальной безопасности, гамма должна быть действительно случайной и использоваться только один раз для каждого сообщения.
- Этот код предназначен только для текста на русском языке.
- Шифрование гаммированием является одним из самых надежных методов шифрования при условии правильного использования.

Выводы

Выводы

Программно реализовано шифрование гаммированием.