Разбор задач Межрегиональной олимпиады школьников по информатике и компьютерной безопасности

Москва, 2017 г.

Межрегиональная олимпиада школьников по информатике и компьютерной безопасности

Организаторы:

- ✔ Академия Федеральной службы безопасности Российской Федерации;
- ✔ Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» при участии входящих в состав ФУМО ВО ИБ вузов.

В 2017/18 учебном году включена в Перечень Минобрнауки России:

уровень – II

профиль – «компьютерная безопасность»

Олимпиада является открытой – в ней может принять участие любой желающий школьник 8-11 классов.

Цели и задачи Олимпиады

- ✔ выявление и развитие у обучающихся творческих способностей и интереса к научной деятельности;
- ✔ создание условий для интеллектуального развития;
- ✔ поддержка одаренных детей, в том числе содействие им в профессиональной ориентации и продолжении образования;
- ✔ распространение и популяризация научных знаний о математических основах защиты информации среди молодежи.

Основные особенности построения заданий Олимпиады

- ✔ для решения заданий требуются знания из основных разделов информатики и компьютерной безопасности;
- ✔ проверяются не только теоретические знания, но и практические навыки программирования в рамках общеобразовательной программы по информатике;
- ✔ внимание акцентируется на использовании общих подходов к решению алгоритмических задач в области компьютерной безопасности;
- ✔ задания не содержат программных или аппаратных деталей реализаций механизмов защиты конкретных систем;
- ✔ в задания включаются специально подобранные примеры, отражающие актуальные задачи, решаемые в области защиты информации.

Тематика задач Олимпиады

- ✔ Анализ алгоритмов и программных реализаций;
- ✔ Анализ защищенности объектов ОС, БД и т.д.;
- ✔ Компьютерные сети (анализ сетевого трафика, алгоритмы распространение данных в сети);
- ✔ Модели безопасности;
- ✔ Стеганография;
- ✔ Шифрование.

Задания олимпиады. Вирус

I этап

Определить константу в интервале от 0x00 до 0xFF такую, что при применении операции «побайтового исключающего ИЛИ» к коду программы подряд будут следовать байты 0xE9 и 0x00.

Константа: 0x8E

Полиморфный вирус дописывает к заражаемой программе: код расшифровщика, команду безусловного перехода, случайные байты и вредоносный код:

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:

```
49 6e 61 67 8e be ba b4 a9 30 d6 9f f5 ea e8 b1 f9 d4 d3 d0 b3 bc d0 b0 b7 aa f9
d4 d3 d0 bc ab ad ba b4 b5 f5 ea eb b1 f9 d4 d3 d0 b3 bc d0 a9 09 41 6c 6b 68 0b
04 68 04 19 08 15 41 6c 6b 68 0b 0c 11 68 06 0e 41 71 ae a3 ae a9 ae 83 84 e3 ec
e7 fc fa e6 ea ef fa eb bf 87 ea ec 87 b6 ae ea fb fe ae a6 a9 ae a9 a7 a2 a9 aa
a9 ae 83 84 ae 83 84 e3 eb fd bd 87 ea ec 87 bf be a2 bf bd a2 bf be a2 bf bd a2
a9
```

…

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

Задания олимпиады. Вирус

II этап

Вычислить значащее значение байта смещения, следующего за байтами 0xE9 и 0x00, для получения точки входа в «тело» вируса.

Смещение: 48 байт

Полиморфный вирус дописывает к заражаемой программе: код расшифровщика, команду безусловного перехода, случайные байты и вредоносный код:

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:

```
...
49 6e 61 67 8e be ba b4 a9 30 d6 9f f5 ea e8 b1 f9 d4 d3 d0 b3 bc d0 b0 b7 aa f9
d4 d3 d0 bc ab ad ba b4 b5 f5 ea eb b1 f9 d4 d3 d0 b3 bc d0 a9 09 41 6c 6b 68 0b
04 68 04 19 08 15 41 6c 6b 68 0b 0c 11 68 06 0e 41 71 ae a3 ae a9 ae 83 84 e3 ec
e7 fc fa e6 ea ef fa eb bf 87 ea ec 87 b6 ae ea fb fe ae a6 a9 ae a9 a7 a2 a9 aa
a9 ae 83 84 ae 83 84 e3 eb fd bd 87 ea ec 87 bf be a2 bf bd a2 bf be a2 bf bd a2
a9
...
```

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

Задания олимпиады. Вирус

III этап

Перейти по вычисленному смещению и получить первые четыре байта кода вируса.

Смещение: 48 байт

Полиморфный вирус дописывает к заражаемой программе: код расшифровщика, команду безусловного перехода, случайные байты и вредоносный код:

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);
}
```

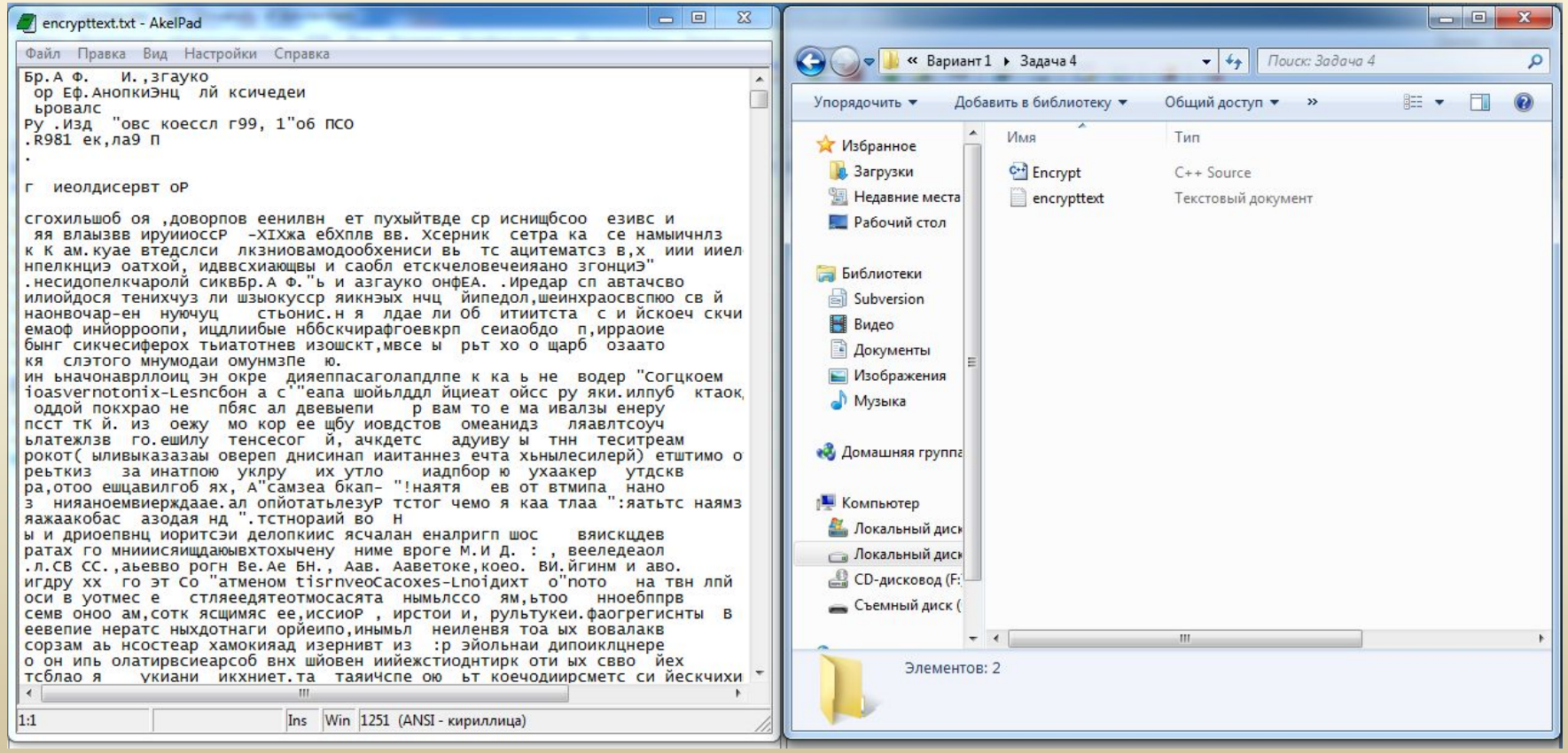
Кроме того, известно, что для перехода на начало собственно вредоносного кода применяется команда безусловного перехода *JMP*, которая в незашифрованном виде имеет код E9. После этого следуют 2 байта величины смещения относительно следующей команды. Найдите первые 4 байта расшифрованного вредоносного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

```
…
49 6e 61 67 8e be ba b4 a9 30 d6 9f f5 ea e8 b1 f9 d4 d3 d0 b3 bc d0 b0 b7 aa f9
d4 d3 d0 bc ab ad ba b4 b5 f5 ea eb b1 f9 d4 d3 d0 b3 bc d0 a9 09 41 6c 6b 68 0b
04 68 04 19 08 15 41 6c 6b 68 0b 0c 11 68 06 0e 41 71 ae a3 ae a9 ae 83 84 e3 ec
e7 fc fa e6 ea ef fa eb bf 87 ea ec 87 b6 ae ea fb fe ae a6 a9 ae a9 a7 a2 a9 aa
a9 ae 83 84 ae 83 84 e3 eb fd bd 87 ea ec 87 bf be a2 bf bd a2 bf be a2 bf bd a2
a9
…
```

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

Задания олимпиады. 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.



Задания олимпиады. Дешифрование

```
void EncryptMass(char * Mass, int n)
{
    if (n!=10) return;
    char temp[10];
    for (int i = 0; i<10; i++)
        temp[i] = Mass[i];
    for (int i = 0;i < n; i++)
        Mass[(i*i*i*i*i+i*i*i+9*i+8) % 10] = temp[i];
    return;
}
        WriteMassToFile(encryptText,buffMass, n);
    }
    return 1;
}
```

Новый индекс элемента вычисляется по формуле i^5+i^3+9i+8

0	1	2	3	4	5	6	7	8	9
8	9	6	5	2	3	4	1	0	7

Задания олимпиады. Дешифрование

0	1	2	3	4	5	6	7	8	9
8	9	6	5	2	3	4	1	0	7

0→8→0 : цикл длинны 2
9→7→1→9 : цикл длинны 3
6→4→2→6: цикл длинны 3
5→3→5: цикл длинны 2

После применения этого преобразование **6 раз подряд** будет получен начальный текст. По условию задачи, преобразование применялось **2015 раз**. Так как **2015 = 6*335 + 5**, то для получения открытого текста **необходимо один раз применить функцию *Encrypt* к файлу «*encrypttext.txt*».**

Задания олимпиады. Дешифрование

```
1
2   char * ReadMassFromFile(ifstream &inFile, int &outN)
3   {
4       char tempMass[10];
5       char buff;
6       int i(0);
7       while (!inFile.eof()&&(i<10))
8       {
9           inFile.get(buff);
10          if (inFile) tempMass[i++] = buff;
11      }
12      char * outMass = new char [i];
13      for (int j = 0; j<i; j++) outMass[j]=tempMass[j];
14      outN=i;
15      return outMass;
16  }
17  void EncryptMass(char * Mass, int n)
18  {
19      if (n!=10) return;
20      char temp[10];
21      for (int i = 0; i<10; i++)  temp[i] = Mass[i];
22      for(int i=0;i<n;i++) Mass[(i*i*i*i*i+i*i*i+9*i+8)%10]=temp[i];
23      return;
24  }
25  void WriteMassToFile(ofstream &outFile, char * mass, int n)
26  {
27      for (int i=0; i<n; i++) outFile.put(mass[i]);
28      delete [] mass;
29      return;
30  }
31  int Encrypt(char * inFile, char* outFile)
32  {
33      ifstream openText(inFile);
34      ofstream encryptText(outFile);
35      if (!openText || !encryptText) return -1;
36      while (!openText.eof())
37      {
38          int n;
39          char *buffMass = ReadMassFromFile(openText,n);
40          EncryptMass(buffMass,n);
41          WriteMassToFile(encryptText,buffMass, n);
42      }
43      return 1;
44  }
45
```

Файл Правка Вид Справка 0 %

Ф.А. Брокгауз, И.А. Ефрон
Энциклопедический словарь

Изд. "Русское слово", 1996 г.
OCR Палек, 1998 г.

Предисловие

Рост больших городов, появление новых путей и средств сообщения и связи вызвали в России рубежа XIX-XX вв. всплеск интереса к различным наукам. Как следствие возникла необходимость в систематизации их, в появлении энциклопедий, охватывающих все области человеческого знания.

"Энциклопедический словарь" Ф.А. Брокгауза и И.А. Ефрона справедливо считается одной из лучших русскоязычных энциклопедий, сохранившей свою справочно-научную ценность и для нас. Обилие статистической и фактической информации, подробные библиографические справки, подробные биографические статьи хорошо известны всем, кто хоть раз обращался к этому многотомному изданию.

Первоначально энциклопедия предполагалась как перевод немецкого "Conversations-Lexicon"'а с небольшой адаптацией для русской публики. Однако такой подход не оправдал себя и первые тома вызвали массу претензий. К тому же общее руководство изданием оставляло желать лучшего. Известен случай, когда студенты университета (которым заказывали переводы и написание незначительных статей) решили отомстить редакции за низкую оплату их труда и плохую работу редактора, восклицавшего "Ах, я собака безпамятная!" - в ответ на напоминания о задерживаемой оплате. Результатом чего стала такая статья: "Безпамятная собака - собака жадная до азартности".

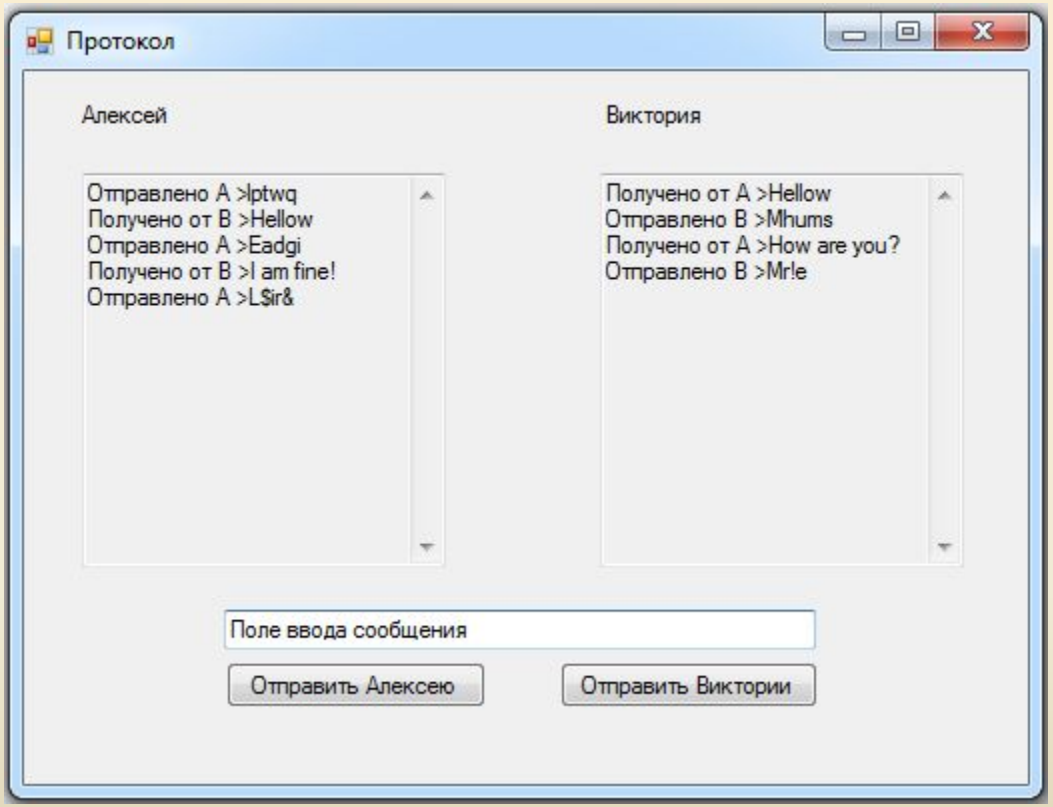
Новый период в истории энциклопедии начался с приглашения в состав редакции многих выдающихся ученых того времени: Д.И. Менделеева, Вл.С. Соловьева, С.А. Венгерова, А.Н. Бекетова, А.И. Воейкова и многих других. С этого момента "Conversations-Lexicon" отходит на второй план и основное место уделяется самостоятельным статьям, особенно по всем вопросам, относящимся к России, ее истории, культуре, географии.

Вытеснение переводных статей оригинальными, появление новых авторов сказалось на самом характере издания: из тривиальной энциклопедии оно превратилось в собрание новейших достижений и открытий во всех областях науки и техники. Читая статью о периодической системе химических элементов недоумеваешь, почему нет ни слова о Д.И. Менделееве, и, только дочитав до конца, узнаешь, что такая несправедливость по отношению к великому химику допущена: им самим.

Еще одно немаловажное достоинство энциклопедии - свободная манера изложения. Элементы беллетристики встречаются не только в биографических статьях, многие из которых читаются как захватывающие рассказы, но и в научных. Во многом такая раскованность в подаче материала тоже следствие привлечения к написанию статей виднейших ученых того времени, ведь, как известно, наиболее доходчиво что-либо объяснить может только тот, кто

Задания олимпиады. Протокол

- Применение навыков программирования;
- Умение анализировать исходные коды программ;
- Применение математических методов для решения вычислительных задач.



Задания олимпиады. 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.

Какой пароль передавался Виктории, если в первом сообщении была перехвачена посланная Алексеем строка ”wskjq”?

Задания олимпиады. Стеганография

Информация в сети передается с помощью пакетов. Каждый из них состоит из заголовка, данных и контрольной суммы:

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			

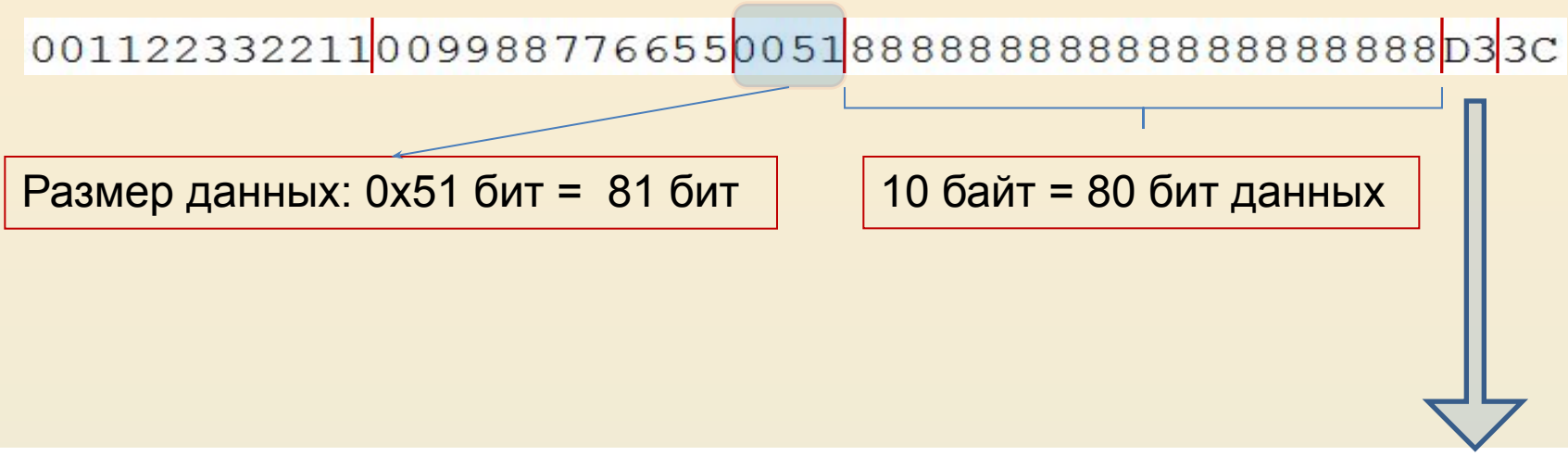
Вася обнаружил в исходящем сетевом трафике своего компьютера несколько странных пакетов и подозревает, что в них содержится скрытое сообщение. Помогите Васе определить, что именно было передано?

80 бит данных

```
001122332211009988776655005188888888888888888888D33C
00112233221100998877665500698888888888888888888888F745
0011223322110099887766550029888888888EF34
0011223322110099887766550039888888888888F237
00112233221100998877665500698888888888888888888888E442
```

Задания олимпиады. Стеганография

Пакет № 1

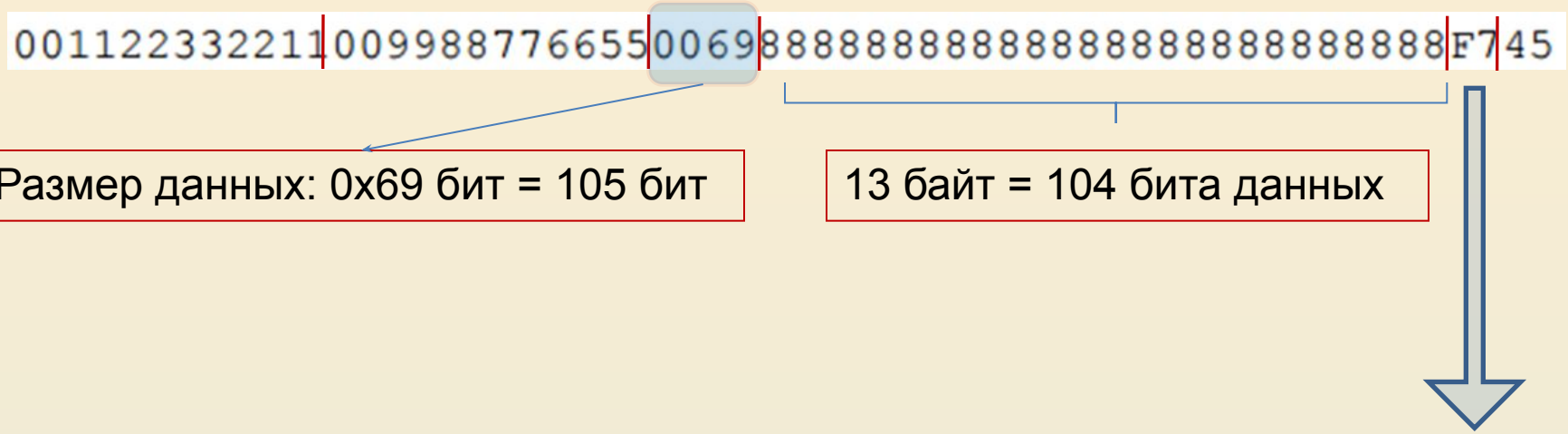


0xD3	1	1	0	1	0	0	1	1
	1 бит	2 бит	3 бит	4 бит	5 бит	6 бит	7 бит	8 бит

0x53	Данные	1	0	1	0	0	1	1
	1 бит	2 бит	3 бит	4 бит	5 бит	6 бит	7 бит	8 бит

Задания олимпиады. Стеганография

Пакет № 2



0xF7	1	1	1	1	0	1	1	1
	1 бит	2 бит	3 бит	4 бит	5 бит	6 бит	7 бит	8 бит

0x77	Данные	1	1	1	0	1	1	1
	1 бит	2 бит	3 бит	4 бит	5 бит	6 бит	7 бит	8 бит

Задания олимпиады. Стеганография

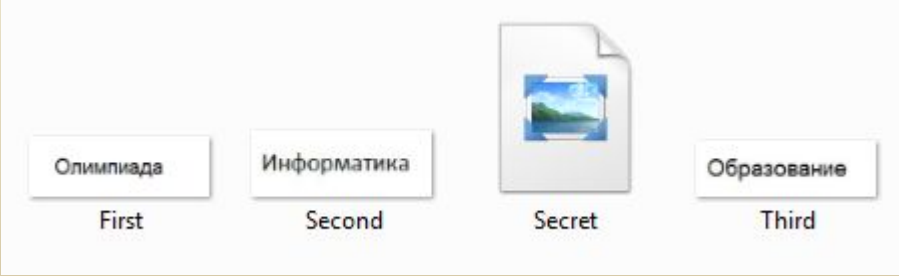
```
00112233221100998877665500518888888888888888888D3BC
00112233221100998877665500698888888888888888888888F745
00112233221100998877665500298888888888EF34
00112233221100998877665500398888888888888F237
00112233221100998877665500698888888888888888888888E442
```

Задания олимпиады. Гамма

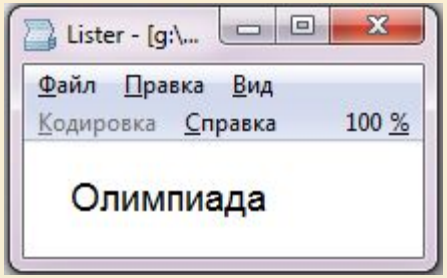
В центр обработки информации поступило четыре файла, каждый из которых является зашифрованным представлением изображения формата PNG. Известно, что шифрование осуществлялось методом «двоичного гаммирования», т.е. путем выполнения операции «побитового исключающего ИЛИ» между байтами исходного файла и байтами, полученными циклическим повторением последовательности из 4-х байтов ключа. Сотрудники центра успели расшифровать только три файла с именами *First.png*, *Second.png* и *Third.png*.

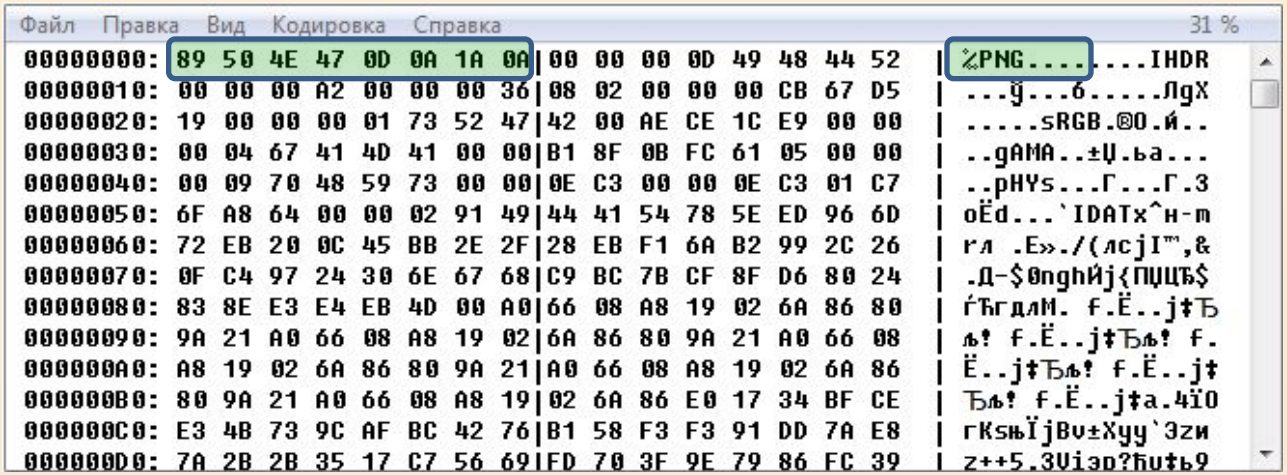
Помогите расшифровать оставшийся файл «*Secret.enc*». В ответе укажите слово, изображенное на полученной картинке формата PNG.

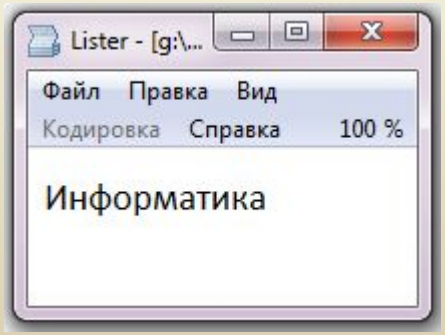
К задаче прилагается: файлы с расшифрованными картинками (First.png, Second.png, Third.png), файл с зашифрованной картинкой Secret.enc, редактор файлов в 16-ном формате (HexEditor).

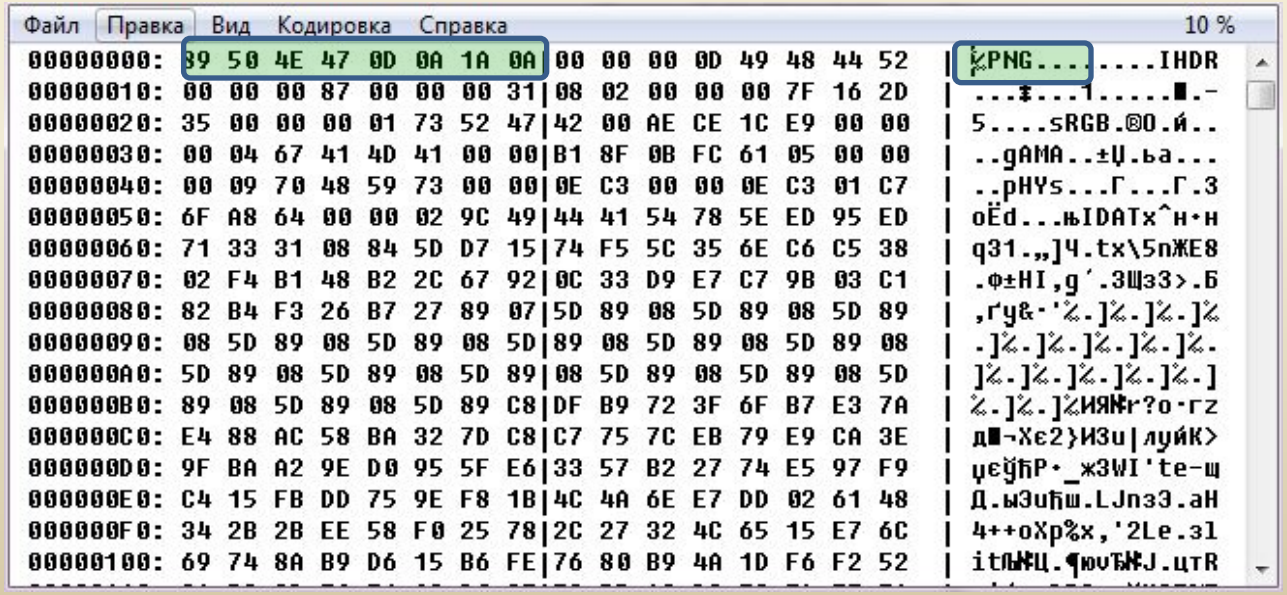


Задания олимпиады. Гамма

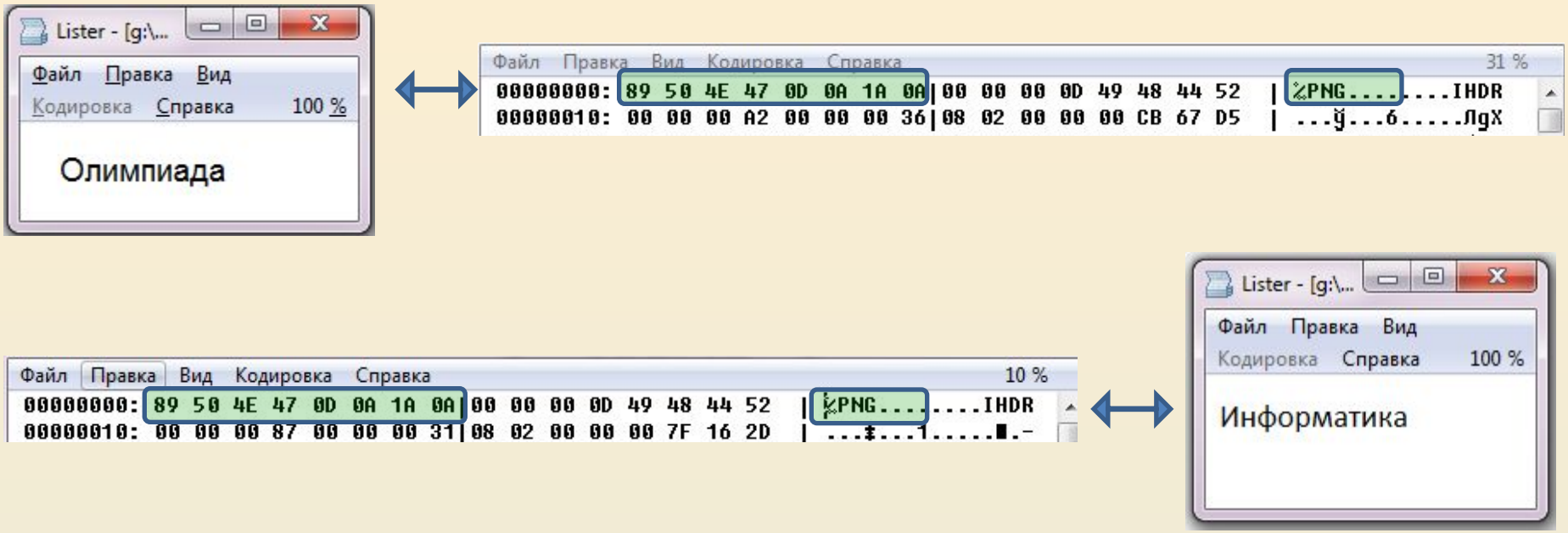








Задания олимпиады. Гамма



Задания олимпиады. Гамма

First.png	89 50 4E 47 0D 0A 1A 0A …
Second.png	89 50 4E 47 0D 0A 1A 0A …
Third.png	89 50 4E 47 0D 0A 1A 0A …
Secret.png	F3 64 5C D7 77 3E 08 9A …

Длина ключа = 4 байта

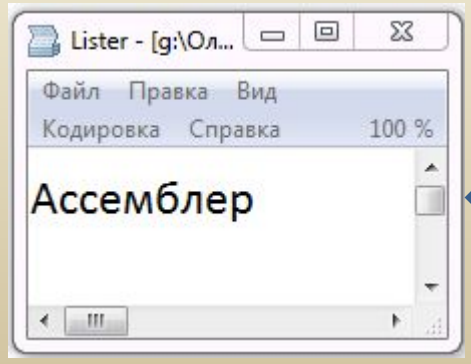
(89 50 4E 47) ^ (F3 64 5C)

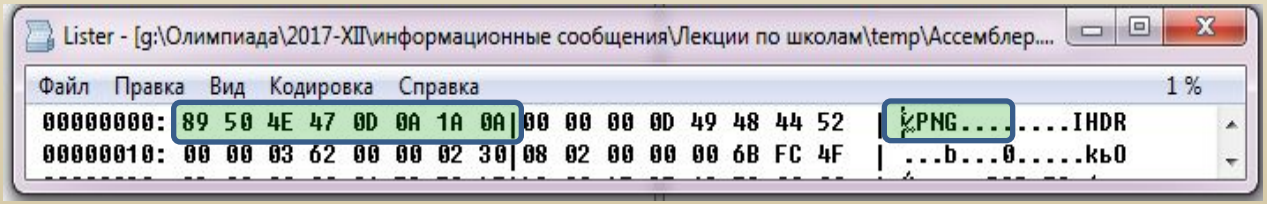
=

7A 34 12 90

Гамма = 7A 34 12 90 7A 34 12 90 7A 34 12 90 … 7A 34 12 90 …

(Secret.png) ^ Гамма





Перечень дополнительной литературы

1. Введение в криптографию / В. Ященко - М.: МЦНМО, 2012. — 352 с.

2. Защита информации в информационном обществе / А. А. Малюк - М.: Горячая линия – Телеком, 2015. — 230 с. ил.

3. Компьютерная безопасность / А. Заика. - М.: Рипол Классик, 2013. — 158 с.

4. [Глава 1] Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. - М.: Солон-Пресс, 2009. — 265 с.

Спасибо за внимание!

XII Межрегиональная олимпиада школьников по информатике и компьютерной безопасности

Отборочный этап Олимпиады

проводится дистанционно на сайте
http://www.v-olymp.ru/

с 18 сентября по 17 октября 2017 г.

Заключительный этап Олимпиады

состоится 29 октября 2017 г. в очной форме

В Москве: Академия ФСБ России, Мичуринский проспект, дом 70;

МИРЭА, 5-я ул. Соколиной горы, дом 22.

Сбор участников в 9:30