Презентация по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Ле Тиен Винь

26 Октября 2024

Информация

- Ле Тиен Винь
- Студент
- Российский университет дружбы народов
- 1032215241@pfur.ru
- https://github.com/tvle2000/information

vinh

Цель работы

Освоить на практике применение режима одноключевого кодирования на примере кодирования различных исходных текстов одним ключом

Выполнения работы

- Мы используем метод шифрования: Выполнение операции сложения по модулю 2 (XOR)
- Поскольку такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой

Выполнения работы

```
int main() {
    string P1 = "ThisIsSecret";
    string P2 = "DontTellThat";
    string key = "123456789123";

    string ciphertext1 = xorOperator(P1, key);
    string ciphertext2 = xorOperator(P2, key);

    cout << "Ciphertext 1: " << ciphertext1 << endl;
    cout << "Ciphertext 2: " << ciphertext2 << endl;

    string Text1 = xorOperator(xorOperator(ciphertext1,ciphertext2),P1);
    string Text2 = xorOperator(xorOperator(ciphertext1,ciphertext2),P2);

    cout << "Text 1: " << Text1 << endl;
    cout << "Text 2: " << Text2 << endl;

    return 0;
}
```

Функция xorOperator

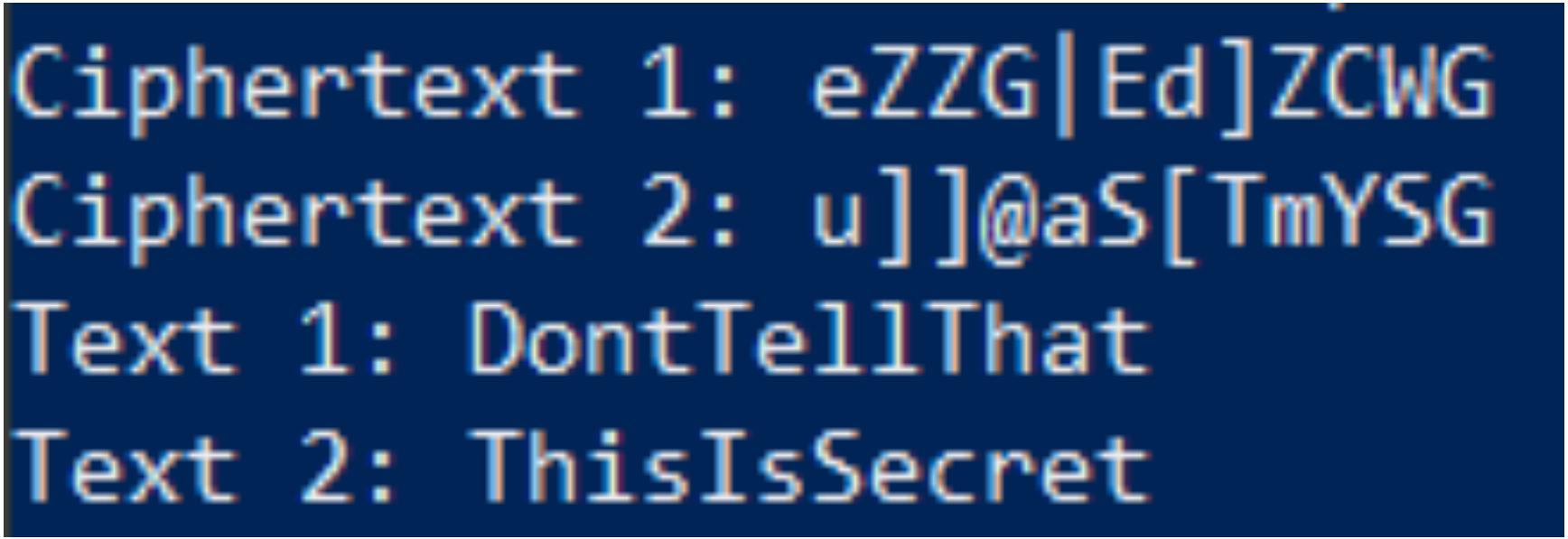
- Функция преобразует каждый элемент введенного текста в новый элемент, зашифрованный на основе ключа, с помощью операцией сложения по модулю 2 (XOR): Ci = Pi + Ki
- Где Ci — i-й символ получившегося зашифрованного послания, Pi — i-й символ открытого текста, Ki — i-й символ ключа, i = 1, …, m

Выполнения работы

```
int main() {
    string P1 = "ThisIsSecret";
    string P2 = "DontTellThat";
    string key = "123456789123";

    string ciphertext1 = xorOperator(P1, key);
    string ciphertext2 = xorOperator(P2, key);

    cout << "Ciphertext 1: " << ciphertext1 << endl;
    cout << "Ciphertext 2: " << ciphertext2 << endl;

    string Text1 = xorOperator(xorOperator(ciphertext1,ciphertext2),P1);
    string Text2 = xorOperator(xorOperator(ciphertext1,ciphertext2),P2);

    cout << "Text 1: " << Text1 << endl;
    cout << "Text 2: " << Text2 << endl;

    return 0;
}
```

- В main мы определем 2 исходного текста с называниями P1 и P2 и ключ key.
- Используовать функцию “xorOperator” для генерации зашифрованного текста и вывода зашифрованного текста на экран.
- В ситуации, когда злоумышленник знал один из двух текста, он может прочитать остальный, не зная ключа и не стремясь его определить, на основе свойства операции XOR: 1 + 1 = 0, 1 + 0 = 1
- Получаем C1 + C2 = P1 + K + P2 + K = P1 + P2, следует C1 + C2 + P1 = P1 + P2 + P1 = P2

Результат программы



Вывод

После лабораторной работы я получил практические навыки по применению режима одноключевого кодирования на примере кодирования различных исходных текстов одним ключом