[an error occurred while processing this directive]

Official List Announcement
February 23, 1998

```
Date: Tue, 24 Feb 1998 23:38:58 -0600
From: David McNett
To: rc5@lists.distributed.net
Subject: [RC5] [ADMIN] The secret message is...
```

Once again I have the great privilege of coming to you with good news.

It is with great pleasure (and a sigh of relief) that I can now inform you
that the DES-II-1 challenge has been successfully met by distributed.net.

The winning key to the challenge was detected and submitted to RSA Labs
at 02:26 GMT on Monday, 23-Feb-1998.

The correct key, 76 9E 8C D9 F2 2F 5D EA, revealed the words which we've
been anticipating these past 39 days:

"The secret message is: Many hands make light work."

(If you ask me, this is a nice nod in our direction. Thanks, RSA Labs!)

In addition to proving that 56-bit DES is no longer sufficient for protecting
valuable information, we've now also proved that blind luck need not be a
factor in brute-force decryption attacks. The original DES Challenge and
the more recent RC5-56 wins were fortunate and did not have to sweep a
significant portion of the keyspace. This time around, however, we managed to
complete almost 90% of the keyspace and have now proven that even when the
law of averages chooses to catch up to us and forces us to pay our dues, we are
still an unstoppable force. Our collective victory is all the more impressive
when you consider what we had to accomplish to achieve it.

We tested sixty-three quadrillion keys. That number is simply staggering.

Assuming *0* growth between now and July, we'll be able to sweep the entire
DES-II-2 keyspace in just under 29 days. That's assuming that we do not
recruit another person, don't add any more machines, and are even more unlucky
next time. I daresay at least one of those assumptions is probably false.

I'd invite all of you to join us in IRC (efnet, #distributed) for a rowdy
victory party. Take a breather. Sit back and watch your clients
automatically roll over to RC5-64.

The only other issue at hand is *who* found the key. The person who found the
winning key has politely asked to remain anonymous. Rest assured, I've been
in contact with them and they know they've won. They will be receiving their
full share of the prize and are quite excited about the victory. All I'd ask
is that we all respect this person's wishes and not bother the list with
public speculation as to their identity. I'm sure we all appreciate just
how important privacy and anonymity can be.

Here are some numbers to chew on while the stats are down:

Project statistics:
        Start of contest: January 13, 1998 at 09:00 PST
        Start of distributed.net effort: January 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)

Prospective:

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 Dr. Pepper, 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.

(on a personal note, It sure feels nice to be doing RC5 blocks again. I feel
like I've just slipped on an old, comfortable pair of loafers that were lost in
the attic for two months)

--

```
_____
|David McNett       |To ensure privacy and data integrity this message has|
|nugget@slacker.com|been encrypted using dual rounds of ROT-13 encryption|
|Birmingham, AL USA|Please encrypt all important correspondence with PGP!|
```

[an error occurred while processing this directive]