Презентация по лабораторной работе №8

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

Нгуен Дык Ань

26 Октябрь 2024

Докладчик

- Нгуен Дык Ань
- Студенческий билет: 1032215251
- Группа: НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/NguyenDucAnh0512

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) как на лаборатоной работе 7

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

```
Ciphertext 1: eZZG|Ed]ZCWG
Ciphertext 2: u]]@aS[TmYSG
Text 1: DontTellThat
Text 2: ThisIsSecret
```

Вывод

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