Лабораторная работа №8

Элементы криптографии. Шифрование различных исходных текстов одним ключом

Шестаков Д. С.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Шестаков Дмитрий Сергеевич
- студент группы НКНбд-01-20
- Российский университет дружбы народов
- dmshestakov@icloud.com

Вводная часть

Объект и предмет исследования

- Элементы криптографии
- Однократное гаммирование
- Язык программирования C++

Цели и задачи

- Освоить на практике применение режима однократного гаммирования.

Материалы и методы

- C++
- bash

Ход работы

Шифратор

```cpp
#include <iostream>
#include <sstream>
#include <string>
#include <vector>
#include <cassert>

std::string Codec(const std::vector<std::string>& key,
                  const std::string& input
                    ) {
    assert(key.size() == input.size());

    std::string res;

    for(size_t i = 0; i < input.size(); ++i)
    {
        int64_t ki, ci;

        std::istringstream iss(key[i]);

        iss >> std::hex >> ki;

        ci = int(input[i]);

        res += char(ci ^ ki);
    }

    return res;
}
```

Рис. 1: Шифрование

Поиск ключа

```
std::vector<std::string> GetKey(const std::string& input,
                                const std::string& output
                                ){
    assert(input.size() == output.size());
    std::vector<std::string> key;
    key.reserve(input.size());

    for(size_t i = 0; i < input.size(); ++i) {
        int64_t ii, oi, ki;

        ii = int(input[i]);
        oi = int(output[i]);

        ki = ii ^ oi;

        std::ostringstream ss;
        ss << std::hex << ki;

        key.push_back(ss.str());
    }

    return key;
}
```

Рис. 2: Поиск ключа

Результаты

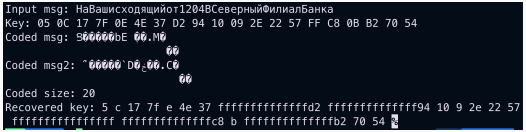

Рис. 3: Результат

Вывод

Освоили на практике применение режима однократного гаммирования.