DRM

Class discussion

Enigma Machine

Encryption

- Plaintext
- Cipher (Algorithm) + Key
- Ciphertext

Simple Encryption

- Plaintext: “HELLO WORLD”
- Cipher, Key: shift forward, 3 letters
- Ciphertext: “KHOOR ZRUOG”

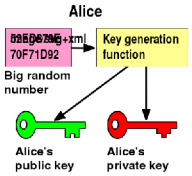
Decryption of Simple Cipher

- Ciphertext: “KHOOR ZRUOG”
- Cipher, Key: shift **backwards**, 3 letters
- Plaintext: “HELLO WORLD”
- Decryption reverses the process, using the same or a related algorithm.

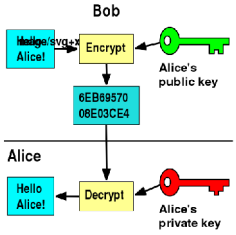
Public-key encryption

- Each participant to the communication generates a pair of mathematically related keys, one public and one private.
  - One-way functions make this keypair computationally easy to create, but very difficult to reverse.
  - Messages encrypted with the public key can be decoded with the private key, and vice versa.
  - The basis of PGP and digital signatures.

Public-Private key pair



Communication



- DRM as "private ordering"
  - Price discrimination / market segmentation / choice
- Property -> contract
  - How is the bargaining power balanced?
  - Will people just short-circuit the shift by piracy/civil disobedience?
  - Clever technical hacks?
- Alternatives:
  - Government-created DRM

Alternatives

- Government-[created | standardized] DRM
  - Eliminate incompatibilities, DRM-provider isn't the bottleneck
  - Privacy concerns
    - Content,
    - centralization
  - Censorship, First Amendment
- Mandated "rights-management system"
  - One target to break
- Compulsory licensing

"The Celestial Jukebox"

- E.g., Yahoo! Music unlimited
  - Subscription "rental"
  - Access to a large number of songs
  - Dock once a month, else it all expires
  - What can you do with the music once you have it?
  - Change how music is made? Fewer albums, less cover art; direct-to-fan communications
  - Will it last?

The Celestial Jukebox

- It's great if you hack it, and pay for it
- So long as it's one of many options
  - Lawful competition, otherwise people will go for unlawful
- Darknet is here to stay:
  - it just takes one person to hack it, then share the hacked copy
  - Can we minimize hacking, as we minimize shoplifiting without eliminating it?
  - Why not allow customers to pay for unrestricted version?
    - Is there a restricted version that's acceptable?
    - Does DRM just hurt the lawful user?

- Shift between artificial and real scarcity?

Restrictions

- Content-restrictions beyond those of copyright
- Can DRM encapsulate copyright?
  - "prior restraint"
  - Hard-code U.S. Code, but what about the fuzzy edges? Leaving the edge-cases to publishers will be too restrictive
  - What about a more permissive DRM with aa monitoring component?
  - User-tailored licenses? We don't know in advance who's a critic. Bloggers becoming "press"
    - Anonymous use
  - Does copyright law have to mandate First Amendment protections?

Contract vs. tech

- Hypo: DRM on G.W.B.'s autobiography: sale with a "no un-vetted review" contract.
  - Unenforceable contract?
  - Get an injunction against the DRM?
  - Shifting the burden of complaining. Chilling effect of a prior restraint. Go to court each time you want a fair use?
  - Moving fair use from a defense (response to suit) to an offensive move (require a DJ)
  - Or is the threat of suit enough to stop fair use?
  - Error costs. Barriers to entry.
- What if everyone in a market moved to DRM restriction?
  - Piracy as a restraint on this market development?

Piracy

- Calculated risk?
- Reverse lottery?
- Check on copyright holder overreach?
- How much piracy should we tolerate? How much should we punish it?
- Indication of market failure?
- What motivates it? Ease? Market failure to supply consumer needs?

Restricted v. unrestricted

- DRM makes the purchased product less valuable than the "free" one
- DRM offers shades of grey between the black and white or fee and free
- Can we set up a market with both some DRM versions and a fully unrestricted version? Would that develop? Would it work?
  - EMI's DRM-free downloads?
  - Will markets look different across different forms of media? Different market structures (concentration or competition)?

Generativity

- Kindle
  - Anti-generative: single-purpose, locked-down,
  - Kindle could be part of a generative system? spurring creative authorship
- User becoming creator, changing the technology's uses
  - Who gets to define the technology?
  - Who gets to anticipate the uses? Repurpose?