

[an error occurred while processing this directive]

Official List Announcement January 9, 1999

Greetings from distributed.net!

I'm extremely pleased to announce that our DES-TEST-1 contest was a success. Not only were we able to evaluate the performance and reliability of our new v300 ("devel") proxies and our v2.7103 clients with quick-start, but we successfully found the key after only 59 hours of searching. The key, 0x5ED9204FECE0B967, was able to recover the plain-text message, "The unknown message is: The DES-test contest's plaintext" We have yet to contact the individual who was running the lucky client, so I won't release his/her email address yet. If (s)he has no objection, I'll announce the winner in another email. The winning block was cracked on a Macintosh PowerPC in the US running v2.7103 of the rc5des client and submitted at 04:17:13 GMT on 01/09/98.

This contest was able to reinforce the astounding growth of distributed.net, both in terms of our CPU power, but also in regards to the amazing functionality of our v2.7103 clients. Within a couple hours of DES-TEST-1's start time, the keymaster was reporting DES rates of over 20Gkey/s. During DES-II-2, it took us about 20 hours to reach that rate.

We would like to thank everyone who participated. This extensive testing allowed us to learn weaknesses of our current quick-start implementation, and we will be able to improve it for maximum performance and efficiency.

However, in order to ensure near-flawless operations during the actual DES-III contest, we would like to announce distributed.net's second DES test challenge, named DES-TEST-2. This challenge will commence at 09:00am PST on Tuesday, January 12th. To simulate a real DES challenge where we have a time limit, we will stop the challenge if the key has not been found within 56 hours.

If you haven't already, please upgrade your clients to v2.7103. You can find the newest clients at <http://www.distributed.net/clients.html> or directly off the FTP site at <ftp://ftp.distributed.net/pub/dcti/v2.7103/>.

Thanks for your support,

[Daniel Baker](mailto:dbaker@distributed.net) dbaker@distributed.net

[an error occurred while processing this directive]