KeyGen Crackme4

(Imprescindible leer el tute de Holy, para comprender lo siguiente.
http://www.mediafire.com/?eacxwgt829qcx05)

Como bien nos dijo Holy en su excelente tute, nos hacen falta 6 clicks en el formulario, en el que sumando las coordenadas de cada click, y multiplicadas cada suma de coordenadas por una serie de constantes, nos debe dar cierto número, en concreto:

Solución= 57230157830.4546

Parece complicado y desde luego la única forma factible de hallarlo parece la fuerza bruta. Con esta perspectiva vamos a analizar las operaciones que se hacen con el primer click:

Siendo x = suma de coordenadas (x, y) del primer click

$$Resultado\ Click1 = x \times 9368 \div 3 \times 37 \div 13 \times 5389 \div 62$$

(Tener en cuenta que las operaciones van de izquierda a derecha, es decir, primero se multiplica x por 9368, el resultado se divide por 3, el resultado se multiplica por 37 …. Etc.)

Si nos damos cuenta se puede reducir todo a la multiplicación de x por una constante que englobe todas las operaciones, esta es:

$$Resultado\ Click1 = x \times 772503{,}56658395247930$$

Si hacemos lo mismo con el resto de los 6 clicks necesarios, quedaría:

$$Click1 = x \times 772503{,}56658395247930$$

$$Click2 = x \times 526614{,}93450000004410$$

$$Click3 = x \times -12078{,}14497516970734$$

$$Click4 = x \times 125{,}23620521581043020$$

$$Click5 = x \times 153475{,}07812054474060$$

$$Click6 = x \times 1789376{,}2442508705100$$

La solución sería:

$$final = 57230157830{,}4546 = \text{Click1} + \text{Click2} - \text{Click3} + \text{Click4} + \text{Click5} + \text{Click6}$$

Es de resaltar la resta que se efectúa con el click3, si miramos la constante que multiplica a la suma de coordenadas, esta es negativa, por lo tanto el Click3 será negativo por lo que esta resta en realidad será una suma y por ello la trataremos a partir de ahora como una suma (y la constante en lugar de negativa la tomaremos como positiva).

Bruteando

Viendo las constantes, me entro una sensación de Deja vú, que me recordaba mucho al crackme de Eddy (que recuerdos!!) (http://ricardo.crver.net/WEB/CONCURSOS 2009/CONCURSO 19/InDulgEo CrackMe by asOlOt.pdf)

Entonces enfoque la solución del mismo modo, que en el crackme mencionado.

Maximos y Minimos

Hallaremos la tabla de máximos y mínimos de los valores que se pueden obtener con los clicks.

En primer lugar debemos tener en cuenta el valor máximo y el valor mínimo que pueden tener las coordenadas. Aquí tendremos en cuenta solo un recuadro que englobe al pibón, ya que si pasamos el ratón por encima de los statics, edits, etc, vemos que las coordenadas no se actualizan, por esto nos centraremos solo en la imagen de la señorita (acaso podemos dejar de mirarla…).

Yo he escogido como máximo 19995 y como mínimo 12000. (Estos valores son la suma de las coordenadas del punto en el que podemos decir tiene los limites la titi, aunque seguramente se puede ajustar mas)

Ahora como ejemplo nos centraremos en el Click6. Escogemos este evento, por ser el que tiene la constante mayor, de hecho a partir de ahora ordenaremos los clicks por el tamaño de la constante que entra en juego en la multiplicación.

Coordenadas máximas = 19995

Suponemos que hacemos click en las coordenadas máximas las 5 primeras veces. Entonces habría que multiplicar 19995 por las constantes de cada click y sumarlo. Vamos a hacerlo con los 5 primeros clicks:

$$\begin{aligned}&(19995 \times 772503{,}56658395247930)\\ +\ &(19995 \times 526614{,}93450000004410)\\ +\ &(19995 \times 12078{,}144975169707340)\\ +\ &(19995 \times 125{,}23620521581043020)\\ +\ &(19995 \times 153475{,}07812054474060)\\ =\ &29288615222{,}895731221495149\end{aligned}$$

Si a la solución final le restamos el número obtenido:

$57230157830{,}4546 - 29288615222{,}895731221495149 = 27941542607{,}558868778504851$= rangoMinClick6

Con esta serie de operaciones hemos hallado el mínimo que debe dar la multiplicación de la constante por las coordenadas del click 6, ya que cualquier valor por debajo, no llegara a la solución final. Dicho de otro modo nuestro programa de fuerza bruta en el click6 si no estamos dentro de este rango no seguiremos con los demás, ya que sería inútil.

Para calcular los máximos habría que poner el valor mínimo que podemos obtener con los clicks, 12000.

$$\begin{aligned}&(12000 \times 772503{,}56658395247930)\\ +\ &(12000 \times 526614{,}93450000004410)\\ +\ &(12000 \times 12078{,}144975169707340)\\ +\ &(12000 \times 125{,}23620521581043020)\\ +\ &(12000 \times 153475{,}07812054474060) = 17577563524{,}6185933812424\end{aligned}$$

$57230157830{,}4546 - 17577563524{,}6185933812424 = 39652594305{,}8360066187576$= rangoMaxClick6

Con esto tenemos que cuando un sexto click pase de este valor, podemos dejar de hacer las siguientes combinaciones, ya que el resultado sería mayor que la solución buscada.

Teniendo estas bases solo que da hacer el programa para que mediante la fuerza bruta nos de las coordenadas.

El esquema que debe seguir el programa es:

- Definir el máximo y mínimo que pueden tener los clicks (yo he definido max = 19995 y min= 12000, siempre pensado hacer click en el pibón… jejeje).
- Calcular los rangos para cada paso.
- Hacer los incrementos de nuestras coordenadas de 15 en 15 (como lo hace el programa)
- En cuanto un click se sale de su rango, volvemos al anterior. Así descartaremos hacer combinaciones inútiles.

Un diagrama del flujo del programa lo tenéis al final del doc.

Esta es una solución que se llega en menos de una hora (seguro que habrá más).

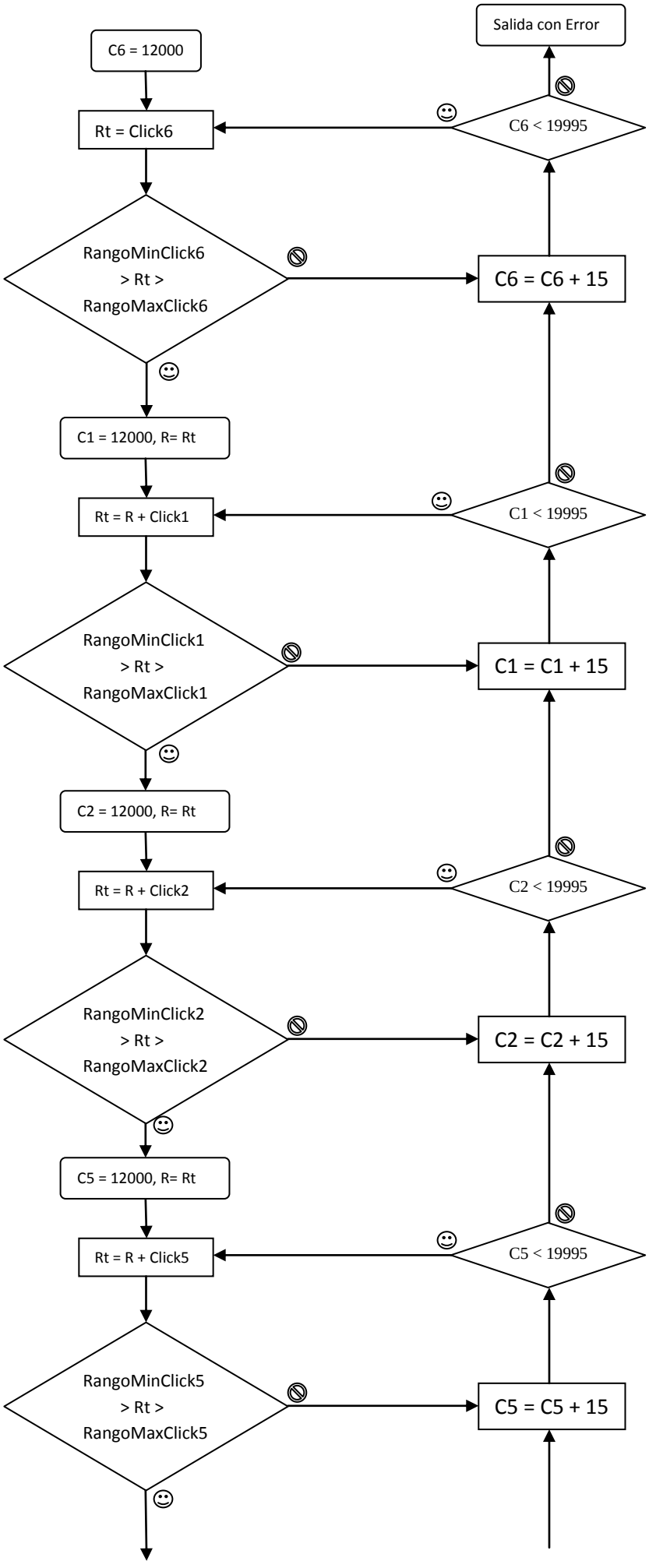
Click 1 = 19110 (12000, 7110)
Click 2 = 16590 (12000, 4590)
Click 3 = 19590 (12000, 7590)
Click 4 = 13800 (12000, 1800)
Click 5 = 17460 (12000, 5460)
Click 6 = 17220 (12000, 5220)

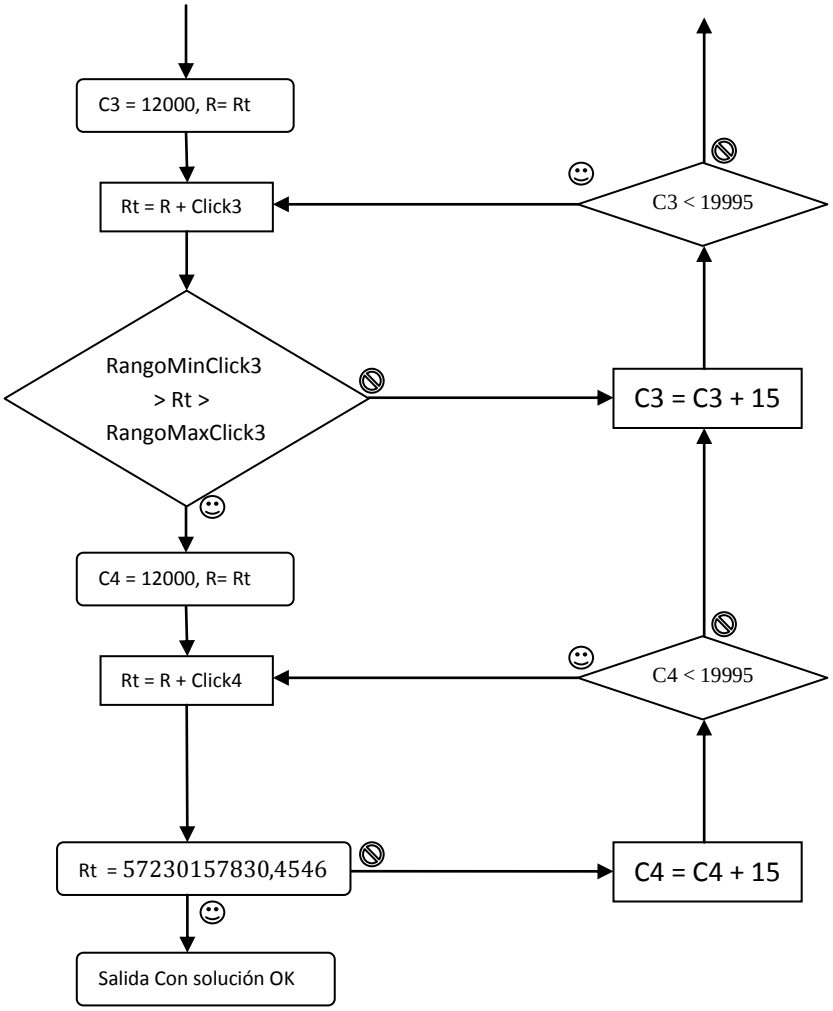
Como veis he escogido en todas una X de 12000, por comodidad, pero con tal de que se cumpla la suma puede ser cualquier otra combinación.

Gracias a Holy por su esplendido tute, y al creador del crackme tincopasan.

Saludos

asOlOt, 2012


Salida con Error
C6 = 12000
Rt = Click6
C6 < 19995
RangoMinClick6
> Rt >
RangoMaxClick6
C6 = C6 + 15
C1 = 12000, R= Rt
Rt = R + Click1
C1 < 19995
RangoMinClick1
> Rt >
RangoMaxClick1
C1 = C1 + 15
C2 = 12000, R= Rt
Rt = R + Click2
C2 < 19995
RangoMinClick2
> Rt >
RangoMaxClick2
C2 = C2 + 15
C5 = 12000, R= Rt
Rt = R + Click5
C5 < 19995
RangoMinClick5
> Rt >
RangoMaxClick5
C5 = C5 + 15


C3 = 12000, R= Rt
Rt = R + Click3
C3 < 19995
RangoMinClick3
> Rt >
RangoMaxClick3
C3 = C3 + 15
C4 = 12000, R= Rt
Rt = R + Click4
C4 < 19995
Rt = 572301578 30,4546
C4 = C4 + 15
Salida Con solución OK