[an error occurred while processing this directive]

# Official List Announcement
# October 22, 1997

It is a great privilege and we are excited to announce that at 13:25 GMT on 19-Oct-1997, we found the correct solution for RSA Labs' RC5-32/12/7 56-bit secret-key challenge. Confirmed by RSA Labs, the key 0x532B744CC20999 presented us with the plaintext message for which we have been searching these past 250 days.

The unknown message is: It's time to move to a longer key length

In undeniably the largest distributed-computing effort ever, the Bovine RC5 Cooperative (http://www.distributed.net/), under the leadership of distributed.net, managed to evaluate 47% of the keyspace, or 34 quadrillion keys, before finding the winning key . At the close of this contest our 4000 active teams were processing over 7 billion keys each second at an aggregate computing power equivalent to more than 26 thousand Pentium 200's or over 11 thousand PowerPC 604e/200's. Over the course of the project , we received block submissions from over 500 thousand unique IP addresses.

The winning key was found by Peter Stuer with an Intel Pentium Pro 200 running Windows NT Workstation, working for the STARLab Bovine Team coordinated by Jo Hermans and centered in the Computer Science Departm ent (DINF) of the Vrije Universiteit (VUB) in Brussels, Belgium. (http://dinf.vub.ac.be/bovine.html/). Jo's only comments were that "$1000 will buy a lot of beer" and that he wished that the solution had been found by a Macintosh, the platform that repr esented the largest portion of his team's cracking power. Congratulations Peter and Jo!

Of the US$10000 prize from RSA Labs, they will receive US$1000 and plan to host an unforgettable party in celebration of our collective victory. If you're anywhere near Brussels, you might want to find out when the party will be held. US$8000, of course , is being donated to Project Gutenberg (http://www.promo.net/pg/) to assist them in their continuing efforts in converting literature into electronic format for the public use. The remaining US$1000 is being retained by distributed.net to assist in fund ing future projects.

Equally important are the thanks, accolades, and congratulations due to all who participated and contributed to the Bovine RC5-56 Effort! The thousands of teams and tens of thousands of individuals who have diligently tested key after key are the reason we are so successful.

The thrill of finding the key more than compensates for the sleep, food, and free time that we've sacrificed!

Special thanks go to all the coders and developers, especially Tim Charron, who has graciously given his time and expertise since the earliest days of the Bovine effort. Thanks to all the coordinators and keyserver operators: Chris Chiapusio, Paul Chvost ek, Peter Denitto, Peter Doubt, Mishari Muqbil, Steve Sether, and Chris Yarnell. Thanks to Andrew Meggs, Roderick Mann, and Kevyn Shortell for showing us the true power of the Macintosh and the strength of its users. We'd also like to thank Dave Avery for attempting to bridge the gap between Bovine and the other RC5 efforts.

Once again, a heartfelt clap on the back goes out to all of us who have run the client. Celebrations are in order. I'd like to invite any and all to join us on the EFNet IRC network channel #rc5 for celebrations as we regroup and set our sights on the n ext task. Now that we've proven the limitations of a 56-bit key length, let's go one further and demonstrate the power of distributed computing! We are, all of us, the future of computing. Join the excitement as the world is forced to take notice of th e power we've harnessed.

Moo and a good hearty laugh.

Adam L. Beberg - Client design and overall visionary
Jeff Lawson - keymaster/server network design and morale booster
David McNett - stats development and general busybody

[an error occurred while processing this directive]