

It is with considerable excitement (and quite a bit of relief) that I can now announce that the DES-III contest is officially ended.

At 07:15 am PST (14:15 UTC), just about the time when we all started getting worried about the 24-hour waypoint, the solution to DES-III arrived. The winning key, 92 2C 68 C4 7A EA DF F2, revealed the plaintext message:

The unknown message is: See you in Rome (second AES conference, March 22-23, 1999

The winning key was found by EFF's Deep Crack hardware, and submitted to the distributed.net servers immediately. RSA confirmation of the success followed shortly thereafter.

It's truly been a joy and a thrill to work with John Gilmore and the other talented and clued people at EFF. Were it not for their contributions to distributed.net, the 24-hour deadline would have been a much more difficult goal to reach.

I'll be running stats for the partial 19-Jan work up to the point of success and posting them this afternoon for the archives.

More details will follow soon as the dust settles, RSA is planning a 12:00 noon PST announcement at the RSA '99 Convention. Both John Gilmore and our own Peter Gildea will be in attendance.

Here's a few statistics on our aggregate success:

Start of contest:	January 18, 1999 at 09:00 PST
End of contest:	January 19, 1999 at 07:15 PST
Elapsed Time:	22 hours 15 minutes
Percentage Complete:	22.2%
Size of key space:	72,057,594,037,927,936
Keys Tested:	16,017,142,616,948,736
Blocks Tested:	29,834,253
Overall Keyrate:	199 Gkeys/sec
Peak Keyrate:	250 Gkeys/sec