

[an error occurred while processing this directive]

Official List Announcement January 15, 1999

Greetings from distributed.net!

Our DES-TEST-2 was a successful failure, in that we didn't find the key within the 56 hour time frame, but we were able to fully test the functionality of the clients and proxies. It turns out that the key was assigned a few hours before the contest closed, but wasn't returned in time for a "win." A sincere thanks to everyone who had their client participate in the contest.

Now, the big topic. DES Challenge III. DES-III begins at 09:00:00PST/17:00:00UTC on 99-01-18 which is just next Monday.. We have 56 hours to find the key. While this may sound difficult, since we didn't find it in our second test, keep in mind that there are lots of other elements that will allow us to speed up between now and then. One of the major factors is EFF's Deep Crack. It's now official, this custom made DES cracking machine will be checking keys for distributed.net at the rate of 88Gkey/s.

Many of you have expressed concern to me about having your clients crunch DES since you won't get ahead in RC5 stats. First of all, I would like to remind you that DES-III is very important to distributed.net. This is our chance to show that large scale Internet distributed computing can be used for short term contests such as this one. We will be hosting DES-III statistics, so don't worry about not having stats throughout the contest.]:8) At most, this is just 56 hours of your cracking time, so we would appreciate it very much if you could put RC5 aside on Monday and check DES keys.

Please take the time and upgrade your clients to the latest v2.7105 clients available on <ftp://ftp.distributed.net/pub/dcti/v2.7105/> and <http://www.distributed.net/clients.html>. For those of you who haven't upgraded recently, the newer v2.710x clients have DES quick-start code which allows clients to start cracking DES shortly after the contest begins instead of having to wait for the clients to automatically flush/fetch blocks. Also, v2.7105 contains Bruce Ford's new DES MMX cores. For those of you with x86 MMX processors, you will see a huge speed increase. I highly recommend you upgrade and be sure you have DES enabled in your client configuration.

Please be careful about buffers during this contest. We need quick turnaround with blocks for this contest, so don't keep hundreds or thousands of blocks buffered. A setting of 5:5 would be perfect for the average online client. Personal proxies tend to minimally buffer about 500 blocks, so please don't run a pproxy unless your situation demands that you do.

Thanks again to everyone running the client and to everyone who has been burning the midnight fuel to get this off the ground. Feel free to join us in our IRC channel (efnet: #distributed) on Monday to watch this take off.

Good Luck!

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

[an error occurred while processing this directive]