

 Search


 S

 DocFind

 S

 Home



 From Network World Fusion:

DES code cracked in record time

By Jason Meserve

Network World, 01/20/99

Records are made to be broken.

Proving that the world record for deciphering a DES-encoded message is no different, a global team of computer users yesterday grabbed the less-than-year-old title.

The distributed.net team, a non-profit organization of computer hobbyists, deciphered a DES-encoded message in just over 22 hours as part of the RSA Data Security's DES Challenge III.

With an estimated 100,000 computers in the distributed.net network and a customized code-cracking computer from the Electronic Frontier Foundation (EFF), the crew smashed the previous record of 56 hours set back in July 1998 by EFF's "Deep Cracker." Therefore, security company RSA, the contest's sponsor, will award the group \$10,000.

"We're obviously quite pleased of our accomplishments," says David McNett, co-founder of distributed.net. "We've gone further in proving the [Data Encryption Standard] and 56-bit cryptography are dead."


DES is a private-key encryption standard developed by IBM and adopted by the government in 1977.

RSA has sponsored three such contests to prove to the government that 56-bit encryption technology is too weak and that encryption export restrictions must be lifted. Currently, encryption technology stronger than 56-bit cannot be exported outside the U.S.

For DES Crack III, RSA placed a 56-hour time restriction on the contest, with a \$10,000 prize for cracking the code in less than 24 hours, \$5,000 for less than 48 hours and \$1,000 for less than 56 hours. The stringent time constraints help prompt the previous two contest winners to join together.

Deep Cracker ultimately uncovered the plain text message "See you in Rome (second AES Conference, March 22-23, 1999)." The message is a plug for the proposed Advanced Encryption Standard initiative that is being proposed by the government in conjunction with private companies as a replacement for DES.

EFF's Deep Cracker was built using a standard PC

 For more info:

[Distributed.net's Web site](#)

[RSA Statement on contest winner](#)

[Government to review 15 DES alternatives](#)
Network World,
8/24/98

[U.S. gov't's encryption standard cracked in record time](#)
Network World,
7/20/98

Today's breaking news

Get daily news delivered to your mailbox with a [free NetFlash subscription](#)

[Lucent's income, overseas sales rise sharply](#)

[Lotus details SmartMove program](#)

[Cisco, NAI, Lucent form research group](#)

[DES code cracked in record time](#)

[Microsoft Q2 earnings soar 74%](#)

[More breaking news](#)

[Ascend deal plugs Lucent ATM leaks](#)

[Swedish trio touts ATM alternative](#)

[SNA development ties Linux to mainframes](#)

[Grass-roots effort pulls SGI toward Linux](#)

[Review and buyer's guide: FRADs](#)

[More news from Network World](#)

 IDG.net




and some 1,500 custom chips for cracking DES encryption by John Gilmore, EFF co-founder and project leader.

Adding Deep Cracker's processing power, distributed.net uses the idle-process time of standard PCs that are connected to the Internet. The organization advertised its need for computing power on its Web site and through its members' newsletter. People wishing to participate in the contest with distributed.net needed only to download a special client that ran in the background, crunching away at assigned blocks of DES keys using a method of brute force - testing every possible combination until the message was uncovered. Keys were distributed to clients via 22 key servers located around the world. A single keymaster oversaw the entire operation.

Combined, the two systems were processing some 245 billion keys per second and had covered 22.2% of the available key space - some 72 quadrillion keys. Luck is somewhat involved in such a process, as the key could have been in the latter percentage of the key space, as it was in the first DES Crack contest when 91% of the key space had been tested before a solution was found, McNett says.

"[This type of system] allows the average person, who cannot purchase some outstanding machine like a Cray supercomputer, to combine their computer's power with others to handle extraordinary complex problems," says Daniel Baker, distributed.net's chief operations officer.

Baker and McNett see the power of distributed computing spreading to more complex problems in the future, not just cracking cryptography codes. "This is the killer app for the Internet - distributed computing," McNett says.



[Feedback](#) | [Network World, Inc.](#) | [Advertiser Index](#)
[How to Advertise](#) | [Copyright](#) | [Terms of Service](#)

[Home](#) | [News](#) | [Reference](#) | [Newsletters](#) | [Forums](#) | [Opinions](#)
[Careers](#) | [Site Map](#) | [What's New](#) | [NW Subscriptions](#)
[Seminars & Events](#) | [Product Showcase](#)
[InfoXpress](#) | [Research Reports](#) | [Vendor white papers](#)