[an error occurred while processing this directive]

Press Release and Background Sheet

FORMAL PRESS RELEASE

For Immediate Release Contact: David McNett
October 22,1997 205-458-8208

SECURE ENCRYPTION CHALLENGED BY INTERNET-LINKED COMPUTERS

CHICAGO, IL (October 22, 1997) 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 RSA Labs' 56-bit RC5 encryption algorithm. Considered by many experts to be a sufficient level of encryption, this feat has cast grave doubts in the minds of analysts as to the level of encryption required to keep private data secure. "Our effort has shown that it is dangerous to consider any 56-bit key secure", says David McNett, one of the primary coordinators of this distributed supercomputing project.

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 47% of the keyspace, or 34 quadrillion keys, before finding the winning key. At the close of the contest there were over 4000 active teams processing over 7 billion keys each second at a combined computing power equivalent to more than 26 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 Peter Stuer, working for the STARLab Bovine Team coordinated by Jo Hermans and centered in the Computer Science Department (DINF) of the Vrije Universiteit in Brussels, Belgium.

Of the US$10000 prize from RSA Labs, Mr. Stuer will receive US$1000. US$8000 is being donated to Project Gutenberg, a non-profit organization created for the purpose of converting the classics of literature into electronic format for the unlimited public use. 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 October 22, 1997

distributed.net data sheet

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

Related sites:
Project Gutenberg: http://www.promo.net/pg/
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 28, 1997
    Start of distributed.net effort:    March 20, 1997
    End of contest:                     October 19, 1997

    Size of keyspace:                   72,057,594,037,927,936
    Number of "blocks":                 268,435,456
    Number of keys in one "block":      268,435,456
    Peak keys/day:                      600,246,644,113,408
    Peak keys/second:                   7,200,000,000 (estimated)

The unencrypted message:  "It's time to move to a longer key length"

Computing equivalents:

    Distributed.net is equivalent in processing power to:

    14,685 Intel Pentium Pro 200 processors
    13,362 Motorola PowerPC 604e/200 processors
    116,326 Intel 486DX2/66 processors
    58,163 Intel Pentium 133 processors

Perspective:
    distributed.net could compromise 46-bit RC5 in under one hour.

    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 6.24 inches
    taller every minute.

    If keys were drops of water, the flow rate would be 464428 litres per
    second.

    If Keys were dollars, we could pay off the U.S. National Debt in 12.44
    minutes.

    If keys were bytes, we could fill 290268 3 1/2" floppy diskettes every
    minute

    If keys were drops of water, the flow rate would be 122609 gallons per
    second.

    If Key Blocks were hamburgers, we could feed the entire city of
    Phoenix, AZ lunch each day

The computer that found the key:
    CPU:              Intel Pentium Pro 200
    RAM:              128 megabytes
    Operating System: Microsoft Windows NT Workstation 4.0
    Owner:            Vrije Universiteit, Brussels, Belgium
    Operator:         Peter Stuer
    More information: http://dinf.vub.ac.be/bovine.html/

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
```

[an error occurred while processing this directive]