


```
...
41 0d 61 01 60 44 69 48 24 28 60 24 2d 2d 41 04 4c 49 05 24 00 28 60 04 41 0d 61
48 4c 04 41 45 20 6c 40 20 20 29 6c 69 41 60 64 04 41 08 20 2c 49 05 2c 49 48 49
49 49 0d 20 64 49 68 25 84 6d 78 9d 98 68 60 60 28 60 60 68 60 04 20 29 60 24 2d
60 24 2d 01 24 c7 b4 d9 38 6c
...
```

Комментарий. В Вашем распоряжении имеется бинарный файл «*virus.bin*», содержащий указанный фрагмент бинарного кода.

Задача 3. Протокол

Алексею необходимо передать Виктории пятисимвольный пароль к учетной записи на сайте. Для того, чтобы пароль не был перехвачен, Виктория предлагает использовать следующий способ:

1. Алексей преобразует пароль (параметр *psw*) с помощью приведенной ниже функции, используя при этом известный только ему ключ (параметр *key*). Полученную строку отправляет Виктории.

```
char * E(char psw[5], char key[5])
{
    char *res = new char[5];
    for(int i = 0 ; i < 5 ; i++)
    {
        res[i] = (psw[i] + key[i])%256;
    }
    return res;
}
```

2. Виктория с помощью этой же функции преобразует полученную строку, указывая ее в качестве параметра *psw*, но используя свой ключ, известный только ей. Результат преобразования отправляется Алексею.

3. Алексей передает в функцию, приведенную ниже, в качестве параметров полученную от Виктории строку и свой исходный ключ:

```
char * D(char msg[5], char key[5])
{
    char *res = new char[5];
    for(int i = 0 ; i < 5 ; i++)
    {
        res[i] = (msg[i] - key[i])%256;
    }
    return res;
}
```

4. Возвращаемое функцией значение отправляется Виктории, по которому она восстанавливает пароль.

Алексей отказался от предложения Виктории, сославшись на то, что если не обеспечить подтверждение подлинности абонентов, то нарушитель сможет узнать пароль при перехвате отправляемых по сети строк. Прав ли Алексей? Какой пароль передавался Виктории, если в первом сообщении была перехвачена посланная Алексеем строка "plwsq".

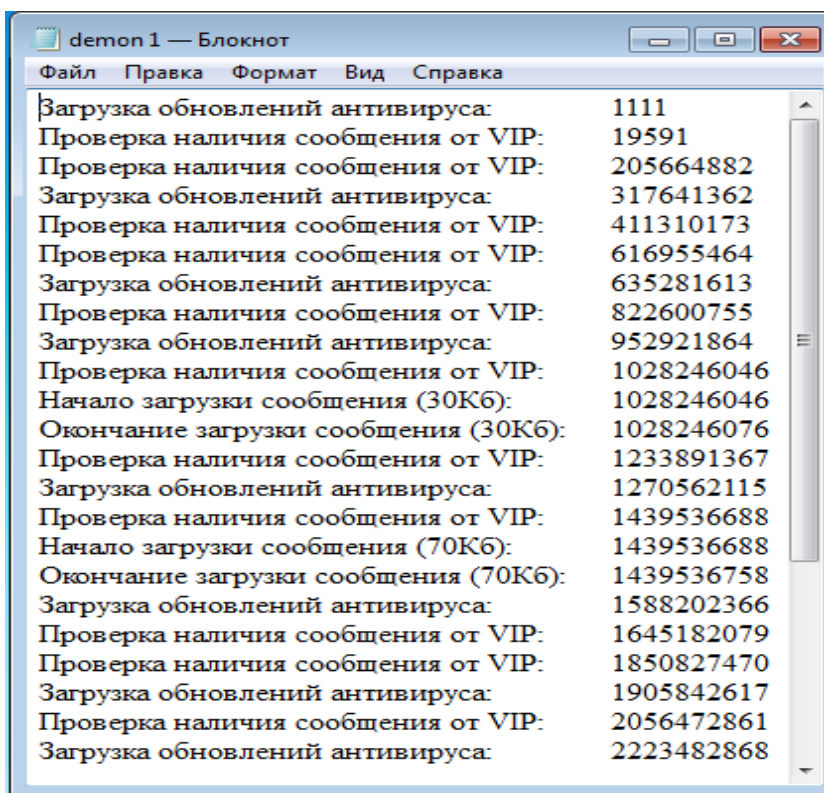
Комментарий. В Вашем распоряжении есть программа «*Protocol.exe*», моделирующая ситуацию, при которой нарушитель может перехватывать посылаемые сообщения. При помощи этой же программы Вы можете посылать любые сообщения Алексею от имени Виктории и Виктории от имени Алексея.

Задача 4. Дешифрование

Текстовый файл «*encrypttext.txt*» был получен, применяя 2015 раз функцию *Encrypt* (см. файл *Encrypt.cpp*) к исходному файлу. Расшифруйте файл «*encrypttext.txt*» по крайней мере в 1000 раз быстрее, чем он был зашифрован.

Задача 5. Антивирус

Нарушителю удалось получить журнал работы двух периодически запускающихся процессов сервера – обновления антивируса и проверки почтовых сообщений. Кроме того, он знает, что если обновление антивируса стартует во время загрузки почтовых сообщений от некоторого абонента VIP, то загружаемое сообщение антивирусом не проверяется. Из-за использования пароля 111 для почтового ящика VIP, нарушителю удалось получить к нему доступ. Сообщения от VIP загружаются со скоростью 1 Кбайт/сек, максимальный размер сообщения 100 Кбайт.



Опишите возможные действия нарушителя по внедрению на сервер вредоносного кода через почтовые сообщения от VIP. В какой минимальный момент времени может произойти внедрение вредоносного кода?