
Real World Crypto
Nate Cardozo, EFF
783A 8CC4 166D 1768 4E8E DAFD 2D76 4786 4AE6 3181
“The Net interprets censorship as damage and routes around it.”

John Gilmore, ~1993
The First Crypto Wars

#!/usr/local/bin/perl -s do
'bigint.pl';($_, $n) = @ARGV; s/\^\.(.\*)*/\$0&/;($k = unpack('B*', pack('H*', $_, $n))) =~ s/\^0*//; $x = 0; $z = $n = ~s/.\$/x= & badd(& bmul($x, 16), hex$&)/ge; while (read(STDIN, $_, $w = ((2*$d-1+$z)&~1)/2)) {$r = 1; $= = substr($_."\0"*$w, $c = 0, $w); s/.\$c = & badd(& bmul($c, 256), ord$&)/ge; $= = $k; s/.\$/r = & bmod(& bmul($r, $r), $x), $&?$r = & bmod(& bmul($r, $c), $x): 0,"/ge; ($r, $t) = & bdiv($r, 256), $= = pack(C, $t).$ _ while $w --+1-2*$d; print}
Download

You are here: Home > Computing & Internet > Download

Download the New Netscape Communicator 4.61

Full Download of Communicator 4.61
If you're now to Communicator, choose either the Windows 95/98/NT or Mac PowerPC (OS 7.6.1 or later) version.

Fast Update for Communicator 4.0 Users
If you're using Communicator or Navigator 4.04 or higher (4.05 for Mac), use SmartUpdate to update to Communicator 4.61.

Full Download of Unix, International, & 128-bit
If you're looking for a Unix, International, 128-bit strong encryption, or other version of Communicator, choose from our directory.

Shareware by CNET
Browse and select from over 20,000 titles.
P & Q prime
N = PQ
ED ≡ 1 mod (P-1)(Q-1)
C = M^E mod N
M = C^D mod N

RSA public-key cryptosystem US Patent # 4,405,829

IT'S JUST AN ALGORITHM
If all you have is a hammer...
If all you have is a hammer...
And the Internet was a safer place for it!
• We thought we had solved the field…
  – But thanks to Comey
  – More work remains
Bill Murray
He's having the day of his life...
over and over again.

Groundhog Day
• FBI Director Comey in 2014:
  “We also need a regulatory or legislative fix to create a level playing field, so that all communication service providers are held to the same standard and so that those of us in law enforcement, national security, and public safety can continue to do the job…”
2015

- Conversation started with device encryption, but quickly moved to end-to-end encryption.
- UK PM Cameron: “Are we going to allow a means of communications which it simply isn't possible to read?”
“Only a Business Model”

- Government have been downplaying corporate support for encryption
  - Comey: “plenty of companies” can read users' data and unlock encrypted phones.
  - “Encryption isn’t just a technical feature; it’s a marketing pitch”
- Combined with backroom pressure
“Secure Back Door” Proposals

- Most common is some variation on key escrow
- E.g. Message sent with symmetric key
- Encrypt symmetric key twice
  - Recipient’s public key and
  - Escrow agent’s public key

What if we re-named back doors?

• Comey: “We aren’t seeking a back-door approach. We want to use the front door”

• Washington Post “a back door can and will be exploited by bad guys, too. However, with all their wizardry, perhaps Apple and Google could invent a kind of secure golden key”
NSLS ARE MAGIC!
Legislation

• Many countries around the world are considering legislation that would either
  – mandate backdoors,
  – mandate access to plaintext or
  – endanger encryption.
UK Snooper’s Charter

• Purports to regulate telecommunications operators all around the world

• § 189(4)(c): Operators may be obligated to remove “electronic protection” if they provided
  – Could be interpreted to require weakening encryption, holding a key or banning end-to-end
UK Snooper’s Charter

- Latest version resented to Parliament in November
  - Currently in committee, which is accepting evidence.
  - Industry and civil society submitted comments
Australia’s Defence Trade Controls Act

- Prohibits the “intangible supply” of encryption technologies.
- Many ordinary teaching and research activities could be subject to unclear export controls with severe penalties.
- International Association for Cryptologic Research organized petition against, signed 100s of experts
India Considers An Encryption Policy

- In September, India released a draft National Encryption Policy
  - Everyone required to store plain text
  - Info kept for 90 days
  - Made available to law enforcement agencies as and when demanded
- Withdrawn after criticism
China’s Anti-Terrorism Law

• Passed last month
• Draft version required tech companies to hand over encryption codes
• Final version: “shall provide technical interfaces, decryption and other technical support”
US: No Bill to Require Backdoors

- *Yet.* Obama “will not —for now—call for legislation requiring companies to decode messages for law enforcement.”
- Senate Intelligence Committee likely to introduce bill in the coming spring
Trans-Pacific Partnership

• Some report that TPP could contain good news on encryption?
  – Alas, no.
• Provider may not be compelled to give key
  – Only “as a condition of sale”
• But provider must still give decrypted content
• TPP still has huge problems throughout
2016

• But what is actually likely?
  – Key escrow mandate
    • If it happens, it’s going to be double-bagged.
    • But I don’t think this is actually going to happen.
  – We don’t care how, just make plaintext available.
    • Now I will go into prediction mode.
2016

- But what is actually likely?
  - Informal pressure
  - No ban will reach FOSS crypto
  - CALEA-like mandate
  - India/Australia/Kazakhstan may do dumb things
  - It’s not going to stop anyone with even a modicum of sophistication from “going dark”
2016

Defaults, not primitives

Backdoor pressure, not backdoor mandates

Any mandate will affect only the masses
Questions?

Nate Cardozo
Staff Attorney, EFF
nate@eff.org
@ncardozo
783A 8CC4 166D 1768 4E8E DAFD 2D76 4786 4AE6 3181