[an error occurred while processing this directive]

CSC Announcement, 9-Jan-2000

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

Behind the scenes, we've been viewing the rapid approach of 100% CSC keyspace completion with mixed feelings. While it's exciting to see how fast we are all tearing through the keyspace, a bit of pre-100 nervousness is to be expected.

When we passed 90% on the statsbox, we decided to explain the impact of work duplication (as detailed in dbaker's plan the other day) because it looked like we might hit an apparent 100% keyspace completion. Anticipating the chance that our work re-verification system might eventually lead to an "over 100%" state on statsbox, we made the announcement explaining its impact.

At the same time, we stepped up our investigation into computer errors and malicious vandalism. Throughout the project, we have kept watch for anything out of the ordinary that might lead to a problem in our key processing. As the big 100 drew near, our suspicions began to rise...

So did the suspicions of many of our users, but until now we've had nothing concrete to tell you. This has changed.

During the the latter part of our search, a clue smacked us in the face and eventually led us to a serious problem, one which affected a section of CSC work performed to date. We received a success packet on the master but were unable to use the reported key to decrypt the ciphertext. By backtracking the reported success, we uncovered an issue which affected the keyspace assignments done by the keymaster. Soon we had isolated it to a specific version of the keymaster code. The bad news: for a period of time, the keymaster was generating blocks with corrupted contest information, making those blocks invalid. Thankfully, the error only affected the CSC contest and not the RC5-64 contest data.

However, the minor error had a major impact on CSC. Roughly 25% of the CSC keyspace was affected by the block corruption. Fortunately, we were able to flag the invalid blocks as "untested", and start dumping them back to clients immediately.

What this means is that a quarter of the CSC work done to date was invalid and needs to be re-tested. Rather than 100% complete, in actuality we're only 75% through the keyspace -- about a week away from true completion, at current rates. It's very fortunate that our user base is so powerful that we can recoup the losses well before this contest comes to a close. It should also be noted that this error actually occured a few weeks ago and was in-advertantly corrected before we knew there was a problem. Because of this, there is no need to dump your buffers; the bad blocks are no longer in the pipeline.

We will be amending the percentage complete reported by the stats server to reflect our true keyspace completion. Participants will still receive full credit for their completed blocks, regardless of their validity. In the near future we will be supplying the stats server with the information it needs to properly discount the effects of any reverification work in the reported percentage.

We realize that a setback of just over a week is quite annoying in a short contest like CSC, but it's entirely possible that the winning key is working its way back to the keymaster right now.

To have passed this problem into the production network is seriously embarrassing. Simply put, we have failed in our responsibility to the users running our client, and we will do everything we can to ensure this never happens again. Despite coordinating some of the most powerful networks on earth, distributed.net is still run by those fallible human being types. We obviously need better testing procedures.

We already have a reliable system in place for client and core coders, to test the proper function of new and beta client code revisions. However, it's now quite apparent that we're lacking an equivalent sandbox (or process) to test changes in the keymaster code and network structure. With recent major revisions to the keymaster code (for OGR, CSC, and others) it's clear that this situation cannot continue.

As a result, distributed.net has committed to building a keyserver testing

environment, complimenting our existing client-tests area. For a very long time the keymaster code was static enough that such a provision wasn't really necessary, but as we undertake more projects this will become less and less true.

We'll also take this time to step back and carefully chart a more reliable route through our development cycle, ensuring that errors and mistakes can be caught long before they would enter production.

On behalf of distributed.net, I'd like to apologize to our users -- and also thank you. The magnitude of your support has given us all a good chance at recovery, despite enormous keyspace fallout. We have learned our lesson, and we're very, very sorry. Now, with your help... let's finish this thing.

David McNett
nugget@distributed.net

-----BEGIN PGP SIGNATURE-----
Version: PGP 5.0
Charset: noconv

iQA/AwUBOHgjqrN5xKXkPF/DEQItuACgyoBsRcjiyxF+GUuatLUyV6tUWE8AoKpZ
MJG/OlgfAaI6B6P9JtrlBoh7
=Qw/F
-----END PGP SIGNATURE-----

[an error occurred while processing this directive]