Лабораторная 8

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

Шалыгин Г. Э.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Шалыгин Георгий Эдуардович
- студент НФИ-02-20
- Российский университет дружбы народов

Вводная часть

Актуальность

- Информационная безопасность - важная часть компетенции в образовательном треке НФИ

Цели и задачи

- Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Материалы и методы

- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
  - `pdf`
  - `html`
- Автоматизация процесса создания: `Makefile`
- Компилятор Julia
- OpenModelica

Результаты

Гаммирование

$$CODE = TEXT \oplus KEY$$

Напишем функцию наложения гаммы

```
string gamma(string dtext, string key){
    string etext = "";
    for(int i = 0; i < dtext.size(); i++){
        char c1 = dtext[i];
        char c2 = key[i];
        etext.push_back(c1 ^ c2);
    }
    return etext;
}
```

Figure 1: Файл httpd.conf

Тест

1. Для тестирования напишем следующий код, расшифровывающий текст без поиска ключа согласно формуле

$$C_1 \oplus C_2 \oplus P_2 = (P_1 \oplus Y) \oplus (P_2 \oplus Y) \oplus (P_2 \oplus Y) = P_1 \oplus P_2 \oplus P_2 = P_1$$

```
int main()
{
    string p1 = "Happy new year friends!";
    string p2 = "I dont like infsq sorry";
    string key = "']W8R(IANRELAq%*FKC=!@";
    string c1 = gamma(p1, key);
    string c2 = gamma(p2, key);
    cout << "C1: " << gamma(key, p1);
    cout << "\nC2: " << gamma(key, p2);
    cout << "\np1 decoded: " << gamma(gamma(c1, c2), p2);
    cout << "\np2 decoded: " << gamma(gamma(c1, c2), p1);
}
```

Figure 2: Тестирующий код

Результат

Убедимся в корректности результатов выполнения программы.

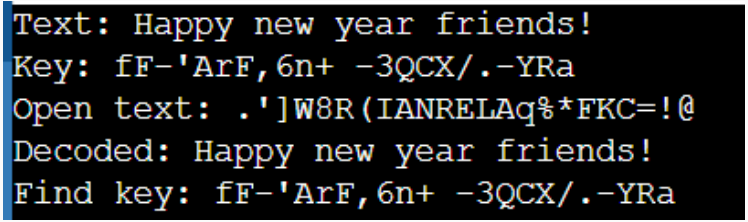

Figure 3: Результаты выполнения

Вывод

Вывод

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.