

Отчёт по лабораторной работе №7

НКНбд-01-21

Юсупов Эмиль Артурович

Содержание

1	Введение	5
1.1	Цель работы	5
2	Выполнение работы	6
3	Заключение	10

Список иллюстраций

2.1	ASCII to Vector	6
2.2	Random Key Generator	6
2.3	Encryption/Decryption methods	7
2.4	Main function	8
2.5	Console output	9

Список таблиц

1 Введение

1.1 Цель работы

- Освоить на практике применение режима однократного гаммирования.

2 Выполнение работы

1. Проанализировали паттерны работы самого шифрования/дешифрования.
2. В программе мы занесли ASCII таблицу в вектор.

```
void pushToVec(vector<char>* v) {  
    for (int i = 0; i < 128; i++) {  
        v->push_back(char(i));  
    }  
}
```

Рис. 2.1: ASCII to Vector

3. Сделали генератор случайного ключа.

```
vector<char> generateRandomKey(const vector<char> *v, size_t len) {  
    random_device rd;  
    mt19937 mt(rd());  
    uniform_int_distribution<> dist(0, v->size()-1);  
  
    vector<char> key;  
  
    for (int i = 0; i < len; i++) {  
        key.push_back((*v)[dist(mt)]);  
    }  
  
    return key;  
}
```

Рис. 2.2: Random Key Generator

4. Написали функции шифрования/дешифрования.

```

vector<char> xorEncryption(vector<char> p, vector<char> k) {
    vector<char> enc;
    if (p.size() == k.size()) {
        for (int i = 0; i < p.size(); i++) {
            enc.push_back(p[i] ^ k[i]);
        }
    }
    return enc;
}

vector<char> findKey(const vector<char>& p, const vector<char>& enc) {
    return xorEncryption(p, enc);
}

vector<char> xorDecryption(const vector<char>& enc, const vector<char>& k) {
    return xorEncryption(enc, k);
}

```

Рис. 2.3: Encryption/Decryption methods

5. Прописали главную функцию со всей логикой.

```

int main()
{
    vector<char> v;
    // 97 - a, z - 122
    pushToVec(&v);

    std::string str;
    cout << "Enter the input: ";
    getline(cin, str);

    vector<char> arr(str.begin(), str.end());
    vector<char> key = generateRandomKey(&v, str.size());
    vector<char> enc = xorEncryption( arr, key);

    cout << "Original: " << str << endl;
    cout << "Generated: ";
    for (char c : key) { cout << c; }
    cout << endl << "Encrypted: ";
    for (char c : enc) { cout << c; }

    vector<char> decrypted = xorDecryption(enc, key);
    cout << "Decrypted: ";
    for (char c : decrypted) { cout << c; }

    vector<char> fKey = findKey(arr, enc);
    vector<char> decMes = xorDecryption(enc, fKey);
    cout << "\nDecrypted with key: ";
    for (char c : decMes) { cout << c; }
    cout << endl;

    return 0;
}

```

Рис. 2.4: Main function

6. Получили в консоль информацию.


```
Enter the input: Hello, World!  
Original: Hello, World!  
Generated: [/"lVaNnT4f  
  Encrypted: JN9Mn9zt8PGDecrypted: Hello, World!  
Decrypted with key: Hello, World!
```

Рис. 2.5: Console output

3 Заключение

Во время выполнения работы, мы получили навыки работы с режимом однократного гаммирования.