Лабораторная 7

Элементы криптографии. Однократное гаммирование

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.

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 (fig. 1).

```
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

Для тестирования напишем следующий код, расшифровывающий текст и находящий ключ (fig. 2).

```
int main()
{
    string s = "Happy new year friends!";
    string s2 = ".']W8R(IANRELAq%*FKC=!@";
    string key = "fF-'ArF,6n+ -3QCX/.-YRa";
    cout << "Text: " << s << '\n';
    cout << "Key: " << key << '\n';
    cout << "Open text: " << gamma(s, key) << '\n';
    cout << "Decoded: " << gamma(s2, key) << '\n';
    cout << "Find key: " << gamma(s, s2) << '\n';

}
```

Figure 2: Тестирующий код

Результат

Убедимся в корректности результатов выполнения программы(fig. 3).

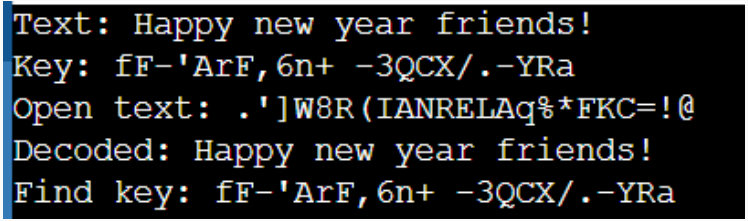

Figure 3: Результаты выполнения

Вывод

Вывод

В результате выполнения работы мы освоили на практике применение режима однократного гаммирования.