

Maratón de Programación - 2014 - Semifinal

CATEGORÍA Grado 11

30/10/2014

Politécnico Colombiano Jaime Isaza Cadavid



**Reglas de la competencia**

**Restricciones:**

1. Los equipos participantes no pueden utilizar ningún tipo de material digital para la realización de los ejercicios.
2. Ninguno de los miembros del equipo puede hablar con los competidores de los otros equipos participantes.
3. Los equipos no pueden utilizar a internet (Navegar) en ningún momento.
4. Cada uno de los integrantes del equipo debe apagar sus equipos móviles (Celulares, Palm’s, portátiles u otros similares).
5. Los miembros de equipo solo pueden usar el computador asignado un lápiz o lapicero y hojas en blanco.

**Método de trabajo:**

1. A cada equipo se le asignará de manera aleatoria uno de los computadores.
2. Los participantes recibirán instrucciones precisas de la forma de trabajo y las reglas del concurso.
3. Cada uno de los equipos tiene aproximadamente 4 horas para completar la prueba.
4. Los ejercicios pueden ser resueltos en diferente orden.
5. Cada ejercicio tiene igual puntuación.
6. Los equipos se clasificarán por tiempo, es decir se suman los tiempos desde el inicio de la prueba hasta la solución de cada ejercicio y se organizan los tiempos de menor a mayor.
7. Si alguno de los equipos termina correctamente (y en el menor tiempo) la solución de todos los ejercicios antes de las 4 horas planeadas se convierte inmediatamente en el ganador.

Los jurados y docentes tienen plena libertad de sancionar con la descalificación cualquier conducta irregular en el desarrollo de la prueba.



**ÉXITOS!!!**

**RETO DE CALENTAMIENTO**

**¿FÁCIL DE DECIR?**

**Nombre del archivo fuente:** password.c, password.cpp, o password.java

Un password seguro es algo delicado. Los usuarios prefieren passwords que sean fáciles de recordar (como *junio*), pero este password puede ser inseguro. Algunos lugares usan un generador randómico de passwords (como *xvtpzyo*), pero los usuarios toman demasiado tiempo recordándolos y algunas veces los escriben en una nota pegada en su computador. Una solución potencial es generar password “pronunciables” que sean relativamente seguros pero fáciles de recordar.

FnordCom está desarrollando un generador de passwords. Su trabajo en el departamento de control de calidad es probar el generador y asegurarse de que los passwords sean válidos. Para ser válido, el password debe satisfacer estas tres reglas:

1. Debe contener al menos una vocal.
2. No debe tener tres vocales consecutivas o tres consonantes consecutivas.
3. No debe tener dos ocurrencias consecutivas de la misma letra, excepto por ‘ee’ o ‘oo’.

**Datos de entrada (entrada estándar)**

La entrada consiste en uno o más passwords potenciales, (uno por línea), seguidos por una línea conteniendo una palabra 'end' que señala el fin de la entrada.

Cada password tiene como mínimo una y como máximo veinte letras de largo y está formado por solo letras en minúscula.

**Datos de salida**

Por cada password, despliegue si es o no aceptable, usando el formato mostrado en el ejemplo de salida.

|  |  |
| --- | --- |
| **Ejemplo de entrada**  Marym  luisfer  jorgee  Mamaaa  End | **Ejemplo de salida**  <Marym>Password incorrecto  <luisfer>Passwordcorrecto  <jorgee>Password correcto  <Mamaaa>Password incorrecto |