Technical Remarks on Government Access to Plaintext

Ronald L. Rivest

Institute Professor
MIT, Cambridge, MA

National Academies Panel
2016-11-11

Outline

Where are we?

Trying to give clear definitions

Challenges for government access

Other issues

Conclusions

Outline

Where are we?

Trying to give clear definitions

Challenges for government access

Other issues

Conclusions

Déjà Vu all over again...

Déjà Vu all over again...

- Crypto Wars 1.0 (80s and 90s)

Déjà Vu all over again...

- Crypto Wars 1.0 (80s and 90s)
- **What if LE had prevailed then?**

CSAIL

Déjà Vu all over again...

- Crypto Wars 1.0 (80s and 90s)
- **What if LE had prevailed then?**
  —Clipper Chip or equivalent in all confidential communications.

CSAIL

Déjà Vu all over again...

- Crypto Wars 1.0 (80s and 90s)
- **What if LE had prevailed then?**
  —Clipper Chip or equivalent in all confidential communications.
  —Still be waiting for e-commerce...

CSAIL

Déjà Vu all over again...

- Crypto Wars 1.0 (80s and 90s)
- **What if LE had prevailed then?**
  —Clipper Chip or equivalent in all confidential communications.
  —Still be waiting for e-commerce...
- Problem is pretty much the same, but the world is **much** more complex now.

CSAIL

What does LE want?

- “Responsible party” to provide **government access to “plaintext”** in some “intelligible format” whenever LE has a suitable warrant but is frustrated by the use of “encryption.”

CSAIL

What does LE want?

- “Responsible party” to provide **government access to “plaintext”** in some “intelligible format” whenever LE has a suitable warrant but is frustrated by the use of “encryption.”
- An anti-encryption “magic wand.”

CSAIL

What does LE want?

- “Responsible party” to provide **government access to “plaintext”** in some “intelligible format” whenever LE has a suitable warrant but is frustrated by the use of “encryption.”
- An anti-encryption “magic wand.”
- Designed, implemented, paid for, and managed by someone else.

CSAIL

What does LE want?

- “Responsible party” to provide **government access to “plaintext”** in some “intelligible format” whenever LE has a suitable warrant but is frustrated by the use of “encryption.”
- An anti-encryption “magic wand.”
- Designed, implemented, paid for, and managed by someone else.
- Effective—hard to evade or subvert.

CSAIL

What would U.S. cryptographers and computer security professionals want?

- **Clear** *technical* requirements.

What would U.S. cryptographers and computer security professionals want?

- **Clear** *technical* requirements.
- **Clarity** as to whether and how rules would apply to all existing and future applications, including products sold internationally.

CSAIL

What would U.S. cryptographers and computer security professionals want?

- **Clear** *technical* requirements.
- **Clarity** as to whether and how rules would apply to all existing and future applications, including products sold internationally.
- **Feasibility** for implementation by **simple** security mechanisms.

CSAIL

What would U.S. cryptographers and computer security professionals want?

- **Clear** *technical* requirements.
- **Clarity** as to whether and how rules would apply to all existing and future applications, including products sold internationally.
- **Feasibility** for implementation by **simple** security mechanisms.
- **No negative impact** on security.

CSAIL

What would U.S. cryptographers and computer security professionals want?

- **Clear** *technical* requirements.
- **Clarity** as to whether and how rules would apply to all existing and future applications, including products sold internationally.
- **Feasibility** for implementation by **simple** security mechanisms.
- **No negative impact** on security.
- Mechanisms **not subject to abuse or catastrophic failure**.

CSAIL

What would U.S. cryptographers and computer security professionals want?

- **Clear** *technical* requirements.
- **Clarity** as to whether and how rules would apply to all existing and future applications, including products sold internationally.
- **Feasibility** for implementation by **simple** security mechanisms.
- **No negative impact** on security.
- Mechanisms **not subject to abuse or catastrophic failure**.
- Clear **international guidelines**.

CSAIL

What would U.S. cryptographers and computer security professionals want?

- **Clear** *technical* requirements.
- **Clarity** as to whether and how rules would apply to all existing and future applications, including products sold internationally.
- **Feasibility** for implementation by **simple** security mechanisms.
- **No negative impact** on security.
- Mechanisms **not subject to abuse or catastrophic failure**.
- Clear **international guidelines**.
- **Fairness to U.S. companies**.

CSAIL

What else is wanted?

- A “compromise” approach?

What else is wanted?

- A “compromise” approach?
- An approach that is arguably and measurably **cost-effective**.

CSAIL

What else is wanted?

- A “compromise” approach?
- An approach that is arguably and measurably **cost-effective**.
- An approach that **doesn’t set standards that empower dictators and authoritarian regimes**.

CSAIL

What else is wanted?

- A “compromise” approach?
- An approach that is arguably and measurably **cost-effective**.
- An approach that **doesn’t set standards that empower dictators and authoritarian regimes**.
- An approach that **doesn’t throw sand in the gears of technical progress**.

CSAIL

Outline

Where are we?

Trying to give clear definitions

Challenges for government access

Other issues

Conclusions

What is “**plaintext**”?

- Whatever LE might have a warrant for...????

CSAIL

What is “**plaintext**”?

- Whatever LE might have a warrant for...????
- It’s like pornography: I know it when I see it...

What is “**plaintext**”?

- Whatever LE might have a warrant for...????
- It’s like pornography: I know it when I see it...
- Plaintext messages, email, or pictures.

CSAIL

What is “**plaintext**”?

- Whatever LE might have a warrant for...????
- It’s like pornography: I know it when I see it...
- Plaintext messages, email, or pictures.
- Anything that has been “encrypted”? (including keys, counters, random bits, other ciphertexts??)

CSAIL

What is “**plaintext**”?

- Whatever LE might have a warrant for...????
- It’s like pornography: I know it when I see it...
- Plaintext messages, email, or pictures.
- Anything that has been “encrypted”? (including keys, counters, random bits, other ciphertexts??)
- Result of applying “decryption” to a “ciphertext”??

CSAIL

What is “**encryption**”?

- Invertible transformation whose inverse (“decryption”) requires a secret key?

CSAIL

Is using AES “encryption”? (AES = Advanced Encryption Standard)

- **Not necessarily**—AES often used for purposes other than confidentiality

Is using AES “encryption”? (AES = Advanced Encryption Standard)

- **Not necessarily**—AES often used for purposes other than confidentiality
- Example: AES “encrypts” last block of CBC ciphertext to obtain CBC message authentication code (MAC). (PT is junk...)

CSAIL

Is using AES “encryption”? (AES = Advanced Encryption Standard)

- **Not necessarily**—AES often used for purposes other than confidentiality
- Example: AES “encrypts” last block of CBC ciphertext to obtain CBC message authentication code (MAC). (PT is junk...)
- Example: AES generating pseudo-random numbers (PT is known counter...)

CSAIL

Is using AES “encryption”? (AES = Advanced Encryption Standard)

- **Not necessarily**—AES often used for purposes other than confidentiality
- Example: AES “encrypts” last block of CBC ciphertext to obtain CBC message authentication code (MAC). (PT is junk...)
- Example: AES generating pseudo-random numbers (PT is known counter...)
- Maybe one has to look at *intent*–is it for confidentiality? (Intent is hard...)

Is using AES “encryption”? (AES = Advanced Encryption Standard)

- **Not necessarily**—AES often used for purposes other than confidentiality
- Example: AES “encrypts” last block of CBC ciphertext to obtain CBC message authentication code (MAC). (PT is junk...)
- Example: AES generating pseudo-random numbers (PT is known counter...)
- Maybe one has to look at *intent*–is it for confidentiality? (Intent is hard...)
- **Hard to tell if using AES is “encryption”!**

What is a “**ciphertext**”?

- Something obtainable (or obtained) by applying “encryption” to a “plaintext”??

CSAIL

What is a “**ciphertext**”?

- Something obtainable (or obtained) by applying “encryption” to a “plaintext”??
- (Are we going in circles with these definitions?)

CSAIL

What is “**intelligible format**”?

- This is hardly a technical definition!

What is “**intelligible format**”?

- This is hardly a technical definition!
- Original “plaintext” before encryption??

What is “**intelligible format**”?

- This is hardly a technical definition!
- Original “plaintext” before encryption??
- Result of applying “decryption” operation??

Who is responsible for providing plaintext?

- Not party with access to ciphertext only (transport server, cloud computing provider, owner, proxy reencryption provider, medical database provider,...)

CSAIL

Who is responsible for providing plaintext?

- Not party with access to ciphertext only (transport server, cloud computing provider, owner, proxy reencryption provider, medical database provider,...)
- Not necessarily a party defining or supporting system (vendor, open source code provider, standards organization,...)

CSAIL

Who is responsible for providing plaintext?

- Not party with access to ciphertext only (transport server, cloud computing provider, owner, proxy reencryption provider, medical database provider,...)
- Not necessarily a party defining or supporting system (vendor, open source code provider, standards organization,...)
- Must be some party with access to plaintext (or to secret decryption key).

CSAIL

Who is responsible for providing plaintext (cont.)?

- "Sender"? (If PK is used, sender needs to remember too much.)

Who is responsible for providing plaintext (cont.)?

- "Sender"? (If PK is used, sender needs to remember too much.)
- "Recipient"? (With PK ciphertext posted publicly, may not be clear who recipient is. Also problematic if keys are updated...)

CSAIL

Who is responsible for providing plaintext (cont.)?

- "Sender"? (If PK is used, sender needs to remember too much.)
- "Recipient"? (With PK ciphertext posted publicly, may not be clear who recipient is. Also problematic if keys are updated...)
- "Trusted Third Party"? (Who is that?) (How does TTP get access?) Requires more bandwidth and computation on **all** messages.

CSAIL

Who is responsible for providing plaintext (cont.)?

- "Sender"? (If PK is used, sender needs to remember too much.)
- "Recipient"? (With PK ciphertext posted publicly, may not be clear who recipient is. Also problematic if keys are updated...)
- "Trusted Third Party"? (Who is that?) (How does TTP get access?) Requires more bandwidth and computation on **all** messages.
- **In any case, TTP becomes a single point of failure.**

Outline

Where are we?

Trying to give clear definitions

Challenges for government access

Other issues

Conclusions

Challenge: **Erasing Data**

- Erasure may be legally required.

Challenge: **Erasing Data**

- Erasure may be legally required.
- Best practice for erasing data is often to: (1) encrypt the data, and (2) erase the key when you want to erase the data.

CSAIL

Challenge: **Erasing Data**

- Erasure may be legally required.
- Best practice for erasing data is often to: (1) encrypt the data, and (2) erase the key when you want to erase the data.
- Works well even if data is backed up many ways.

CSAIL

Challenge: **Erasing Data**

- Erasure may be legally required.
- Best practice for erasing data is often to: (1) encrypt the data, and (2) erase the key when you want to erase the data.
- Works well even if data is backed up many ways.
- But this leaves ciphertexts no one can decrypt!

CSAIL

Challenge: **Erasing Data**

- Erasure may be legally required.
- Best practice for erasing data is often to: (1) encrypt the data, and (2) erase the key when you want to erase the data.
- Works well even if data is backed up many ways.
- But this leaves ciphertexts no one can decrypt!
- Examples: Corporate emails. Snapchat.

CSAIL

Challenge: **Erasing Data**

- Erasure may be legally required.
- Best practice for erasing data is often to: (1) encrypt the data, and (2) erase the key when you want to erase the data.
- Works well even if data is backed up many ways.
- But this leaves ciphertexts no one can decrypt!
- Examples: Corporate emails. Snapchat.
- **Government access seems to preclude this best practice for data erasure.**

Challenge: **Forward Secrecy**

- It is best practice not to keep message keys around longer than necessary.

Challenge: **Forward Secrecy**

- It is best practice not to keep message keys around longer than necessary.
- Many systems now use Diffie-Hellman key agreement to derive a transient message encryption key; this key is discarded once the message is decrypted.

CSAIL

Challenge: **Forward Secrecy**

- It is best practice not to keep message keys around longer than necessary.
- Many systems now use Diffie-Hellman key agreement to derive a transient message encryption key; this key is discarded once the message is decrypted.
- Future compromises of sender or receiver don't reveal message key (or message, if it is also deleted once read).

CSAIL

Challenge: **Forward Secrecy**

- It is best practice not to keep message keys around longer than necessary.
- Many systems now use Diffie-Hellman key agreement to derive a transient message encryption key; this key is discarded once the message is decrypted.
- Future compromises of sender or receiver don't reveal message key (or message, if it is also deleted once read).
- **Government access would require violation of this best practice.**

CSAIL

Challenge: **Computing on encrypted data**

- Recent advances in theory of cryptography allow providers to maintain and, **work with**, encrypted databases (without decrypting).

CSAIL

Challenge: **Computing on encrypted data**

- Recent advances in theory of cryptography allow providers to maintain and, **work with**, encrypted databases (without decrypting).
- Powerful techniques such as **fully homomorphic encryption (FHE)** allow provider to **create new ciphertexts by combining old ones** in many ways.

CSAIL

Challenge: **Computing on encrypted data**

- Recent advances in theory of cryptography allow providers to maintain and, **work with**, encrypted databases (without decrypting).
- Powerful techniques such as **fully homomorphic encryption (FHE)** allow provider to **create new ciphertexts by combining old ones** in many ways.
- New ciphertexts may even be encrypted with different public keys.

CSAIL

Challenge: **Computing on encrypted data**

- Recent advances in theory of cryptography allow providers to maintain and, **work with**, encrypted databases (without decrypting).
- Powerful techniques such as **fully homomorphic encryption (FHE)** allow provider to **create new ciphertexts by combining old ones** in many ways.
- New ciphertexts may even be encrypted with different public keys.
- **Government access methods may not be compatible with FHE.**

CSAIL

Challenge: **Threshold cryptography**

- Best practice may require “**two-man rule**” or the like, usually implemented with “**threshold cryptography**” (aka “**secret-sharing**”).

CSAIL

Challenge: **Threshold cryptography**

- Best practice may require "**two-man rule**" or the like, usually implemented with "**threshold cryptography**" (aka "**secret-sharing**").
- Each party may hold only a "share" of a ciphertext.

CSAIL

Challenge: **Threshold cryptography**

- Best practice may require "**two-man rule**" or the like, usually implemented with "**threshold cryptography**" (aka "**secret-sharing**").
- Each party may hold only a "share" of a ciphertext.
- A single share is not decryptable; several must be combined in order to decrypt.

CSAIL

Challenge: **Threshold cryptography**

- Best practice may require "**two-man rule**" or the like, usually implemented with "**threshold cryptography**" (aka "**secret-sharing**").
- Each party may hold only a "share" of a ciphertext.
- A single share is not decryptable; several must be combined in order to decrypt.
- **Government access may not be compatible with threshold cryptography.**

Challenge: **Quantum cryptography**

- Cryptographic methods based on **quantum mechanics** are starting to become tested and commercially available.

CSAIL

Challenge: **Quantum cryptography**

- Cryptographic methods based on **quantum mechanics** are starting to become tested and commercially available.
- It isn't clear (to me) what it would mean for a quantum-based cryptographic system to provide "government access."

CSAIL

Challenge: **Quantum cryptography**

- Cryptographic methods based on **quantum mechanics** are starting to become tested and commercially available.
- It isn't clear (to me) what it would mean for a quantum-based cryptographic system to provide "government access."
- **Government access may not be compatible with quantum cryptography.**

CSAIL

Challenge: **Other New Forms of Cryptography**

Cryptography is rapidly evolving and producing many new and useful ways of achieving confidentiality. You can encrypt so that:

- only those who **know a solution to a hard problem** can decrypt.

CSAIL

Challenge: **Other New Forms of Cryptography**

Cryptography is rapidly evolving and producing many new and useful ways of achieving confidentiality. You can encrypt so that:

- only those who **know a solution to a hard problem** can decrypt.
- decryption is only possible after **a certain amount of time**.

CSAIL

Challenge: **Other New Forms of Cryptography**

Cryptography is rapidly evolving and producing many new and useful ways of achieving confidentiality. You can encrypt so that:

- only those who **know a solution to a hard problem** can decrypt.
- decryption is only possible after **a certain amount of time**.
- **decryption doesn't always succeed** (yes, this can be useful!).

CSAIL

Challenge: **Other New Forms of Cryptography**

Cryptography is rapidly evolving and producing many new and useful ways of achieving confidentiality. You can encrypt so that:

- only those who **know a solution to a hard problem** can decrypt.
- decryption is only possible after **a certain amount of time**.
- **decryption doesn't always succeed** (yes, this can be useful!).
- a user can **convincingly deny that a given "ciphertext" has any associated "plaintext"**

CSAIL

Challenge: **Other New Forms of Cryptography (cont.)**

You can encrypt so that:

- a group of parties is required to interact collaboratively to decrypt. (MPC)

CSAIL

Challenge: **Other New Forms of Cryptography (cont.)**

You can encrypt so that:

- a group of parties is required to interact collaboratively to decrypt. (MPC)
- you can **search for ciphertexts encrypting a given plaintext**.

CSAIL

Challenge: **Other New Forms of Cryptography (cont.)**

You can encrypt so that:

- a group of parties is required to interact collaboratively to decrypt. (MPC)
- you can **search for ciphertexts encrypting a given plaintext**.
- you can **encrypt and authenticate at the same time**.

CSAIL

Challenge: **Other New Forms of Cryptography (cont.)**

You can encrypt so that:

- a group of parties is required to interact collaboratively to decrypt. (MPC)
- you can **search for ciphertexts encrypting a given plaintext**.
- you can **encrypt and authenticate at the same time**.
- **Government access may be incompatible with these (and other) new forms of cryptography.**

CSAIL

Outline

Where are we?

Trying to give clear definitions

Challenges for government access

Other issues

Conclusions

Issue: Innovation may be harmed

- Cryptography is an essential component of of information infrastructure.

Issue: Innovation may be harmed

- Cryptography is an essential component of of information infrastructure.
- Regulation of cryptography may stifle innovation critical for the growth of the American internet-based economy.

CSAIL

Issue: Does LE really want access to **all** encrypted data?

- **Votes** in voting scheme?

CSAIL

Issue: Does LE really want access to **all** encrypted data?

- **Votes** in voting scheme?
- **Bid information** in an government auction?

CSAIL

Issue: Does LE really want access to **all** encrypted data?

- **Votes** in voting scheme?
- **Bid information** in an government auction?
- **Password database** in a password manager?

CSAIL

Issue: Does LE really want access to **all** encrypted data?

- **Votes** in voting scheme?
- **Bid information** in an government auction?
- **Password database** in a password manager?
- **Medical information**?

CSAIL

Issue: Does LE really want access to **all** encrypted data?

- **Votes** in voting scheme?
- **Bid information** in an government auction?
- **Password database** in a password manager?
- **Medical information**?
- **Classified information**?

CSAIL

Issue: Does LE really want access to **all** encrypted data?

- **Votes** in voting scheme?
- **Bid information** in an government auction?
- **Password database** in a password manager?
- **Medical information**?
- **Classified information**?
- **Government access may need to be limited to certain kinds of information**.

CSAIL

Issue: Cost of implementing government access may be high

- Costs of “letting LE in” may be at least as high or higher than the cost of “keeping Chinese out”.

CSAIL

Issue: Cost of implementing government access may be high

- Costs of “letting LE in” may be at least as high or higher than the cost of “keeping Chinese out”.
- **It may be better for our country if our security engineers focus on “keeping the Chinese out.”**

CSAIL

Issue: Regulation likely to be ineffective

- AES invented by Belgians!
- Number of apps for sale having encryption: "There are at least 865 hardware or software products incorporating encryption from 55 different countries. This includes 546 encryption products from outside the US, representing two-thirds of the total. ... 66% are proprietary, and 34% are open source."
- There are other ways of achieving confidentiality besides "encryption."
- **Government access policy would need to be international and cover other mechanisms for confidentiality.**

Outline

Where are we?

Trying to give clear definitions

Challenges for government access

Other issues

Conclusions

Conclusions

- “Government access to plaintext” is a complex issue.

Conclusions

- “Government access to plaintext” is a complex issue.
- I’ve only touched on a few of the issues and examples.

Conclusions

- “Government access to plaintext” is a complex issue.
- I’ve only touched on a few of the issues and examples.
- Please think hard about the challenges given here, and the **25 unanswered questions** at end of “**Keys Under Doormats** paper.

Conclusions

- “Government access to plaintext” is a complex issue.
- I’ve only touched on a few of the issues and examples.
- Please think hard about the challenges given here, and the **25 unanswered questions** at end of “**Keys Under Doormats** paper.
- **This committee may be looking for a “solution” that doesn’t exist...**

CSAIL

The End