From: Chen, Lily (Fed)
To: Stein, Ben (Fed); Boisvert, Ronald F (Fed); Scholl, Matthew (Fed)
Cc: Esser, Mark (Fed)
Subject: RE: Seeking your guidance on encryption-related "Fun Fact Friday"
Date: Thursday, April 6, 2017 2:30:00 PM

The link is good. Thank you Ron.

I think if you want to be a little specific, it can talk RSA cryptosystem with the following facts:

1. Two public-key cryptographic algorithms: RSA encryption and RSA signature
2. In a public-key cryptographic algorithm, each user has two keys, a public key and a private key.
3. For encryption, the recipient's public key is used, while the private key is used for decryption.
4. For signature, a signer uses his/hers private key to generate signature while the verifier uses the public key to verify signature.
5. RSA is based on the hardness of integer factorization.
6. How hard it is? (then use the data in the link Ron sent. Factorization of a 2048 bits of integer will take … years)
7. You may also want to point out that multiplying two primes together is easy while given an integer, factorization is hard.
8. You may also want to tell, with quantum computer plus Shor algorithm, factorization is not hard any more. People need to build new algorithms based on problems which are hard to resistant quantum computing.

One option is just to talk facts 5 and 6. If you have further questions, please let me know.

Lily

From: Stein, Ben (Fed)
Sent: Thursday, April 06, 2017 11:35 AM
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: Seeking your guidance on encryption-related "Fun Fact Friday"

Thanks so much, Ron. We could say "over a million billion years…" or simply "billions upon billions" of years. We don't need to be precise, but just in the right ballpark.
Ben

From: Ronald Boisvert [mailto:ronald.boisvert@nist.gov]
Sent: Thursday, April 06, 2017 11:19 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Stein, Ben (Fed) <benjamin.stein@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>

Cc: Esser, Mark (Fed) <mark.esser@nist.gov>
Subject: Re: Seeking your guidance on encryption-related "Fun Fact Friday"

FYI ... here is an interesting analysis done by a particular crypto company, digicert. They estimate that a "standard desktop computer" using today's best algorithm would have to compute for 6.4 quadrillion years to break one of their 2028-bit certificates.

https://www.digicert.com/TimeTravel/math.htm

It's a _really_ long time, even if their estimate is off by factors of a million. Lily can verify whether this is credible.

Ron

On 4/6/2017 10:52 AM, Chen, Lily (Fed) wrote:

> I will have someone from my group to tal with you. I may myself. But I am extremely busy the next two weeks. I will get this back to you before EoB today.
>
> Lily
>
> ---
>
> **From:** "Stein, Ben (Fed)" <benjamin.stein@nist.gov>
> **Date:** Thursday, April 6, 2017 at 10:01 AM
> **To:** Ronald Boisvert <boisvert@nist.gov>, Matthew Scholl <matthew.scholl@nist.gov>
> **Cc:** "Esser, Mark (Fed)" <mark.esser@nist.gov>, Lily Chen <lily.chen@nist.gov>
> **Subject:** RE: Seeking your guidance on encryption-related "Fun Fact Friday"
>
> Thank you, Ron! If anyone in the Crypto Group could send us a plausible ballpark estimate on how long it would take for a conventional computer to factor a 2048-bit RSA key that would be great. We are hoping to finalize tomorrow's Fun Fact Friday as early as we can today. We greatly appreciate this help at short notice!
> Ben
>
> ---
>
> **From:** Ronald Boisvert [mailto:ronald.boisvert@nist.gov]
> **Sent:** Wednesday, April 05, 2017 1:45 PM
> **To:** Stein, Ben (Fed) <benjamin.stein@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
> **Cc:** Esser, Mark (Fed) <mark.esser@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>
> **Subject:** Re: Seeking your guidance on encryption-related "Fun Fact Friday"
>
> Ben,

The article you site is about AES, which is a symmetric cryptosystem. It is not based on the hardness of factoring. The attack they describe in the article is the simplest (and least efficient) one possible, brute force.

Factoring is at the heart of "public-key" cryptography like RSA. If one can factor, then one can break RSA.

So, the question is, how long would it take to factor a 2048-bit RSA key. That can only be estimated, and I don't know enough to provide such an estimate, though I expect someone in the NIST Crypto Group does.

Ron

On 4/5/2017 1:26 PM, Stein, Ben (Fed) wrote:

> Dear Ron and Matt,
>
> This week, we are planning to run a “Fun Fact Friday” on how long it would take conventional computers to break Internet security. We currently say “billions of years.”
>
> But since it’s Math Awareness Month, and much of our audience may be a bit more math-aware than average, we thought we should be more specific, as it might be more interesting to them.
>
> Would you be able to recommend a ballpark figure we can express?
>
> We have only 168 characters, but we will see what we can pack in!
>
> We found this on IEEE’s website:
> http://www.eetimes.com/document.asp?doc_id=1279619
> To wit: “Even with a supercomputer, it would take 1 billion billion years to crack the 128-bit AES key using brute force attack. This is more than the age of the universe (13.75 billion years). If one were to assume that a computing system existed that could recover a DES key in a second, it would still take that same machine approximately 149 trillion years to crack a 128-bit AES.” key.
>
> Thanks for any guidance you can provide!
>
> Ben