X ОЛИМПИАДА ПО ИНФОРМАТИКЕ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ
Вариант 2

Задача 1. Стеганография

Информация в сети передается с помощью пакетов. Каждый из них состоит из заголовка, данных и контрольной суммы (см. схему).

Заголовок			**Данные**	**Выравнивание до целого числа байт**	**Контрольная сумма**
Адрес источника	Адрес назначения	Размер данных (бит)			1 байт (количество единиц в бинарном представлении по модулю 256)
6 байт	6 байт	2 байта			

Вася обнаружил в исходящем сетевом трафике своего компьютера несколько странных пакетов и подозревает, что в них содержится скрытое сообщение. Помогите Васе определить, что именно было передано?

```
009988776655001122332211005988888888888888888888D43E
009988776655001122332211006188888888888888888888E13F
00998877665500112233221100318888888888E233
0099887766550011223322110039888888888888EC37
00112233221100998877665500598888888888888888888E53F
```

Задача 2. Вирус

Полиморфный вирус дописывает к заражаемой программе: код расшифровщика, команду безусловного перехода, случайные байты и вредоносный код (см. схему):

Код расшифровщика	Код заражаемой программы	E9(JMP) (1 байт)	Смещение (2 байта)	Случайные байты	Вредоносный код

При этом вредоносный код записывается в зашифрованном виде. Ниже приведена функция, которая использовалась для шифрования:

```
// crypto_const – неизвестная константа;
char encode(char code, const char crypto_const)
{
     return (code ^ crypto_const);
}
```

Кроме того, известно, что для перехода на начало собственно вредоносного кода применяется команда безусловного перехода *JMP*, которая в незашифрованном виде имеет код E9. После этого следуют 2 байта величины смещения относительно следующей команды. Найдите первые 4 байта расшифрованного вредоносного кода, если известно, что величина этого смещения не больше 250 байт.
Фрагмент кода программы после внедрения вируса:

…
```
a8 a0 88 a0 28 89 01 a8 a0 89 a8 a8 81 a0 a8 80 a0 a0 a9 a8 a8 80 a8 81 a0 a0 80
81 88 a0 a8 89 81 20 20 28 20 20 28 20 00 40 a9 84 59 d7 29 a8 01 89 21 08 89 09
89 09 a0 41 19 71 59 d7 89 21 80 08 89 01 a0 00 81 a0 80 29 88 20 a8 20 a0 a9 a9
81 a9 89 20 20 29 81 20 08 a0 09 a8 00 01 89 21 88 08 00 01 81 a0 a8 00 a0 a0 a9
a8 29 01 20 20 00 81
```
…

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 ”lptwq”.

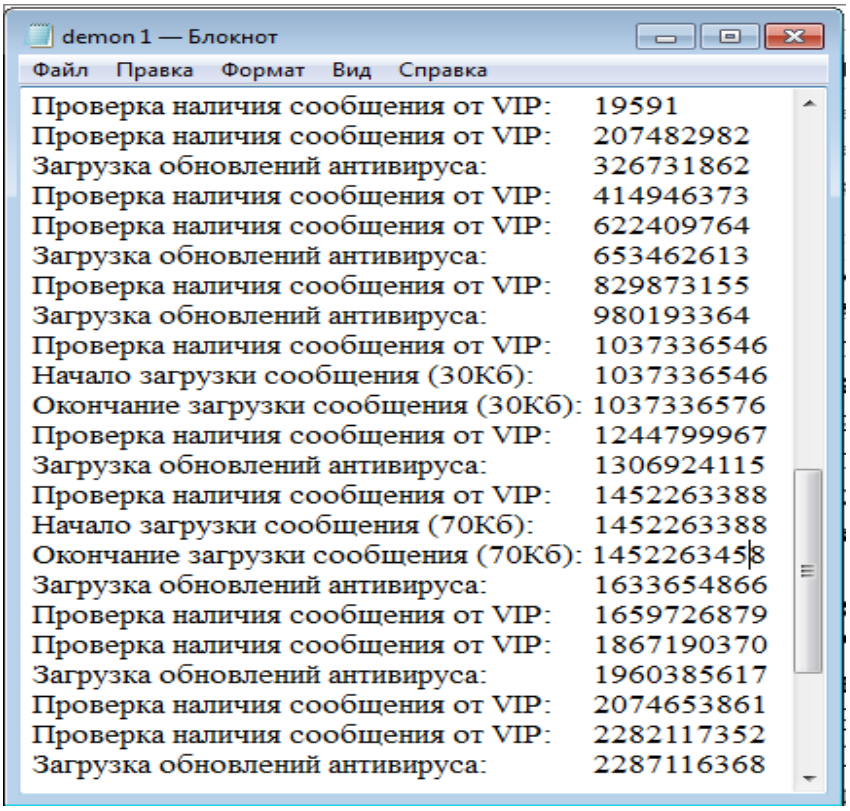
Комментарий. В Вашем распоряжении есть программа «*Protocol.exe*», моделирующая ситуацию, при которой нарушитель может перехватывать посылаемые сообщения. При помощи этой же программы Вы можете посылать любые сообщения Алексею от имени Виктории и Виктории от имени Алексея.

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?