Олимпиада школьников по информатике и компьютерной безопасности (2008 год)

11 класс

Решение задачи № 1

Решение задачи связано с переводом из системы счисления с основанием 5 в систему счисления с основанием 9. Для того чтобы сделать это, можно воспользоваться промежуточным переводом из системы счисления с основанием 5 в десятичную систему счисления, а затем осуществить перевод уже из десятичной системы счисления в систему счисления с основанием 9.

Для того чтобы перевести из системы счисления с основанием 5 в десятичную систему счисления, можно воспользоваться полиномом разложения:

$$A = \sum_{i=0}^{n-1} k_i * 5^i$$

где A – число в десятичной системе счисления, n- количество цифр в числе, которое нужно перевести, i – позиция цифры в числе, которое нужно перевести, k_i - цифра, которая находится на i-ой позиции в числе, которое нужно перевести.

Тогда A = $1*5^2+0*5+2*1 = 27$.

Для того чтобы перевести из десятичной системы счисления в систему счисления с основанием 9, нужно последовательно делить искомое число на основание той системы счисления, в которую осуществляется перевод. При этом остатки от деления будут являться цифрами числа в искомой системе счисления, записанными в обратном порядке.

27/9 = 3 27%9 = **0**. Результат – 30.

Решение задачи № 2

Для того, чтобы решить задачу, необходимо получить реальный физический адрес ячейки памяти. Для этого необходимо проделать все операции по

формированию физического адреса из логического адреса, которые описаны в условии задачи.

Возьмем первый адрес – 45:14. Сначала запишем его в двоичной системе счисления. Для этого можно воспользоваться формулой сокращенного перевода из 16-ричной системы счисления в двоичную системы счисления. Для этого каждый разряд числа в 16-ричной системе счисления заменяется 4 разрядами числа в двоичной системе счисления.

Тогда будет сформирован следующий адрес:

01000101:00010100 (SR:OR).

Адрес 44:19 соответственно будет преобразован в адрес

01000100:00011001 (SR:OR).

Затем содержимое регистра SR сдвигается на 2 бита влево и к нему прибавляется значение регистра OR.

01000101 -> 0100010100 + 00010100 = 0100101000.

01000100 -> 0100010000 + 00011001 = 0100101001.

Видно, что второй адрес больше первого. Значит, адрес 44: 19 больше, чем адрес 45:14.

Решение задачи № 3

Решение задачи связано с подсчетом возможного количества вариантов пароля. Затем это количество умножается на время одной попытки, что дает максимальное время, которое потребуется на подбор пароля.

Если предположить, что пароль состоял из одного символа, то тогда есть 20 вариантов. Для двух символов это число равно 20*20. И так далее. В итоге получим следующую формулу:

$N = 20 + 20*20 + 20*20*20 + 20*20*20*20 + 20*20*20*20*20 + 20*20*20*20*20*20 + 20*20*20*20*20*20*20$

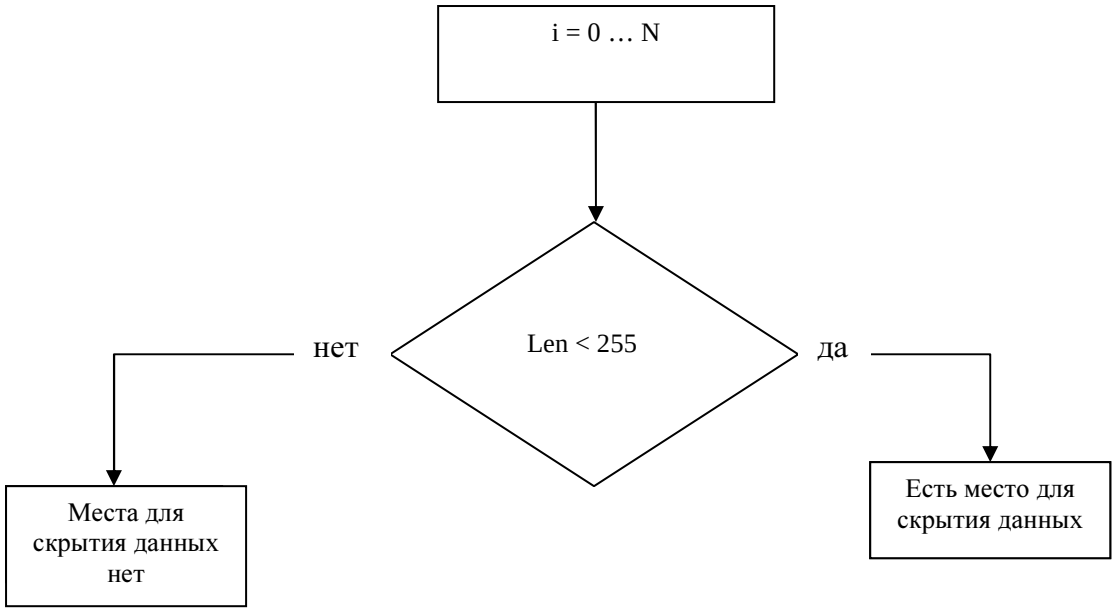
Теперь, чтобы подсчитать время необходимо число опробуемых паролей умножить на время опробования *T =N*10 сек.*

Решение задачи № 4

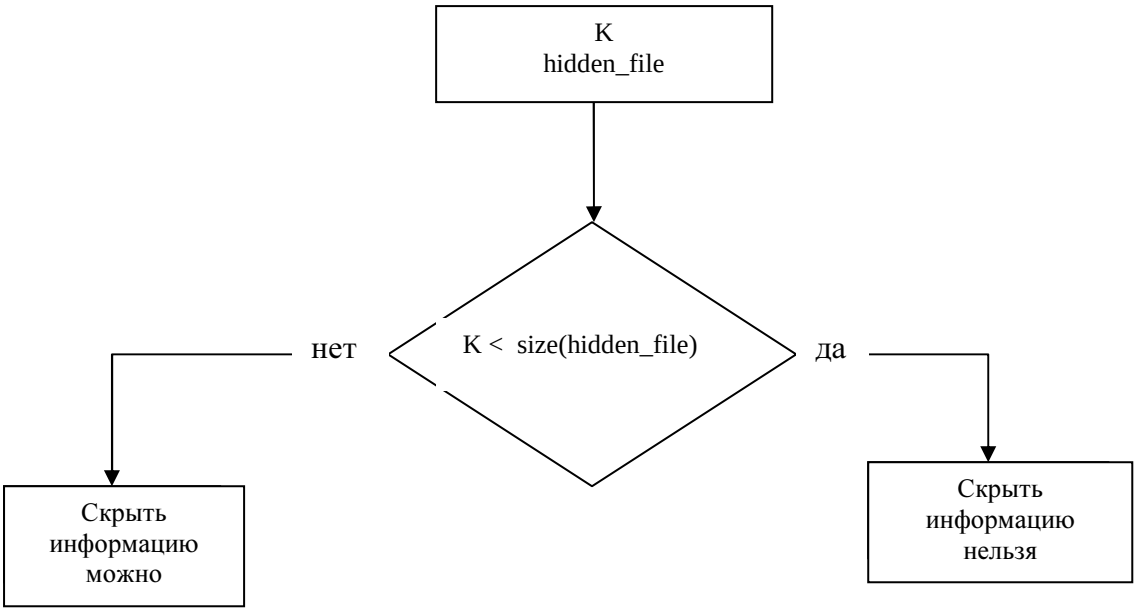
Сокрытие данных в записях файла основано на том, что длина *Record Data* может не совпадать с действительным количеством записанной в него информации. Если *Len* равно 255, то тогда количество информации в поле *Record Data* в точности равно размеру самого поля.

Если *Len* меньше 255, то тогда количество информации в поле меньше размера самого поля, и существует (255 – *Len)* свободных байт, которые можно использовать для сокрытия информации.

Алгоритм нахождения записей, в которых можно реализовать сокрытие данных, можно записать в виде такой блок-схемы:



Полученное количество информации, которое можно скрыть, сравнивается с размером файла со скрываемой информацией. Пусть K – количество информации, которое можно скрыть, hidden_file – файл с данными, которые нужно скрыть. Алгоритм определения возможности сокрытия необходимого количества данных в файле можно записать так



Если скрыть информацию можно, то осуществляется ее побайтовая сохранение в те записи исходного файла, где есть возможность добавить информацию.

Решение задачи № 5

Зашифрованный пароль представляет собой последовательность цифр, которая связана с открытым текстом. Первая цифра – это номер строки открытого текста, вторая цифра – это номер слова в данной строке, третья цифра – это номер буквы в данном слове. Если применить данный закон, то можно будет определить пароль. Решение – **терабайт.**

Решение задачи № 6

Нам известно, что для расчета хэш-образа пароля берется остаток от деления кода символа на 31. Необходимо предложить алгоритм нахождения самого короткого пароля. Это означает, что в этом пароле должно быть максимально возможное количество символов с таким кодом, который дает самый большой остаток отделения на 31. Такой символ – Z. После этого нужно определить оставшийся символ. Его хэш можно определить по следующей формуле:

$$HashX = StoredHash - (n * 90\%31),$$

где

StoredHash – эталонное хэш-образ, вычисленный на основании верного пароля,

n – найденное количество букв “*Z*”.

HashX – хэш оставшегося символа.

Если *StoredHash* < 90%31, то это означает, что пароль состоит из одного символа.