Crypto Wars:
Plus ça Change, Plus C'est la Même Chose

Susan Landau
Worcester Polytechnic Institute
The First Crypto Wars: 1970s

• 1976: Invention of public-key crypto.

• 1977: Invention of RSA algorithm.

• 1978: NSA attempts to control publication.
The First Crypto Wars: 1970s

- 1976: Invention of public-key crypto.
- 1978: NSA attempts to control publication.
The First Crypto Wars: 1970s

• 1976: Invention of public-key crypto.

• 1977: Invention of RSA algorithm.

• 1978: NSA attempts to control publication.

• 1988: NSA helps remove security order imposed on Zero-Knowledge paper.
The First Crypto Wars: 1980s

- Who controls crypto? NIST or NSA?
The First Crypto Wars: 1980s

- Who controls crypto? NIST or NSA?

— "We were blindsided." Clint Brooks, NSA
The First Crypto Wars: 1980s

- Who was blindsided?


The First Crypto Wars: 1990s

- Cryptography export controls.
- What were they?
- How did they work?

Clint Brooks, NSA—"We were blindsided."
The Emd of the Crypto Wars: 2000

- Change in export controls regs.
- What was the change?
- Why did they change?
The Emd of the Crypto Wars: 2000

• Change in export controls regs.

• What was the change?

• Why did they change?
Alice and Bob Talking
Alice and Bob Talking

Everyone and Everything Participating on the Network
Alice and Bob Talking

Everyone and Everything Participating on the Network
The Communications Assistance for Law Enforcement Act (CALEA): 1994

• Law requires all digital telephone networks to be built wiretap enabled.

• Doesn’t apply to “information services.”
The Communications Assistance for Law Enforcement Act (CALEA): 1994

- Law requires all digital telephone networks to be built wiretap enabled.

- Doesn’t apply to “information services.”

- But in 2003 ...
The Communications Assistance for Law Enforcement Act (CALEA): 1994

• Law requires all digital telephone networks to be built wiretap enabled.

• Doesn’t apply to “information services.”

• But in 2003 ...

• Then in 2005 ...
The Communications Assistance for Law Enforcement Act (CALEA): 1994

- Law requires all digital telephone networks to be built wiretap enabled.

- Doesn’t apply to “information services.”

- But in 2003 ... 

- Then in 2005 ...

- And in 2010 ...
The Communications Assistance for Law Enforcement Act (CALEA): 1994

• Law requires all digital telephone networks to be built wiretap enabled.

• Doesn’t apply to “information services.”

• But in 2003 ...

• Then in 2005 ...

• And in 2010 ...
2015

• Charlie Hebdo.
• ISIS.
2015

• Charlie Hebdo.
• ISIS.
• Golden keys.
• Exceptional access.
The Crypto Wars: 2010s

• FBI wants access to plain text.

• They don’t care how.
The Crypto Wars: 2010s

• FBI wants access to plain text.

• They don’t care how.

• Not so simple.
The Crypto Wars: 2010s


• Exceptional access breaks forward secrecy.

• Exceptional access breaks authenticated encryption.
The Crypto Wars: 2010s

• Different types of threats than in the 1990s.

• Alternate forms of investigative tools.

• Alternate ways of obtaining content than “golden key,” “exceptional access,” etc.
The Crypto Wars: 2015

*Obama Won’t Seek Access to Encrypted User Data*

By NICOLE PERILROTH and DAVID E. SANGER   OCT. 10, 2015

CUPERTINO, Calif. — The Obama administration has backed down in its bitter dispute with Silicon Valley over the encryption of data on iPhones and other digital devices, concluding that it is not possible to give American law enforcement and intelligence agencies access to that information without also creating an opening that China, Russia, cybercriminals and terrorists could exploit.
The Crypto Wars: 2030s

It’s tough to make predictions, especially about the future.