I Olimpiada Informática Asturiana
Modalidad B

# Consideraciones generales[1]

- Esta modalidad consta de dos pruebas obligatorias. En caso de que algún participante desista de una de ellas quedará descalificado inmediatamente.
- El tiempo máximo para cada una de las pruebas es de 2 horas y se celebrarán una en cada día de la olimpiada.
- El factor fundamental para evaluar cada prueba es el tiempo empleado para resolverla aunque para cada una de ellas se proporcionan detalles adicionales.
- Para cada una de las pruebas se obtendrá una clasificación de los participantes. Dicha clasificación permitirá asignar una puntuación a los participantes del siguiente modo: **25 puntos para el primer clasificado, 18 puntos para el segundo, 15 para el tercero, 12 para el cuarto, 10 para el quinto, 8 para el sexto, 6 para el séptimo, 4 para el octavo, 2 para el noveno y 1 punto para el décimo clasificado.** Aquellos participantes que queden clasificados más allá de la décima posición no recibirían puntos. Los tiempos se medirán con una precisión de minutos con lo cual es posible que haya empates en tiempos y, en consecuencia, en puntuaciones.
- La puntuación final de la modalidad será el resultado de sumar los puntos obtenidos en ambas pruebas siempre y cuando el participante no haya sido descalificado.
- Puesto que en esta modalidad participan estudiantes procedentes de distintos niveles del sistema educativo y edades muy dispares se concederá cierta ventaja en la salida a unos participantes sobre otros. Así, los alumnos de ESO serán los primeros en comenzar no pudiendo comenzar los alumnos de Bachillerato y Ciclos Formativos de Grado Medio hasta que un alumno de ESO haya superado correctamente el primer reto o ejercicio o hayan transcurrido 15 minutos; a su vez, los alumnos de Ciclos Formativos de Grado Superior no podrán comenzar hasta que un alumno de Bachillerato o de CFGM haya superado el primer reto o ejercicio o hayan transcurrido 15 minutos desde el comienzo de la segunda tanda.

[1] Las consideraciones generales deben proporcionarse por escrito a todos los participantes.

# Resolución de problemas[2]

- El único factor que se tendrá en cuenta para la clasificación es el tiempo requerido para resolver el ejercicio de manera completamente correcta.
- Sin perjuicio de lo anterior, se anotarán los tiempos empleados para ejercicios resueltos de forma parcial. Por "forma parcial" se entiende un ejercicio que no supera todas las pruebas de los jueces. Dichos tiempos se utilizarían para la clasificación de los participantes que no terminasen todos los ejercicios de la prueba.

## Primer ejercicio

Algunos textos contienen mensajes ocultos. En esta ocasión el mensaje oculto esta formado por la primera letra de cada palabra del texto en el orden en que aparecen.

El participante debe implementar un algoritmo que dada una cadena de texto formada únicamente por letras minúsculas y espacios retorne el mensaje oculto.

Una palabra será la secuencia máxima de letras consecutivas que no incluyan espacios. Puede haber más de un espacio entre palabras e, incluso, puede haber texto formado sólo por espacios (en ese caso el mensaje oculto sería la cadena vacía).

Algunos ejemplos:

- Texto original: `o c u l t o`; resultado: `oculto`.
- Texto original: `otro curioso uzbeko le trajo oro`; resultado `oculto`.

Para la prueba de este ejercicio los jueces proporcionarán, de manera sucesiva, 10 textos de longitudes arbitrarias aunque **siempre con 255 palabras o menos** (es decir, el mensaje oculto tendrá una longitud inferior a 255 caracteres).

En el siguiente enlace puede encontrarse un archivo con los ejemplos anteriores en formato texto y Excel.

`http://tinyurl.com/olimpiada2012-B1`

## Segundo ejercicio

Si alguna vez has comprado algo en la Web o utilizado servicios bancarios seguramente has visto las siglas HTTPS. La S hace referencia a que la transferencia de datos es "segura", es decir, los datos han sido cifrados de tal manera que aunque fuesen interceptados el "espía" no pudiese saber qué contenido ha sido transmitido.

Son varios los algoritmos usados para cifrar esos datos pero muchos de ellos se basan en la utilización de números primos muy grandes que son multiplicados para obtener un tercer número. Uno de los primos se usa como clave pública (para cifrar) y el otro como clave privada (para descifrar).

[2]Los enunciados de los retos de esta prueba deben proporcionarse por escrito a todos los participantes junto con las Consideraciones generales.

La fortaleza de este tipo de sistemas radica en que un "espía" tendría que factorizar un número enorme y dicho número tiene, por su construcción, dos únicos factores. Así, el "espía" tendría que dedicar tanto tiempo a la factorización que para cuando pudiese descifrar el mensaje ya no tendría importancia el contenido del mismo.

Esto hace que encontrar números primos sea una tarea importante en criptografía y en este ejercicio el participante deberá implementar un algoritmo para determinar si un número es o no es primo.

Para ello debe tenerse en cuenta la definición de número primo:

*Aquel número natural mayor que 1 y que sólo es divisible por 1 y por sí mismo.*

A modo de ejemplo, los números primos menores que 100 son los siguientes:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

Para la prueba de este ejercicio los jueces proporcionarán de forma sucesiva 20 números naturales **menores que 1024** y el participante deberá indicar usando su algoritmo si el número es o no es primo.

## Tercer ejercicio

El cajero automático de un aparcamiento acepta monedas y billetes de euro y retorna cambio en monedas comprendidas entre el céntimo de euro y los dos euros.

El participante debe desarrollar un algoritmo que reciba como valores de entrada el importe a pagar y el saldo introducido por el cliente y retorne una secuencia de valores indicando cuántas monedas de 2 euros, 1 euro, 50 céntimos, 20 céntimos, 10 céntimos, 5 céntimos, 2 céntimos y 1 céntimo debería devolver el cajero.

**¡Atención!** El cajero debería devolver el menor número posible de monedas. Es decir, no sería aceptable devolver 6 céntimos en monedas de céntimo pudiendo usarse una moneda de 5 céntimos y otra de 1 céntimo. En este sentido se supondrá que la provisión de monedas del cajero es ilimitada.

Algunos ejemplos:

Importe: 3,50 €, saldo: 5 €; resultado: "0 1 1 0 0 0 0 0" (1 moneda de un euro y una moneda de 50 céntimos).

Importe: 7,35 €, saldo: 10 €; resultado: "1 0 1 0 1 1 0 0" (1 moneda de 2 euros, 1 moneda de 50 céntimos, 1 moneda de 10 céntimos y 1 moneda de 5 céntimos).

Importe: 10,02 €, saldo: 11 €; resultado "0 0 1 2 0 1 1 1" (1 moneda de 50 céntimos, 2 monedas de 20 céntimos, 1 moneda de 5 céntimos, 1 moneda de 2 céntimos y 1 moneda de 1 céntimo).

Para la prueba de este ejercicio los jueces proporcionarán de forma sucesiva 10 pares `<importe, saldo>`; el saldo siempre sera mayor o igual que el importe y no es necesario verificar este extremo.

En el siguiente enlace puede encontrarse un archivo con los ejemplos anteriores en formato texto y Excel.

`http://tinyurl.com/olimpiada2012-B3`

# Aprender a aprender[3]

El objetivo de esta prueba es conseguir uno de los tres billetes dorados encerrados en la caja fuerte custodiada en el salón de actos. Los participantes no podrán tocar en ningún momento la caja sino que deberán proporcionar la combinación a un juez que será el que verifique que, efectivamente, dicha combinación abre la caja y proporcione al participante uno de los billetes dorados (de quedar alguno).

Si todos los billetes dorados fuesen alcanzados por los participantes la clasificación tendría en cuenta los tiempos totales empleados para conseguirlos. En caso contrario se tendría en cuenta para la clasificación el número de *tokens* conseguidos por los jugadores y los tiempos parciales empleados para conseguirlos.

De este modo, estarían mejor clasificados los jugadores con más *tokens* y a igualdad de *tokens* los jugadores más rápidos.

Los *tokens* son secuencias alfanuméricas que se obtienen al resolver distintos retos que irán surgiendo a lo largo de la prueba. Dichos *tokens* deben ser anotados por el participante y proporcionados a un juez para que éste deje constancia del tiempo empleado.

**¡Atención!** Los retos de esta prueba deben resolverse en orden, cada reto saltado supondría una penalización y no eximiría al participante de resolverlo.

Los retos están organizados de tal modo que:

1. Pueden resolverse con los medios proporcionados por la organización (básicamente ordenadores con conexión a Internet).

2. Proporcionan pistas para llegar al siguiente reto y en última instancia la combinación de la caja fuerte.

3. Requieren conocimientos informáticos que, en principio, no deberían tener los participantes pero con los que no deberían tener problemas para familiarizarse al buscar documentación en la Web.

4. En ocasiones pueden requerir al participante realizar alguna actividad física.

La primera pista será proporcionada por los jueces al inicio de la prueba.

[3] La descripción de esta prueba debe proporcionarse por escrito a todos los participantes junto con las Consideraciones generales.

# Descripción extendida de la segunda prueba (no distribuir a los participantes)

La segunda prueba de la modalidad B está organizada a modo de gincana; es decir, los participantes tendrán que resolver diversos retos (siempre relacionados con algún aspecto de la informática) para obtener un *token* y una pista para el siguiente reto.

Los participantes deben anotar los *tokens* (cadenas alfanuméricas) y proporcionárselos a un juez en el salón de actos obligatoriamente; el objetivo es doble, por un lado permite llevar un control de qué retos han superado qué participantes y, por otro, los participantes pueden ver la tabla de puntuaciones y su posición en la misma.

Los participantes serán recibidos en el salón de actos donde se les comunicarán verbalmente las siguientes

## Instrucciones

1. Antes de nada los participantes deben proporcionar a la organización el alias que van a utilizar a lo largo de la prueba. Dichos alias serán los que se usen en la tabla de puntuaciones.

2. A continuación se les indicará su objetivo: obtener uno de los tres billetes dorados encerrados en una caja fuerte presente en el salón de actos. Se les indicará así mismo que nunca tendrán acceso directo a la caja y que, en consecuencia, deben obtener la combinación de la misma y proporcionársela a un juez para que la abra.

3. Para obtener dicha combinación deberán resolver una serie de retos pudiendo utilizar los recursos que localicen en la Web usando los ordenadores de un laboratorio próximo. Dicho laboratorio también tiene un teléfono por si tuviesen que utilizarlo ya que los suyos les serán retirados.

4. Cada vez que resuelvan un reto encontrarán un *token* y una pista para el reto siguiente. Dicho *token* debe ser anotado y llevado con un juez al salón de actos para que quede constancia del tiempo empleado por cada participante.

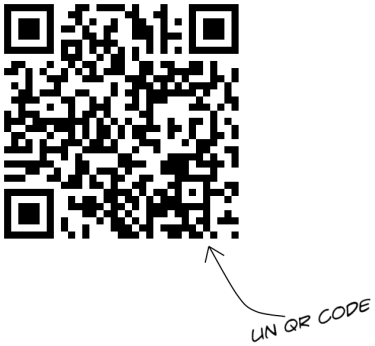
5. Los retos deben superarse en orden, si alguien se saltase algún reto sería penalizado y aún así el reto saltado debería completarse.

6. Los participantes no pueden hablar entre ellos ni con sus tutores, sólo con los miembros de lo organización y siempre en privado.

7. El comienzo de la prueba se realizaría de manera escalonada como en la primera prueba.

## Descripción de los retos (no distribuir a los participantes)

- Todos los participantes serían conducidos a un laboratorio donde entrarían en sesión de forma escalonada (ESO, Bachillerato y CFGM, CFGS).
- Al entrar en sesión se encontrarían con un entorno Windows "estándar" con la salvedad de que el fondo de escritorio es un código QR[4]. La imagen tendría, además, el texto `QR Code`.




- Al no proporcionarse más información desde la organización es de esperar que los participantes supongan que el código QR es la primera pista. En consecuencia buscarían un lector de QRs (podría ser una aplicación para Windows o bien una aplicación online) y lo aplicarían sobre la propia imagen o sobre una captura de pantalla. De ese modo obtendrían una URL que les llevaría a una página[5] que contendría el **primer *token*** (`105a3`) y un segundo enlace.
- Con el primer *token* aparecería un recordatorio de que el *token* debe ser anotado y comunicado a un juez para actualizar la tabla de puntuaciones. Una vez hecho eso podrían volver a trabajar sobre el segundo enlace.
- **Tiempo estimado para este primer reto: entre 5 y 30 minutos (incluyendo la visita al salón de actos).**
- Dicho enlace permite descargar un archivo de nombre `noesloqueparece.txt`[6]. Al abrir el archivo con un editor (p.ej. Notepad) aparecería en la primera línea algo semejante a `Rar! Ïs Ö.t 4 o J ÷g=:=3`... Teniendo en cuenta el nombre del archivo, la apariencia absolutamente extraña del texto y el comienzo `Rar!` del mismo parece razonable suponer que los participantes deduzcan que hay que cambiar la extensión del archivo a `.rar` y tratar de descomprimirlo.
- Al descomprimir el archivo encontrarían dos ficheros: `leeme.txt` y `DTMF.wav`. El primero contendría el **segundo *token*** (`1548a`) y el recordatorio de transmitirlo a un juez mientras el segundo sería un archivo de audio.

[4] http://en.wikipedia.org/wiki/QR_code
[5] http://tinyurl.com/olimpiada2012-QR
[6] http://156.35.98.175/apache2-default/olimpiada2012/noesloqueparece.txt

- **Tiempo estimado para el segundo reto: entre 10 y 20 minutos.**

- Tras transmitir el segundo *token* volverían a escuchar el archivo que correspondería al sonido de un teclado telefónico. Por otro lado, al introducir las siglas DTMF en un buscador descubrirían que, efectivamente, es una forma de enviar señales por líneas analógicas. Además, si usan Google (bastante probable) encontrarían como segunda recomendación la consulta `dtmf decoder` que les permitiría acceder a varios decodificadores de ese tipo de señales. De ese modo obtendrían el número 71044 (un número de teléfono interno de la universidad).

- Es de esperar que en ese momento recuerden que se les señaló que tenían un teléfono que podían usar llegado el caso y que, en consecuencia, prueben a marcar el número obtenido. Al llamar a dicho número oirían una grabación que les proporcionaría un par de números reales separados por una coma (i.e. las coordenadas GPS 43.354344, -5.852537).

- Con independencia de que reconozcan la pista como coordenadas si utilizan Google obtendrían un mapa que les mostraría una localización próxima al lugar de celebración de la olimpiada. Puesto que para dicha localización no habría fotografías de Google Street View no les quedaría otra opción que visitarla físicamente. En ese lugar encontrarían un cartelón con 3 líneas de texto[7]; la primera sería el **tercer *token*** (`7080a`) que estaría claramente señalado, la segunda seria el texto cifrado `YNPBZOVANPVBAQRYNPNWNRFQBFFRVFGERFHAB`, y la tercera y última sería el texto `ROT13` escrito a modo de firma de grafitero. Los participantes volverían con el *token* que proporcionarían a un juez y tratarían de resolver la pista.

- **Tiempo estimado para el tercer reto: entre 20 y 45 minutos.**

- Al tratarse de una pista tan extraña es de esperar que traten de utilizar un buscador. El texto cifrado no va a producir ningún resultado pero sí `ROT13`. De hecho, descubrirán que se trata de un sistema de cifrado sencillo y entre los resultados encontrarán herramientas para descifrar el mensaje obteniendo el siguiente texto plano: `LACOMBINACIONDELACAJAESDOSSEISTRESUNO`, es decir, la combinación de la caja (2631) que es el objetivo final de la prueba.

- Con esa combinación el participante iría a un juez que debería verificar la combinación, abrir la caja, entregar el billete dorado (de haberlo) y cargar el *token* del billete (`b5b42`) que tendría como consecuencia la actualización de la tabla de puntuaciones señalando que el participante ha terminado la prueba.

- **Tiempo estimado para el cuarto reto: entre 5 y 20 minutos.**

- **Tiempo total estimado: entre 40 y 115 minutos.**

[7] Puesto que un error en la transcripción del texto cifrado sería muy problemático el cartelón incluiría un enlace acortado donde encontrarían el mismo texto.

## Aspectos logísticos (no distribuir a los participantes)

- Generales:
  - **PENDIENTE:** Debe prepararse una hoja de cálculo en la que anotar tiempos y estado de cada reto en cada prueba.
  - **PENDIENTE:** Debe disponerse de un cronómetro global para la toma de tiempos.
  - **PENDIENTE:** Los ordenadores deben disponer de navegador, conexión a Internet, Excel y los entornos de programación solicitados por los participantes.
- Primera prueba:
  - **PENDIENTE SEGUNDO SERVIDOR:** Deben prepararse archivos de ejemplo en formato texto y Excel y colgarse en dos servidores diferentes.
  - **PENDIENTE:** Deben prepararse archivos de prueba en formato texto y Excel y colgarse en dos servidores diferentes.
- Segunda prueba:
  - **PENDIENTE:** Debe prepararse una infraestructura web para los retos de la gincana y colgarse en dos servidores diferentes.
  - **PENDIENTE:** Debe prepararse una infraestructura web para el tablero de puntuaciones. Dicha aplicación debería permitir anotar tiempos asociados a cada alias, mostrar iconos para retos y penalizaciones y proporcionar una fanfarria para los 3 mejores y un mensaje para los siguientes participantes que terminen el reto.
  - **HECHO:** Debe prepararse un QR code con el primer enlace.
  - **HECHO:** Debe prepararse un archivo de audio con los tonos del teléfono.
  - **HECHO:** Debe prepararse un archivo .rar con el token y el archivo de audio.
  - **HECHO:** Debe prepararse un mensaje grabado con las coordenadas.
  - **PENDIENTE IMPRESIÓN:** Debe prepararse el cartelón con el mensaje cifrado.
  - **HECHO:** Debe prepararse un enlace acortado con el texto del cartelón.
  - El cartelón con el mensaje cifrado debe situarse en las coordenadas **una vez** los participantes están en el laboratorio y no antes.
  - **PENDIENTE:** Deben prepararse los billetes dorados.
  - **PENDIENTE:** Todos los ordenadores del laboratorio deben disponer de altavoces o auriculares.
  - **PENDIENTE:** Todos los ordenadores del laboratorio deben contar con una cuenta olimpiada/olimpiada y estar configurados para mostrar las extensiones de los archivos.