Who Can you Trust? (When you're trusting trust)

JPEG Privacy & Security Workshop

Jeremy Malcolm and Cory Doctorow

La Jolla, CA

February 23, 2016

Outline

1. **Crypto**
   - Crypto and privacy
   - Crypto and content restriction
2. **Law**
   - Anti-Circumvention Law
   - Skirting Around Anti-Circumvention Law

1. **Crypto**
2. Law

How Crypto Works for Privacy

- Used to distribute files safely

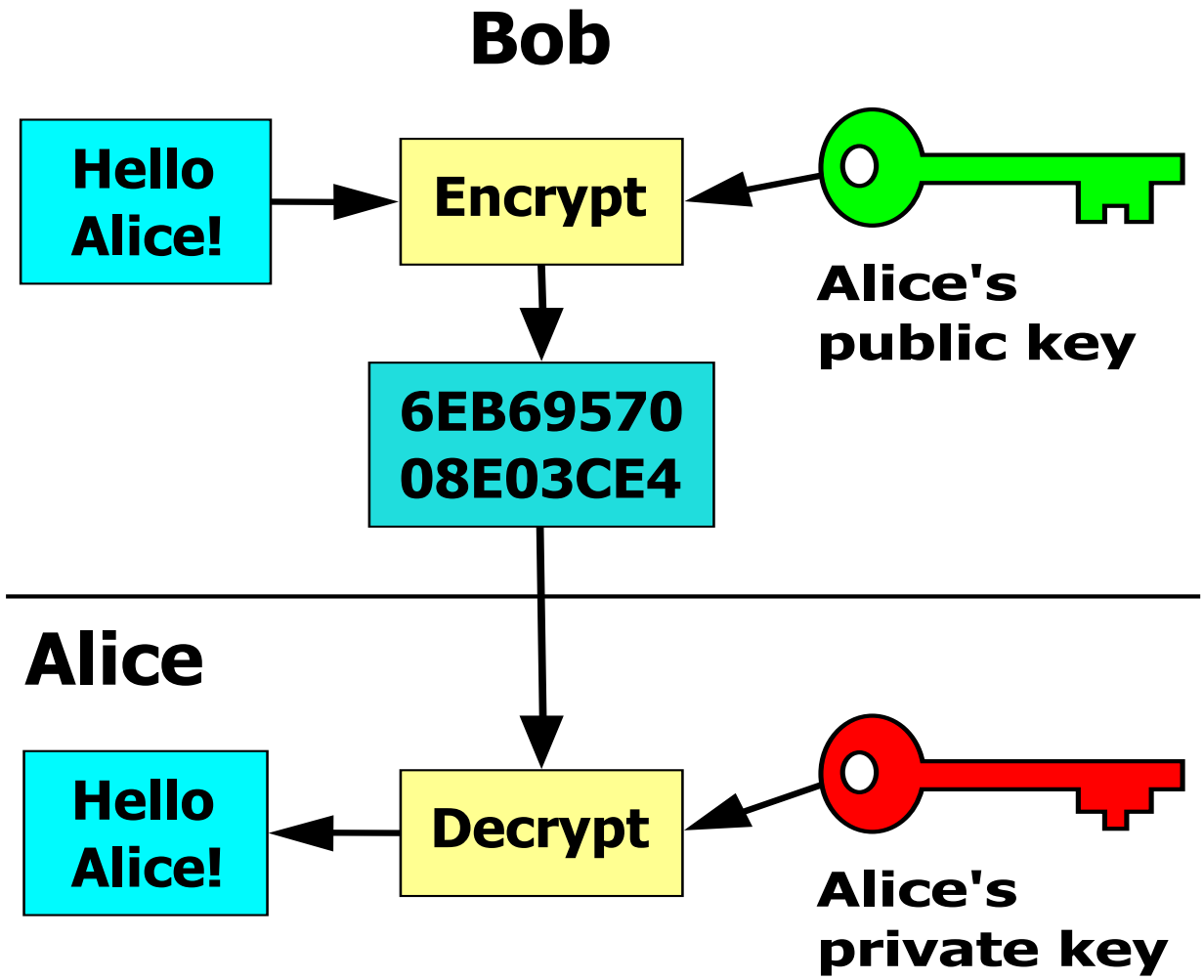
How Crypto Works for Privacy

- Used to distribute files safely
- Requires a key-management system to ensure only the intended party can decrypt

How Crypto Works for Privacy

- Used to distribute files safely
- Requires a key-management system to ensure only the intended party can decrypt
- In asymmetric encryption, each party only controls their own private key

Asymmetric Key Encryption



How Crypto "Works" for DRM

- Asymmetrical encryption is still typically used, to reduce processing load
- Symmetrical encryption can be used, for simpler media formats

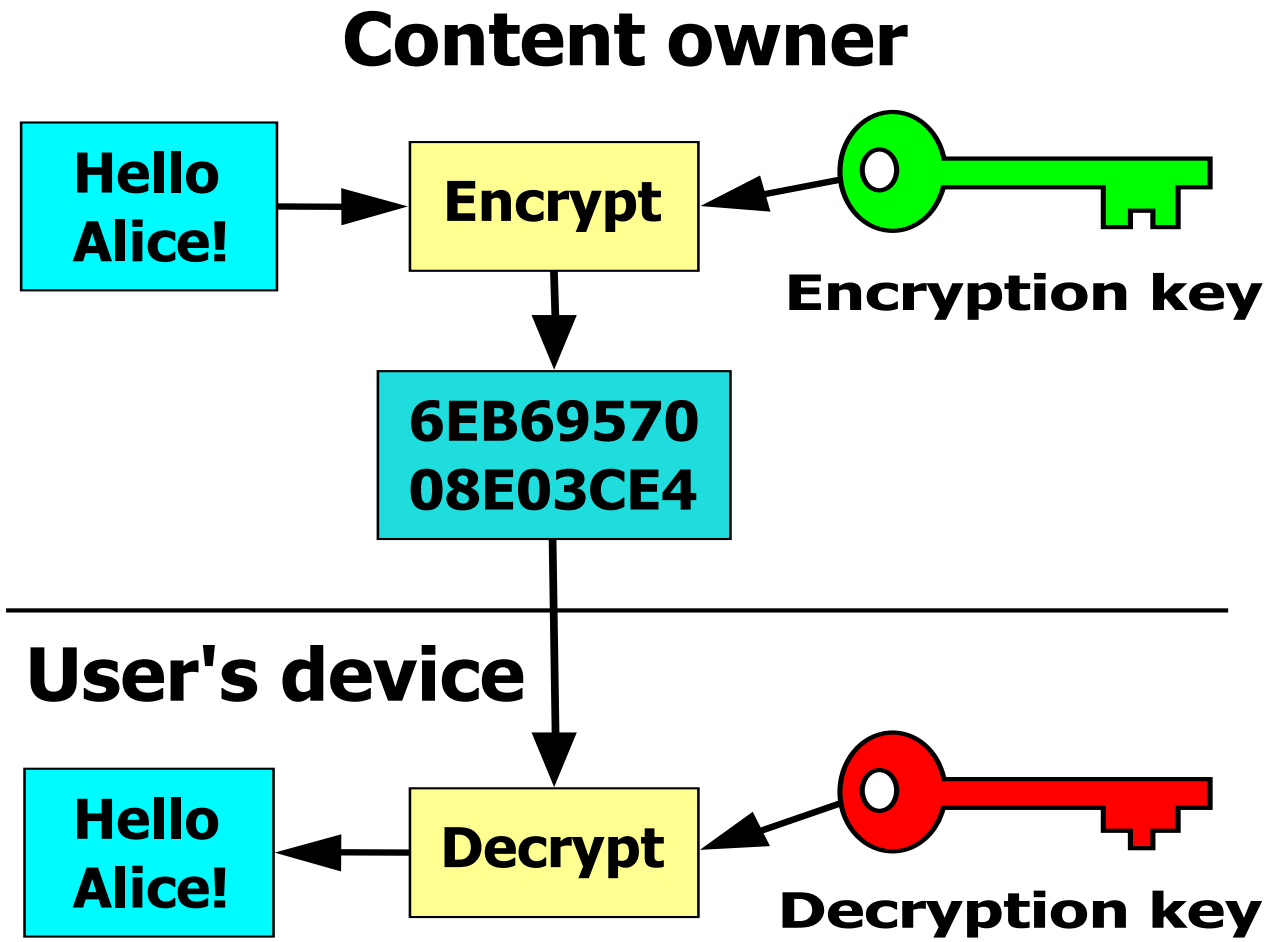
How Crypto "Works" for DRM

- Asymmetrical encryption is still typically used, to reduce processing load
- Symmetrical encryption can be used, for simpler media formats
- However, the content owner tries to control *both* keys

How Crypto "Works" for DRM

- Asymmetrical encryption is still typically used, to reduce processing load
- Symmetrical encryption can be used, for simpler media formats
- However, the content owner tries to control *both* keys
- This is, of course, impossible

DRM Encryption



DRM Crypto Is Weaker Than Privacy Crypto

- DRM systems, symmetric or asymmetric, will always be crackable

DRM Crypto Is Weaker Than Privacy Crypto

- DRM systems, symmetric or asymmetric, will always be crackable
- Partial non-solutions:
  - Session keys
  - Obfuscation of the decryption key stored in the device
  - Remote key revocation if (when) keys are cracked

1. Crypto
2. **Law**

Why Anti-Circumvention Law?

- Because crypto is not fit for the purposes of DRM, the law steps in to make its circumvention illegal

Why Anti-Circumvention Law?

- Because crypto is not fit for the purposes of DRM, the law steps in to make its circumvention illegal
- This only applies to copyright
- No similar provision prevents breaking any other kind of crypto, such as that protecting user privacy
- The implication? Copyright has more value than privacy

Why Anti-Circumvention Law?

- Because crypto is not fit for the purposes of DRM, the law steps in to make its circumvention illegal
- This only applies to copyright
- No similar provision prevents breaking any other kind of crypto, such as that protecting user privacy
- The implication? Copyright has more value than privacy

Example

No person shall circumvent a technological measure that effectively controls access to a work protected under this title. — 17 U.S. Code § 1201

Side-Effects of Anti-Circumvention Law

Anti-circumvention law can result in five years prison terms for coders who:

- merely report vulnerabilities in the code
- implement a compatible player
- supply tools for others to use *even for lawful exceptions to anti-circumvention law!*

And the worst part is...

We are exporting this crappy law all around the world

How JPEG Committee Should Implement Crypto

- Adding privacy and security features to images is a great concept
- But in order to avoid coders being made subject to 1201 liability:
  - It should only facilitate encryption of (seldom copyrightable) metadata
  - Encryption of image data should not be part of the specification
    - (or if it is, the user should retain access to their own crypto keys)
- This will enable JPEG to remain an open and interoperable standard

Summary

- Cryptography is an amazing technology
- But it is supported by amazingly bad laws
- To avoid this, JPEG should avoid allowing the specification to be used to lock up copyright content especially if the user does not control their own private or decryption key