

Factoring 1024-bit RSA

Nadia Heninger

Zakir Durumeric Eric Wustrow Alex Halderman

Announcement: New Factorization Results

RSA-768 : December 12, 2009 Kleinjung et al. 2 years

Announcement: New Factorization Results

RSA-768 : December 12, 2009 Kleinjung et al. 2 years

RSA-704 : July 2, 2012 Bai et al. 1 year

Announcement: New Factorization Results

RSA-768 : December 12, 2009 Kleinjung et al. 2 years

RSA-704 : July 2, 2012 Bai et al. 1 year

Our running time:

1024-bit **RSA modulus** :

1.5 hours (\$5 of EC2 compute time)

Announcement: New Factorization Results

RSA-768 : December 12, 2009 Kleinjung et al. 2 years

RSA-704 : July 2, 2012 Bai et al. 1 year

Our running time:

198 **512-bit**

11 **768-bit**

16477 **1024-bit**

29 **2048-bit RSA moduli**

1.5 hours (\$5 of EC2 compute time)

Algorithm

1. Collect RSA moduli.
2. Calculate $\gcd(N_i, N_j)$ for all (i, j) .

Obtaining RSA moduli

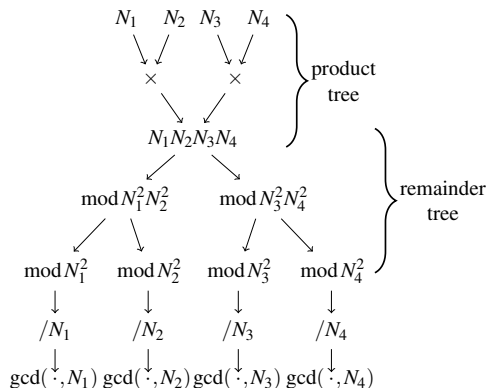
Scanned IPv4 space for TLS certificates, SSH host keys.

Obtained 11,170,883 distinct moduli.

Implementation

40 lines of Sage. Too unstable. :(

350 lines of C. More stable. :)



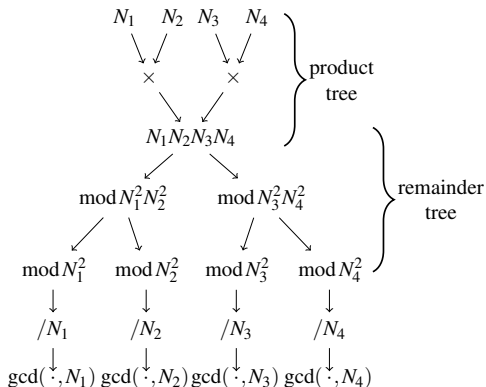
Bernstein, D. J. "How to find the smooth parts of integers"

Implementation

40 lines of Sage. Too unstable. :(

350 lines of C. More stable. :)

16,717 keys factored.



Bernstein, D. J. "How to find the smooth parts of integers"

IRONKEY THE WORLD'S FIRST FIPS 140-2 LEVEL 3 FLASH DRIVE AES 256-BIT HARDWARE ENCRYPTION LEARN MORE Advertise on NYTimes.com

Flaw Found in an Online Encryption Method

By JOHN MARKOFF Published: February 14, 2012

SAN FRANCISCO — A team of European and American mathematicians and cryptographers have discovered an unexpected weakness in the encryption system widely used worldwide for online shopping, banking, e-mail and other Internet services intended to remain private and secure.

The flaw — which involves a small but measurable number of cases — has to do with the way the system generates random numbers, which are used to make it practically impossible for an attacker to unscramble digital messages.

While it can affect the transactions of individual Internet users, there is nothing an individual can do about it. The operators of large Web sites will need to make changes to ensure the security of their systems, the researchers said.

Readers' Comments


Readers shared their thoughts on this article. Read All Comments (127) »

RECOMMEND TWITTER LINKEDIN COMMENTS (127) SIGN IN TO E-MAIL PRINT REPRINTS SHARE SOUND OF MY VOICE IN THEATRES 04.27.2012 Click to View

Log in to see what your friends are sharing on nytimes.com. Privacy Policy | What's This? Log In With Facebook

What's Popular Now Why I Am Leaving Goldman Sachs The Benefits of Bilingualism

Gazzang Encrypt, Decrypt, & Access MySQL Data in Realtime! I SPOURED MY CLOUD DATA. HAVE YOU?




Enter Your Online ID Sign In

Save this Online ID

Select account location

Help/options



Online
Take charge

Get started

Information for:

promo.bankofamerica.com/takechar

General Details

Certificate Hierarchy

- Built-in Object Token: VeriSign Class 3 Public Primary Certification Authority
 - VeriSign Class 3 Extended Validation SSL CA
- www.bankofamerica.com

Certificate Fields

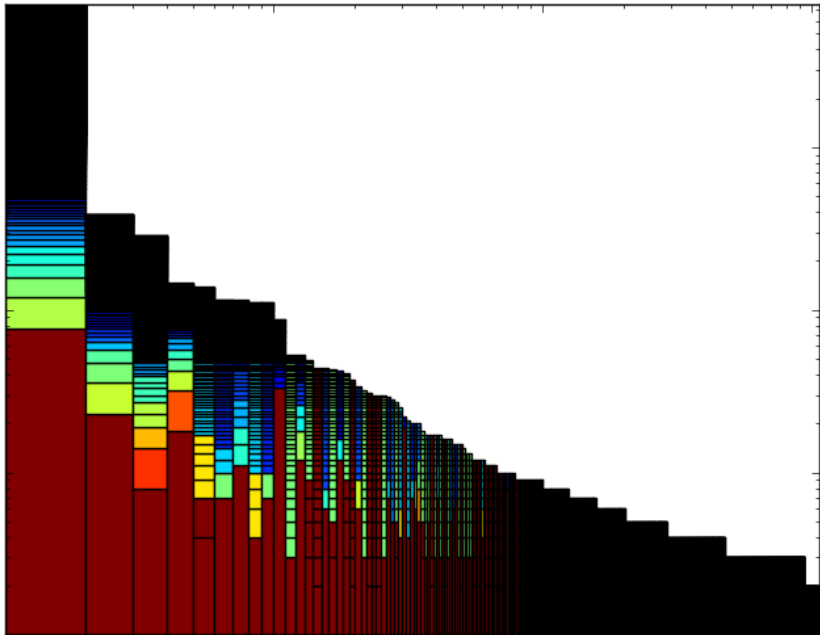
- Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key
- Extensions
 - Certificate Basic Constraints

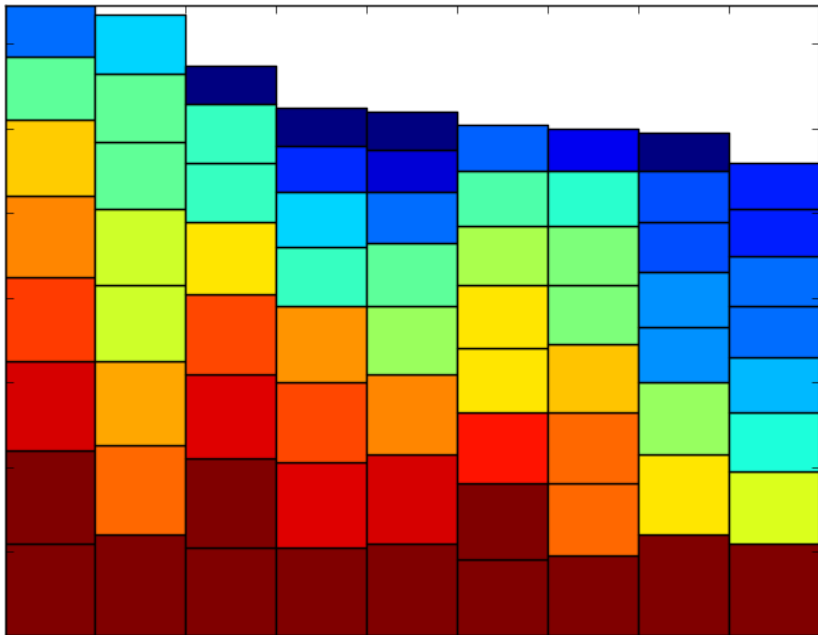
Field Value

Modulus (2048 bits):

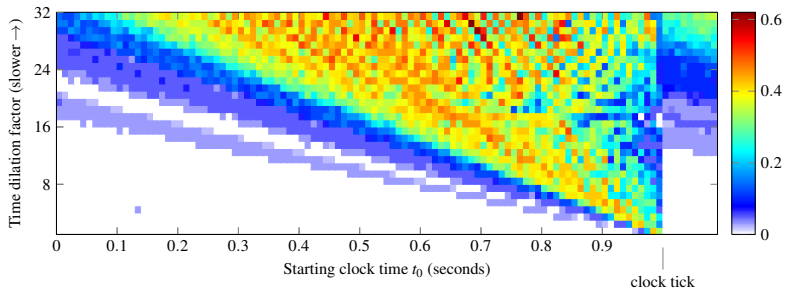
```
CE CF 90 EC 9B BC 5B 50 C8 A4 84 04 E7 68 28 19
4B 8F 14 D9 F5 A8 44 DE 44 A2 95 9B 47 F8 BB CE
EA 46 A4 43 7D 1A 46 07 AA 07 D2 8A 14 30 55 42
58 DF 72 27 42 AB BC 42 EE BB A9 F2 2B 60 B0 58
60 D6 CD 7B D5 47 F0 44 F4 9D CD C2 FB B3 F8 60
1B BD 2B 30 7F B6 9E 4D 97 8E 5B D8 AF 1A F0 58
```







Fraction of keys generated that we could factor



factorable.net