Условия задач заключительного этапа

Задача 1. Парольная комбинация

У администратора Ивана на рабочем компьютере стоит четырехзначный пароль, состоящий из цифр. После трех неудачных попыток ввода пароля компьютер блокируется. Известно, что сумма первых двух цифр и сумма последних двух цифр пароля равны простым числам.

Помощник шпиона пригласил Ивана в кафе на обед. На какое минимальное время необходимо задержать Ивана, чтобы шпион смог гарантированно подобрать пароль от компьютера и скопировать данные, если на ввод пароля требуется 1 секунда, блокировка компьютера осуществляется на 10 секунд, а время копирования нужных данных составляет 2 минуты?

Задача 2. Секретное сообщение

Аналитику удалось перехватить зашифрованное изображение, но программа шифрования утеряна. Известно, что шифрование осуществлялось методом «двоичного гаммирования», т.е. путем последовательного выполнения операции «побитового исключающего ИЛИ» между каждым байтом изображения и байтом ключа. Известно также, что ключ формировался в самой программе шифрования.

Восстановите текст, записанный на изображении, а также алгоритм шифрования и используемый ключ.

Задача 3. Контроль доступа

Система охраны осуществляет удаленный учёт прохода сотрудников на предприятие с использованием карт сотрудников и контрольной суммы. Для внесения в электронный журнал записи о проходе сотрудника вычисляется контрольная сумма на основе текущей даты, фамилии сотрудника и серийного номера карты.

Для получения контрольной суммы, в первую очередь, вычисляется последовательность $(t_1 t_2 \dots t_p)$ по формуле:

$$t_1 = 1,$$
$$t_{i+1} = (t_i * d + m) \bmod N,$$

где $i = 0, 1, \ldots, p-1$,
p – количество символов в фамилии сотрудника,
d – текущая дата (день месяца),
m – номер текущего месяца,
N – количество символов в алфавите (для русского алфавита N=32) ,
mod – операция получения остатка от деления числа.

Далее каждый номер символа фамилии умножается на соответствующий элемент последовательности. Контрольная сумма вычисляется из суммы полученных произведений, умноженной на серийный номер карты сотрудника:

$$CRC = \left(t_1 * L_1 + t_2 * L_2 + \cdots + t_p * L_p\right) * Serial \bmod V,$$

где
V – общее количество сотрудников ($V = 10\,000$);
Serial – серийный номер карты сотрудника (десятичное число в диапазоне от 1000 до 9999 включительно),
L_i – номер i-го символа фамилии сотрудника в алфавите:

А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**
0	1	2	3	4	5	6	7	8	9	10	11	12
Н	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**
13	14	15	16	17	18	19	20	21	22	23	24	25
Ъ	**Ы**	**Ь**	**Э**	**Ю**	**Я**							
26	27	28	29	30	31							

Например, если сотрудник по фамилии ПЕТРОВ пройдет через пропускной пункт 10 мая по карте с серийным номером 1350, то контрольная сумма будет вычислена следующим образом.

Последовательность t будет состоять из 6 значений:

$t_1 = 1$,
$t_2 = (1 * 10 + 5) \bmod 32 = 15$,
$t_3 = (15 * 10 + 5) \bmod 32 = 27$,
$t_4 = (27 * 10 + 5) \bmod 32 = 19$,
$t_5 = (19 * 10 + 5) \bmod 32 = 3$,
$t_6 = (3 * 10 + 5) \bmod 32 = 3$.

Контрольная сумма равна:

$$CRC = (1 * 15 + 15 * 5 + 27 * 18 + 19 * 16 + 3 * 14 + 3 * 2) * 1350 \bmod 10000 = 928 * 1350 \bmod 10000 = 2800.$$

Конкурент хочет проникнуть на предприятие под фамилией ВИЛКИН. Ему удалось добыть фрагмент журнала входа, а также имеется оборудование по программированию карт входа.

```
01.06 - ВИЛКИН - 9038
02.06 - ВИЛКИН - 2262
03.06 - ЛОЖКИН - 5066
04.06 - ЛОЖКИН - 5955
05.06 - ВИЛКИН - 5106
06.06 - ВИЛКИН - 1174
07.06 - ЛОЖКИН - 1462
08.06 - ЛОЖКИН - 4867
09.06 - ВИЛКИН - 6102
10.06 - ВИЛКИН - 5158
11.06 - ЛОЖКИН - 7858
12.06 - ЛОЖКИН - 3779
```

Какой серийный номер записать на карту, чтобы успешно пройти на предприятие? В какие дни лучше всего посетить предприятие, чтобы не вызвать подозрений. Ответ обоснуйте.

К задаче прилагается:
файл журнала log_v1.txt.

Задача 4. Reverse engineering

Имеется фрагмент программы на языке C:

```
#include <stdio.h>
#include <string.h>

int main ()
  {
    int code = 0;
    char password[10];
    printf ("Введите пароль:");
    gets (password);
    /*
    ...
    утерянный фрагмент кода
    ...
    */
    if (code == 0)
    {
      /*
      ...
      вычисление значения code
      ...
    */
    }

    if (code == 21827)
       printf ("Пароль верный!");
    else
       printf("Пароль неверный!");
  }
```

Был получен фрагмент скомпилированного исполняемого файла в шестнадцатеричном формате, в котором удалось обнаружить следующий программный код:

Адрес памяти	Байты в памяти	Их содержание
001C1231	C2 E2 E5 E4 E8 F2 E5 20 EF E0 D0 EE EB FC 3A 00	Строка «Введите пароль:»
001C1241	CF E0 D0 EE EB FC 20 E2 E5 F0 ED FB E9 21 00	Строка «Пароль верный!»
001C1250	CF E0 D0 EE EB FC 20	Строка «Пароль неверный!»

	ED E5 E2 E5 F0 ED FB E9 21 00	
001C1261	00 00 00 00 00 00 00 00 00 00	Массив password (10 байт)
001C126B	00 00 00 00	Переменная code (целое число, 4 байта)
001C126F	68 61 12 1C 00	Машинная команда, передающая параметр password (его адрес) в подпрограмму gets (переход по адресу начала тела подпрограммы)
001C1274	FF 75 15 1C 00	Вызов подпрограммы gets
001C1279	83 C4 04	Вспомогательная команда, выполняемая после возвращения из подпрограммы, имеющей один параметр
001C127C	8B 45 6B 12 1C 00	Копирование значения переменной code в регистр процессора
001C1282	39 45 00	Сравнение значения регистра с константой 0
001C1285	76 11 13 1C 00	Если результат сравнения false, то переход на выполнение команды по адресу 00 1C 13 11
001C128A	...	Вычисление переменной code
...	...	
001C1311	8B 45 6B 12 1C 00	Копирование значения переменной code в регистр процессора
001C1317	3B 45 43 55	Сравнение значения регистра с константой 21827
001C131A	77 2C 13 1C 00	Если результат сравнения true, то переход по адресу 00 1C 13 2C
001C131F	68 50 12 1C 00	Машинная команда, передающая адрес строки «Пароль неверный!» в подпрограмму printf как параметр
001C1324	FF 90 16 1C 00	Вызов подпрограммы printf
001C1329	83 C4 04	Вспомогательная команда, выполняемая после возвращения из подпрограммы, имеющей один параметр
001C132B	C3	Команда завершения работы программы
001C132C	68 41 12 1C 00	Машинная команда, передающая адрес строки «Пароль верный!» в подпрограмму printf как параметр
001C1331	FF 90 16 1C 00	Вызов подпрограммы printf
001C1336	83 C4 04	Вспомогательная команда, выполняемая после возвращения из подпрограммы, имеющей один параметр
001C1339	C3	Команда завершения работы программы
...	...	
001C1575		Тело функции gets
...	...	
001C168F	C1	Возврат к команде, следующей после точки вызова
001C1690		Тело функции printf
...	...	
001C185F	C1	Возврат к команде, следующей после точки вызова

Определите, что нужно подать на вход программы, чтобы в результате выполнения вывелась строка «*Пароль верный!*». Ответ обоснуйте.

Применяемая реализация подпрограммы *gets* принимает на вход любые данные без ограничений. Специальные символы (нулевой байт, символ конца строки и т.п.) во входном потоке не прерывают ввод строки.

Задача 5. Web-сайт

Олег создал сайт, в котором спрятал IP-адрес своего секретного сервера в формате `xxx.xxx.xxx.xxx` (`xxx` – число от 0 до 255). На сайте Олег оставил подсказки. Определите IP-адрес секретного сервера Олега.

К задаче прилагается:
папка с содержимым web-сайта.