FORMAL PRESS RELEASE

For Immediate Release
January 19th, 1999

Contact: David McNett
205-458-8208

US GOVERNMENT'S ENCRYPTION STANDARD BROKEN IN LESS THAN A DAY

BIRMINGHAM, AL (January 19, 1999) For the second time in as many years, the US government's standard data encryption algorithm (Data Encryption Standard, or DES) has fallen to a brute-force attack by Distributed Computing Technologies, Inc. (distributed.net), a not-for-profit organization dedicated to the advancement of distributed computing. As part of a contest sponsored by RSA Labs, and working in conjunction with the Electronic Frontier Foundation, distributed.net successfully found the correct key to decrypt the message 'See you in Rome (second AES Conference, March 22-23, 1999)' in less than 24 hours. "It has already been proven that DES doesn't protect well against a brute force attack," said David McNett, one of distributed.net's primary coordinators, "but what this effort shows is that data encrypted with DES is safe for less than a day." In previous contests, DES was cracked in 96 days by Rocke Verser, 41 days by distributed.net, and 56 hours by Deep Crack.

The attack was accomplished using EFF's 'Deep Crack', a purpose built DES cracking machine, and the idle CPU time of around 100,000 computers around the world. These computers ranged from lowly early 1990's PCs up to powerful multi-processor machines. These machines ran a small software program that sits quietly in the background and uses CPU time that would otherwise be wasted.

Not wasting any time, distributed.net has already resumed its attack on a stronger encryption protocol (64 bit RC5), another contest sponsored by RSA Labs. Preparations are also underway to work on finding more Optimum Golumb Rulers, which are useful for determining the spacing between devices in a measurement array, such as a radiotelescope. "Our true purpose is exploring the concepts of distributed computing. Our growth has been nothing short of remarkable and I am confident that we will continue 'pushing the envelope' of large scale Internet distributed computing," stated Daniel Baker, another organizer, shortly after the contest closed. "Our initial explorations of distributed computing represent only a very rudimentary use of the massive amount of normally wasted computational power sitting idle in the world. We hope to demonstrate many other uses of large-scale distributed computing with our future efforts," confirmed Jeff Lawson, one of the head programmers. "We're looking into projects beyond OGR, like Mersenne Primes for example."

At the end of the contest, over 250 billion keys (possible codes for decrypting the encrypted message) were being checked each second. To put this in perspective:

At this rate, if keys were dollars, you could pay off the entire US debt twice every minute.

If keys were sheets of paper and you stacked the sheets up, the stack would grow 1,530 miles (2,460 kilometers) every second.

If keys were drops of water our flow rate would be 9.52 million gallons (35.7 million liters) per second. That rate could fill (or drain) lake Erie in 136 days.

During the course of the contest, we checked enough keys to make a stack of paper 980 million miles (1,580 million kilometers) high, and would have flowed 605 billion gallons (2,290 billion liters), enough to flood the city of Chicago to a depth of 12.7 feet.

ABOUT DISTRIBUTED.NET Distributed Computing Technologies, Inc. is the largest non-profit venture focused on developing the full potential of distributed computing. Its purpose is to utilize the Internet, allowing home and office computer users to join forces in tackling great and seemingly insurmountable computational challenges. The net result is computing power sufficient to challenge the dominance of even the most expensive mainframes and research computers. More information is available from the official distributed.net web site at: http://www.distributed.net/

ABOUT EFF
The Electronic Frontier Foundation is a nonprofit public interest organization protecting rights and promoting liberty online. It was founded in 1990 by Mitchell Kapor, John Perry Barlow, and John Gilmore. The Foundation seeks to educate individuals, organizations, companies, and governments about the issues tha arise when computer and communications technologies change the world out from under the existing legal and social matrix. EFF can be reached at http://www.eff.org

ABOUT RSA
RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics Technologies, Inc. (NASDAQ: SDTI), is a leading supplier of software components that secure electronic data, with more than 400 million copies of RSA encryption and authentication technologies installed worldwide. RSA technologies are part of existing and proposed standards for the Internet and World Wide Web, ISO, ITU-T, ANSI, IEEE, and business, financial and electronic commerce networks around the globe. RSA develops and markets platform-independent security components and related developer kits and provides comprehensive cryptographic consulting services. RSA can be reached at http://www.rsa.com.

MEDIA CONTACTS:
David McNett, Voice: (205) 458-8208, Fax: (205) 458-8206
nugget@distributed.net

ALTERNATE:
Daniel Baker, Voice: (713) 569-6902, dbaker@distributed.net