Отчет по лабораторной работе 7

Дисциплина: Информационная безопасность

Дяченко Злата Константиновна, НФИбд-03-18

Прагматика выполнения лабораторной работы

Данная лабораторная работа выполнялась мной для приобретения теоретических знаний и практических навыков применения однократного гаммирования.

Цель выполнения лабораторной работы

Освоить на практике применение режима однократного гаммирования.

Задачи выполнения лабораторной работы

Определить вид шифротекста при известном ключе и известном открытом тексте (рис. 1).

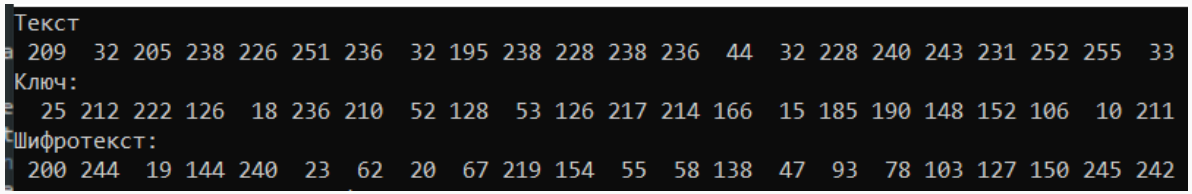

Figure 1: Открытый текст, ключ и шифротекст

Задачи выполнения лабораторной работы

```
void convert(string letter, int array[])
{

    for (int i = 0; i < letter.length(); i++)
    {
        unsigned char x = letter.at(i);
        array[i]= int(x);
    }
}

void printM (int array[], int len){
    for (int j = 0; j < len; j++) {
        cout << setw(4) << array[j];
    }
    cout<<endl;
}

void keyGen (int key[], int len){
    srand(time(NULL));
    for (int i = 0; i < len; i++){
        key[i]= rand() % 256;
    }
}

void gammir(int text[], int key[], int len, int shifrotext[]){
    for (int i=0; i<len; i++){
        shifrotext[i]=text[i]^key[i];
    }
}

void getKey(int shifrotext[], int text[], int len, int key[]){
    for (int i=0; i<len; i++){
        key[i]=shifrotext[i]^text[i];
    }
}
```

Figure 2: Функции программы

Задачи выполнения лабораторной работы

```
int main (){

    setlocale(LC_ALL, "Russian");
    string text;
    int len;
    text="С Новым Годом, друзья!";
    len=text.size();
    int shifr[len];
    convert(text, shifr);
    cout<<"Текст"<<endl;
    printM(shifr, len);

    int key[len];
    keyGen(key, len);
    cout<<"Ключ:"<<endl;
    printM(key, len);

    int shifrotext[len];
    gammir(shifr, key, len, shifrotext);
    cout<<"Шифротекст:"<<endl;
    printM(shifrotext, len);
```

Figure 3: Функция main. Шифрование

Задачи выполнения лабораторной работы

Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис. 4).

```
int newKey[len];
getKey(shifrotext, shifr, len, newKey);
cout<<"Ключ, полученный, зная шифротекст и открытый текст :"<<endl;
printM(newKey, len);

string text2= "С Новой бедой, друзья!";
int shifr2[len];
convert(text2, shifr2);
cout<<"Текст, который хочу получить "<<endl;
printM(shifr2, len);
getKey(shifrotext, shifr2, len, newKey);
cout<<"Ключ, который для этого нужно использовать (шифротекст не изменяется):"<<endl;
printM(newKey, len);
```

Figure 4: Определение ключа

Задачи выполнения лабораторной работы

```
Ключ, полученный, зная шифротекст и открытый текст :
  25 212 222 126  18 236 210  52 128  53 126 217 214 166  15 185 190 148 152 106  10 211
Текст, который хочу получить
 209  32 205 238 226 238 233  32 225 229 228 238 233  44  32 228 240 243 231 252 255  33
Ключ, который для этого нужно использовать (шифротекст не изменяется):
  25 212 222 126  18 249 215  52 162  62 126 217 211 166  15 185 190 148 152 106  10 211
```

Figure 5: Результат

Результаты выполнения лабораторной работы

В результате выполнения работы я освоила на практике применение режима однократного гаммирования.