



Crypto: State of the Law

DEF CON 24

Nate Cardozo, Senior Staff Attorney, EFF

783A 8CC4 166D 1768 4E8E DAFD 2D76 4786 4AE6 3181



"*End to end encryption is legal. Period.*"

Jennifer Granick, Black Hat 2016



Questions?


WILSHIRE
SAFE & SCALE CO.
SAN FRANCISCO.



"*The Net interprets censorship as damage and routes around it.*"

John Gilmore, ~1993



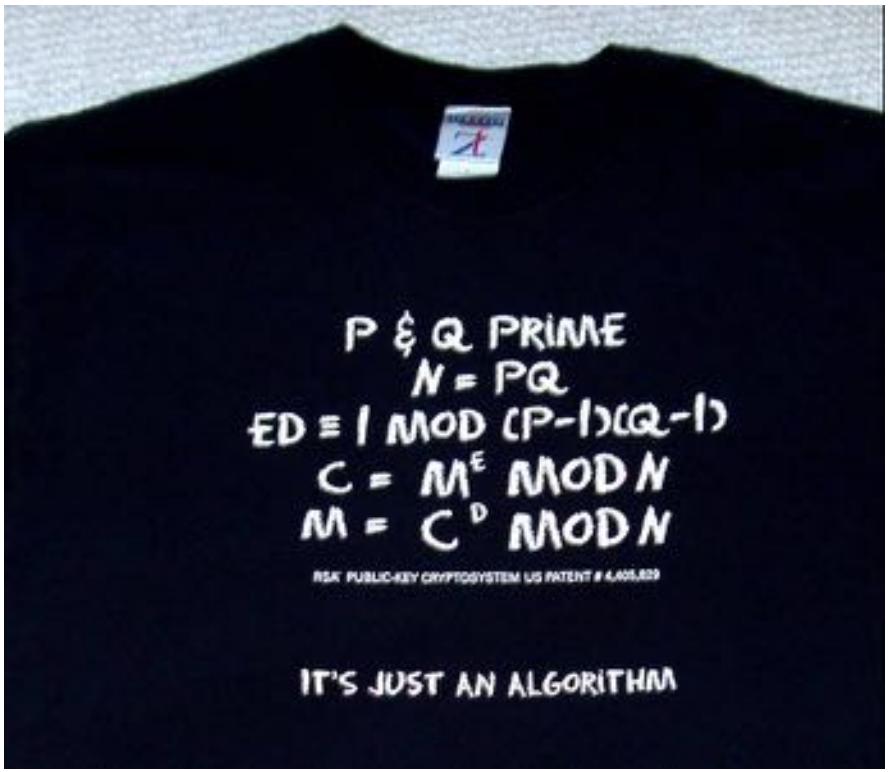
The First Crypto Wars

```
#!/usr/local/bin/perl -s do
'bigint.pl';($_,$n)=@ARGV;s/^.(..)*$/0$&/;($k=unpack('B*',pack('H*',$_)))=~
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($_."\0"x$w,$c=0,$w);s/.|\n/$c=&badd(&bmul
($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}
```

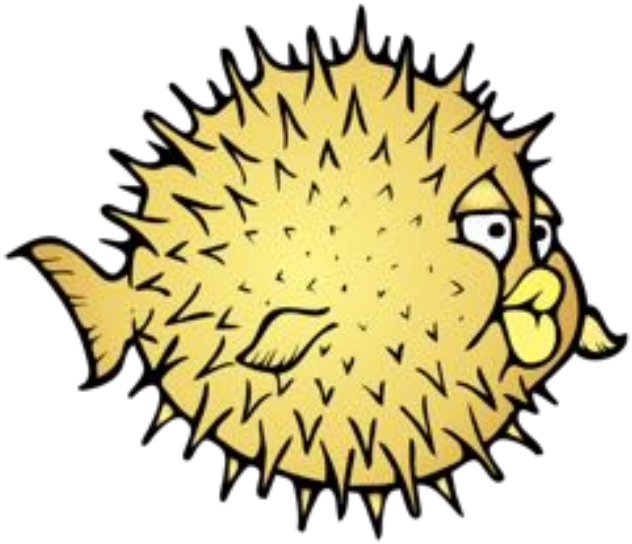
The First Crypto Wars




Netscape
Search | WebMail | My Netscape | Members | Download
Netscape Network ad
Click Here!
You are here: Home > Computing & Internet > Download
Download
Departments
SmartUpdate
Netscape Browsers
Netscape Servers and Tools
Browser Plug-ins
Shareware
Computing & Internet
Store
Download
Hardware
Tech Resources
Tech News
Web Site Services
Software Reviews
Games
Support
Download the New Netscape Communicator 4.61
English, 56-bit standard encryption, including Navigator
Full Download of Communicator 4.61
If you're new 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.
Netscape Network ad
Netscape Network ad
SmartDownload
New! Click Here New!
to get SmartDownload
(for Win 95/98/NT only)
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





OpenBSD


SEALAND.COM
HAVEN.COM
SEALAND


VLSI
9351AS456432
VM06578-B
MYK-78T
MYKOTRONX



If all you have is a hammer…



If all you have is a J.D. …

Daniel J. BERNSTEIN, Plaintiff,

v.

UNITED STATES DEPARTMENT OF STATE, et al., Defendants.

No. C–95–0582 MHP.

United States District Court, N.D. California.

April 15, 1996.

Mathematician sought declaratory and injunctive relief against enforcement of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) on the grounds that they were unconstitutional on their face and as applied to mathematician's cryptographic computer source code. On government's motion to dismiss for lack of justiciability, the District Court, Patel, J., held that: (1) cryptographic computer source code is "speech" protected by First Amendment, and (2) colorable constitutional challenges to statute and regulations were justiciable.

how to make the encryption algorithm (the idea) functional. U.S.C.A. Const.Amend. 1.

See publication Words and Phrases for other judicial constructions and definitions.

3. Federal Civil Procedure ⇐1773

Motion to dismiss will be denied unless it appears that plaintiff can prove no set of facts which would entitle him or her to relief. Fed.Rules Civ.Proc.Rule 12(b)(6), 28 U.S.C.A.

4. Federal Civil Procedure ⇐1829, 1835

On motion to dismiss, all material allegations in complaint will be taken as true and construed in light most favorable to plaintiff. Fed.Rules Civ.Proc.Rule 12(b)(6), 28 U.S.C.A.

5. Federal Civil Procedure ⇐1832

Although, on motion to dismiss, court is generally confined to consideration of allegations in the pleadings, when complaint is accompanied by attached documents, such documents are deemed part of the complaint and may be considered in evaluating merits of motion. Fed.Rules Civ.Proc.Rule 12(b)(6),


ELECTRONIC FRONTIER FOUNDATION
eff.org
DEFCON
D3KJNJ2NW2AP9LKM7L07GRCZJ2NW2APXUD
M7OE5V7S2FV8DKND3DYBH48VHDHNVDA4GD
UVT2APE83UC0D3J1SOSP33CHDPW28RUDKJ
GRCZJ2NW2AP9LKM7OE5V7S2FV8CKND3DYB
HDHNVDA4GDJXNDUVOE83UGJG04J15W96RU
L07GRCZJ2RUDKAP9LKM7OE5V7S2FVQD5ND


KEY ESCROW
RSA DATA SECURITY, INC

And the Internet was a safer place for it!





ELECTRONIC FRONTIER FOUNDATION eff.org



Thank your lucky PKIs for ECCN 5D002!!

§ 740.17 Encryption commodities, software and technology (ENC).

License Exception ENC authorizes export and reexport of systems, equipment, commodities and components therefor that are classified under ECCNs 5A002.a.1, .a.2, .a.5, .a.6, .a.9, or .b, systems, equipment and components therefor classified under ECCN 5B002, and equivalent or related software and technology classified under ECCNs 5D002 or 5E002. This License Exception ENC does not authorize export or reexport to, or provision of any service in any country listed in Country Group E:1 in supplement no. 1 to part 740 of the EAR, or release of source code or technology to any national of a country listed in Country Group E:1. Reexports and transfers under License Exception ENC are subject to the criteria set forth in paragraph (c) of this section. Paragraphs (b) and (d) of this section set forth information about encryption registrations and classifications required by this section. Paragraph (e) sets forth reporting required by this section. For items exported under paragraphs (b)(1), (b)(3)(i), (b)(3)(ii) or (b)(3)(iv) of this section and therefore excluded from paragraph (e) reporting requirements, exporters are reminded of the recordkeeping requirements in part 762 of the EAR and that they may be required to make such records available upon request. All classification requests, registrations, and reports submitted to BIS pursuant to this section for encryption items will be reviewed by the ENC Encryption Request Coordinator, Ft. Meade, MD.

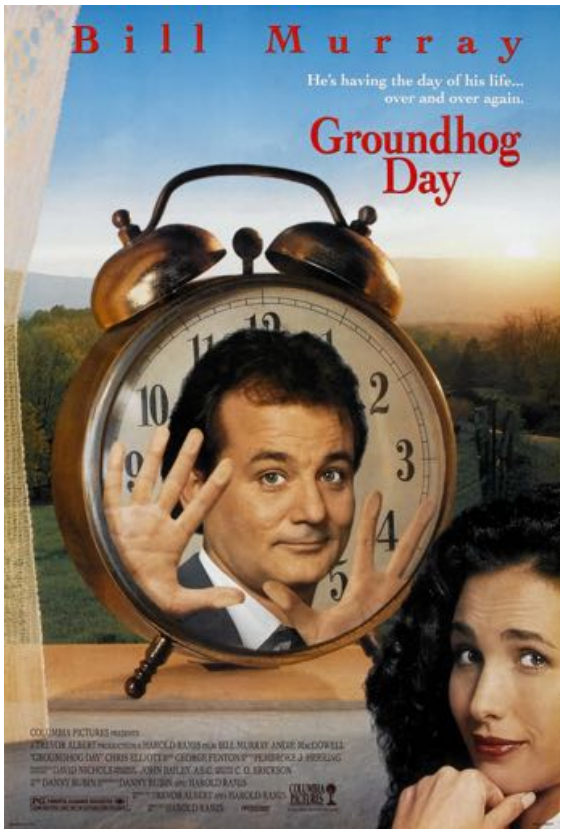
(a) ***No classification request, registration or reporting required*** -

(1) ***Internal "development" or "production" of new products.*** License Exception ENC authorizes exports and reexports of items described in paragraph (a)(1)(i) of this section, to end-users described in paragraph (a)(1)(ii) of this section, for the intended end-use described in paragraph (a)(1)(iii) of this section without submission of encryption registration, classification request, self-classification report or sales report to BIS.

(i) ***Eligible items.*** Eligible items are those classified under ECCNs 5A002.a.1, .a.2, .a.5, .a.6, .a.9, or .b, ECCN 5B002, and equivalent or related software and technology classified under ECCNs 5D002 or 5E002.

(ii) ***Eligible End-users.*** Eligible end-users are "private sector end-users" wherever located that are headquartered in a country listed in supplement no. 3 of this part.

- 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



The Next Crypto Wars



iOS Security

iOS 9.3 or later

May 2016

What could possibly go wrong?





ELECTRONIC FRONTIER FOUNDATION eff.org

DEFCON

Keys Under Doormats:

MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

What if we re-named back doors?





The slide you are about to see is false.

ELECTRONIC FRONTIER FOUNDATION eff.org

DEFCON

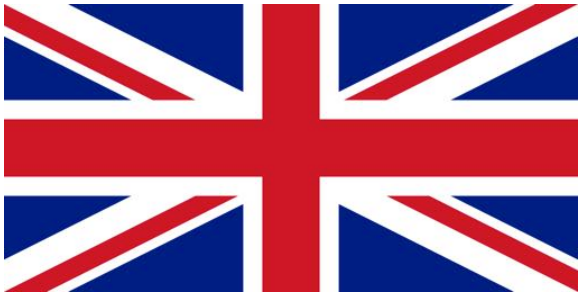


Legislation

- Many countries around the world are considering legislation that would either
  - mandate backdoors,
  - mandate access to plaintext or
  - endanger encryption.



UK IPB and the Death of e2e





Draft Investigatory Powers Bill



AUS DSGL and the Death of all crypto…





Australian Government

Department of Defence





Thanks Obama

- October 2015:

  We “will not —**for now**—call for legislation requiring companies to decode messages for law enforcement.”

Thanks Obama

- November 2015:

  Identify laws that need to be changed to deal with “going dark.”

Thanks Obama

- March 2016:

  “My conclusion so far is that you cannot take an absolutist view on this…it's fetishizing our phones above every other value. And that can't be the right answer.”

All Writs Act Litigation

- Apple v. FBI
  - This is the San Bernardino iPhone case
  - Also, a case in EDNY

Other Litigation

- Wiretap Act litigation may be coming
  - New York Times report re: WhatsApp
- There may be FISA Court orders
  - EFF is in the middle of a FOIA case to get access to them

Burr-Feinstein Bill

- Would require providers to decrypt on demand
  - Criminal and civil penalties
- Applies to comms, storage, and licensing
  - This includes app stores and open source
- Not just e2e and FDE
  - This would outlaw computers as we know them

2016

- What are we looking at?
  - Key escrow mandate
    - I don't think this is actually going to happen.
  - Burr-Feinstein
    - This definitely won't happen (in the current form)
  - We don't care how, just make plaintext available.
    - This is the route the UK seems to be taking…

Defaults, not Primitives

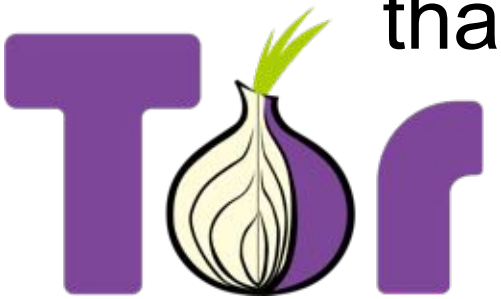
- California AB 1681
- New York A8093A

2016

- But what is actually likely?
  - Informal pressure
  - No ban will reach FOSS crypto
  - CALEA-like mandate
  - Countries around the world may do dumb things



It’s not going to work this time any better than it did the last time.







So what's to be done?

- What if you're a developer staring down the barrel of an order/request/demand/NSL?
- What if you're a regular person?
- What if you just have some questions?



mailto:info@eff.org



https://ssd.eff.org





Questions?

Nate Cardozo

Senior Staff Attorney, EFF

✉: nate@eff.org

: @ncardozo

783A 8CC4 166D 1768 4E8E DAFD 2D76 4786 4AE6 3181