[an error occurred while processing this directive]

Press Release and Background Sheet

FORMAL PRESS RELEASE

For Immediate Release Contact: David McNett
February 23, 1998 205-458-8208

SECURE ENCRYPTION CHALLENGED BY INTERNET-LINKED COMPUTERS

CHICAGO, IL (February 23, 1998) In what could be called the largest distributed-computing effort ever, tens of thousands of computers linked across the Internet, under the leadership of distributed.net, decrypted a message encoded with the government's 56-bit DES encryption algorithm. This was part of a contest sponsored by RSA Labs. "Once again, we have shown that 56 bit encryption is not strong enough for protecting sensitive data," said David McNett, one of the projects primary coordinators. This successful breach of the 56-bit DES algorithm represents the second such achievement by distributed.net and the third time a 56-bit algorithm has been compromised in the past year.

The distributed.net effort to decrypt the encoded message required massive computing power, harnessed by utilizing the idle, or otherwise unused computing power from ordinary office and home computers. Combined, these machines managed to evaluate 88% of the keyspace, or 63 quadrillion keys, before finding the winning key. At the close of the contest there were nearly 1400 active teams processing over 34 billion keys each second at a combined computing power equivalent to more than 22 thousand high-end personal computers. The work was performed entirely using consumer PCs during off-hours or otherwise idle time. Add them all together, however, and you have the world's largest computer.

The winning key was found by a Alpha-based computer running DEC Unix. Of the US$5000 prize from RSA Labs, the winner, who wishes to remain anonymous, will receive US$1000. US$3000 is being donated to the Free Software Foundation, a non-profit organization dedicated to eliminating restrictions on copying, redistribution, understanding, and modification of computer programs. They do this by promoting the development and use of free software in all areas of computing---but most particularly, by helping to develop the GNU operating system. The remaining US$1000 is being retained by distributed.net to assist in funding future projects.

Distributed.net is the brainchild of Adam L. Beberg. It 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.

Information about distributed.net is available from the official distributed.net web site at: http://www.distributed.net/

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

ALTERNATE:
Adam L. Beberg, (708) 396-9532, beberg@distributed.net

SECURE ENCRYPTION CHALLENGED BY INTERNET-LINKED COMPUTERS
Background for release dated February 23, 1998

distributed.net data sheet

distributed.net web site:
http://www.distributed.net/

Related sites:
Free Software Foundation: http://www.fsf.org/
RSA Labs: http://www.rsa.com/rsalabs/

```
   RSA Secret Key Challenge:
   http://www.rsa.com/rsalabs/97challenge/

Principal organizers:
   Adam L. Beberg, Software Engineer,
          Chicago, Illinois
   Jeff Lawson, Junior Computer Science Major, Harvey Mudd
   College,
          Claremont, California
   David McNett, Computer Programmer/Network Administrator,
          Birmingham, Alabama

Project statistics:
   Start of contest:            January 13, 1998 at 09:00 PST
   Start of distributed.net effortJanuary 13, 1998 at 09:08 PST
   End of Contest:             February 23, 1998 at 02:26 PST

   Size of keyspace:                    72,057,594,037,927,936
   Approximate keys tested:             63,686,000,000,000,000

   Number of 2^30 (average) keyblocks:              67,108,864
   Number of keys in average keyblock:           1,073,741,824
   Peak blocks per day:                              5,540,982
   Peak keys per second:                        34,430,460,000

   The unencrypted message: Many hands make light work

Computing equivalents:

   Distributed.net is equivalent in processing power to:

         11,264              DEC Alpha 21064 533s
         15,316              Sun Ultra I 167s
         22,393              Intel Pentium II 333s
         23,909              Macintosh PowerPC 604e/200s.
         41,712              Intel Pentium 166s
        399,374              Intel 486DX2/66s
      7,446,033              Intel 386SX/20s

(based solely on DES client performance)

Perspective:

If Keys were dollars, we could pay off the U.S. National Debt in
6.25 minutes

If Keys were pennies, we could buy 536249385 Mazda Miatas each
day.

If Keys were pennies, we could buy 256728249 Jeep Cherokees each
day!

If you printed a single page to represent each key block as it was
checked and placed those pages in a stack, it would grow 12.83
inches taller every minute.

If blocks were liters of your favorite carbonated beverage, we
could produce 6381493 six-packs each day

If Key Blocks were cheeseburgers, fries, and a large Dr. Pepper,
we could feed the entire city of Toronto, Ontario lunch each day.
```

[an error occurred while processing this directive]