From:	Chen, Lily (Fed)
To:	Stein, Ben (Fed); Boisvert, Ronald F (Fed); Scholl, Matthew (Fed)
Cc:	Esser, Mark (Fed)
Subject:	RE: Draft Fun Fact Friday for next week
Date:	Friday, April 7, 2017 2:55:00 PM

Ben:

How many people know RSA key includes an integer? If some people think RSA key as a binary string, "factor a RSA key" may confuse them. Try something like:

A desktop computer would take a quadrillion (10^15) years–more than the age of the universe–to factor a 2048-bit integer (used) as RSA public-key used for Internet security.

Lily

From: Stein, Ben (Fed)
Sent: Friday, April 07, 2017 2:47 PM
To: Boisvert, Ronald F (Fed) <boisvert@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Cc: Esser, Mark (Fed) <mark.esser@nist.gov>
Subject: RE: Draft Fun Fact Friday for next week

"Desktop" would work great; more specific yet still completely understandable. Yes, we meant non-quantum, but that's a good point about how the best non-quantum computers could shave off a lot of time in factoring the number!
Ben

From: Ronald Boisvert [mailto:ronald.boisvert@nist.gov]
Sent: Friday, April 07, 2017 2:44 PM
To: Stein, Ben (Fed) <benjamin.stein@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Cc: Esser, Mark (Fed) <mark.esser@nist.gov>
Subject: Re: Draft Fun Fact Friday for next week

Only a slight quibble ... I'm not sure how to read "conventional." If it means "typical desktop" then we are OK, since that's what the estimate is based on. But if it means "not quantum" then you are admitting parallel supercomputers, which might be able to shave a few off the exponent. So, I'd be more comfortable if you said "desktop" rather than "conventional," though these estimates are so highly speculatory that it probably doesn't make a whole lot of difference.

Ron

On 4/7/2017 2:34 PM, Stein, Ben (Fed) wrote:

> Dear Ron, Lily, and Matt,

Here is our revised Fun Fact Friday. The draft reflects a 168-character limit (including spaces) due to design constraints--and the fact needs to be understandable to a nontechnical audience! (We are assuming that many interested members of the NIST social media audience may have a little bit of IT-savvy and might recognize buzzwords such as RSA and would recognize scientific notation.)

We hope the fact is reasonably accurate. If you can send any corrections or other suggestions by the end of Monday, April 10 that would be great.

Here it is:

A conventional computer would take a quadrillion (10^{15}) years–more than the age of the universe–to factor a 2048-bit RSA key used for Internet security.

Thank you!

Ben