

 [Deja News](#)[Home](#) · [Resource Directories](#) [Quick Search](#) · [Power Search](#) · [Search Filter](#) · [Interest Finder](#) · [Browse Groups](#) [Wanna write code? Need more resources? Sign up here for help.](#)[Wanna write code? Need more resources? Sign up here for help.](#)**Article 3 of exactly 18**[Text Only](#)  [Help](#)  [\[](#)  [\[](#)  [\[](#)  [\[](#)  [\[](#)[Previous Article](#) [Next Article](#) [Current Results](#) [View Thread](#) [Post Message](#)

Subject: **RC5 Bovine - encontrada la solución**
From: **alvy@idg.es (Alvaro Ibanez)**
Date: **1997/10/23**
Message-ID: **<alvy-2310971621380001@194.133.96.49>**
Newsgroups: **es.comp.hackers**
[\[More Headers\]](#)

Este mensaje es simplemente para anunciar que el concurso de RSA para crackear el código RC5-32/12/7 56-bit ha terminado. A las 13:25 GMT del 19-Oct-1997 se encontró la clave correcta (0x532B744CC20999) que se había estado buscando durante 250 días. El mensaje era

"It's time to move to a longer key length"

("Es hora de pasar a usar claves más largas")

Bovine RC5 ha sido calificado como "el mayor esfuerzo computacional de todos los tiempos", realizado a través de Internet mediante ordenadores de todo el mundo (4.000 equipos de todo el mundo). El primer equipo español está en el puesto #79 linux@jet.es.

La potencia de todas las máquinas conectadas a **distributed.net** es equivalente a

16.685 Pentium/200
13.362 PowerPC 604e/200

La clave la encontró Peter Stuer con un Intel Pentium Pro 200 bajo Windows NT, trabajando en el equipo STARLab Bovine Team coordinado por Jo Hermans y con sede en el Computer Science Department (DINF) de la Vrije Universiteit (VUB) de Bruselas, Bélgica (<http://dinf.vub.ac.be/bovine.html>).

Los únicos comentarios de Jo fueron que "con \$1000 se puede comprar un montón de cerveza..." y que "hubiera deseado que la solución la hubiera encontrado un Macintosh, la plataforma que representaba la mayor parte de la potencia de cálculo de nuestro equipo."

Más información en <http://www.distributed.net/pressroom/56-PR.html>

Más sobre **distributed.net** en <http://www.distributed.net>

y temas similares

RSA Labs: <http://www.rsa.com/rsalabs>
RSA Secret Key Challenge: <http://www.rsa.com/rsalabs/97challenge>

Saludos digitales,

Alvaro Ibanez e-mail personal: alvy@idg.es

 [Wanna write code? Need more resources? Sign up here for help.](#)[Wanna write code? Need more resources? Sign up here for help.](#)[Previous](#) | [Next](#) | [Results](#) | [View Thread](#) | [Author Profile](#) | [Post Message](#) | [Post Reply](#) | [Send Email](#)

Copyright © 1995-97 [Deja News, Inc.](#) All rights reserved.