



Last bit on Anonymity; Privacy and Decentralization I

Information Privacy with Applications
David Sidi (dsidi@email.arizona.edu)



Administrative Items

- Final project proposals due tonight (unless we've talked)
- Anonymity assignment Thursday
- Integrated session also Thursday!



Session keys are negotiated using Diffie-Hellman Key Exchange

- First published in 1976; still around
- Alice and Bob want to share a secret key for use in a symmetric cipher. Every piece of information that they exchange is observed by their adversary Eve. How is it possible for Alice and Bob to agree on a key without making it available to Eve?

Diffie-Hellman

Publicly choose:

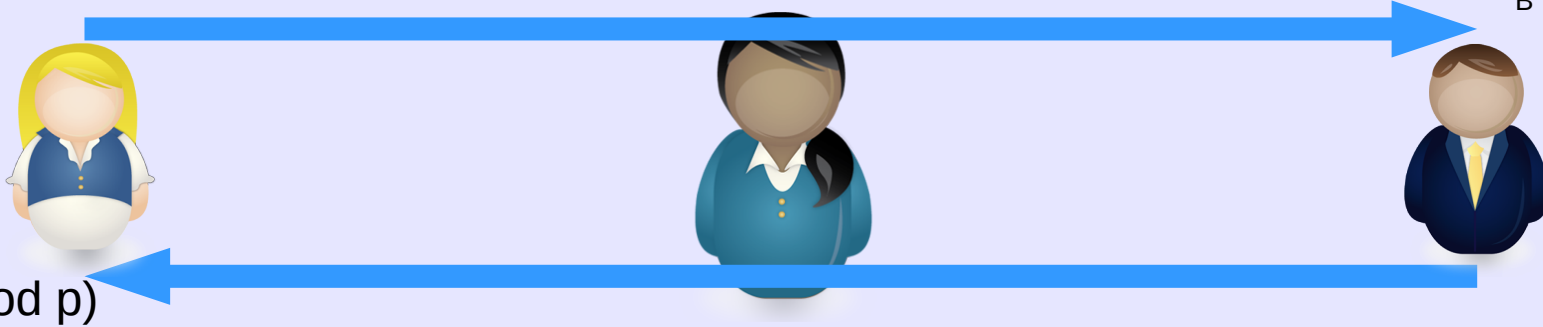
- a safe large prime p (e.g. Tor docs use rfc2409 section 6.2. But see Logjam)
- g , a primitive root mod p , with $2 \leq g \leq p-2$

Secretly generate:

- Alice and Bob randomly choose secret integers $1 \leq x, y \leq p-2$ respectively

$$A := g^x \pmod{p}$$

$$K_B := A^y \pmod{p}$$

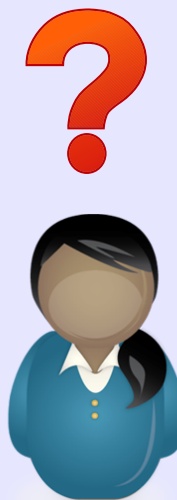


$$B := g^y \pmod{p}$$

$$K_A = (g^y)^x = (g^x)^y = K_B \text{ is the key}$$



Diffie-Hellman



$$x = \log_g A \pmod{p}$$

$$y = \log_g B \pmod{p}$$

Diffie-Hellman



$$x = \log_g A \pmod{p}$$

$$y = \log_g B \pmod{p}$$

Discrete Log Problem is in NP

Diffie Hellman Problem is no harder than DL problem; there is no proof of the converse

Question

- Ian Goldberg long ago remarked that a good way to fight mass surveillance by a global passive adversary would be to “do a quick Diffie-Hellman” by default when setting up otherwise unprotected connections. He notes that this won’t help against an active attack. Can you guess what he means by an active attack?

MiTM Diffie-Hellman

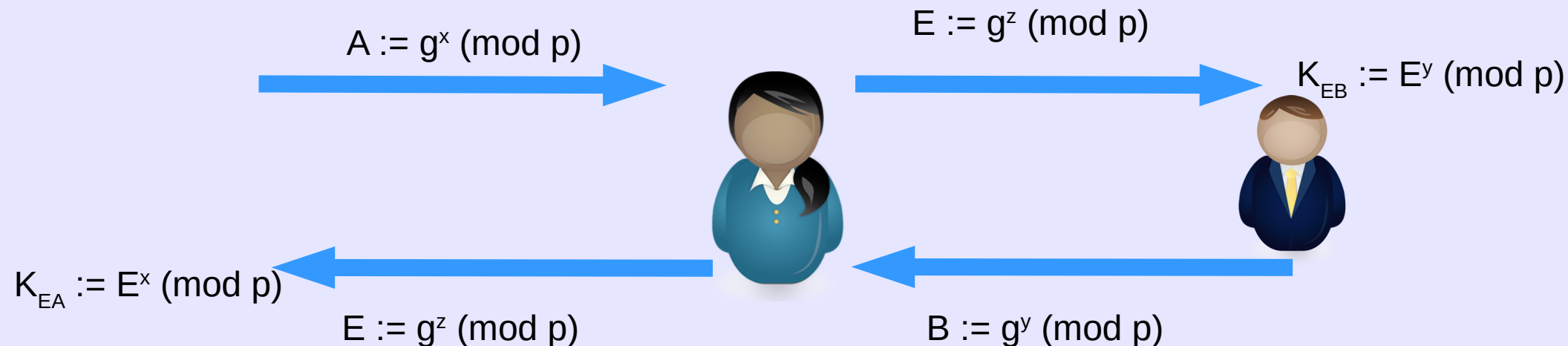
Publicly choose:

a secure large prime p

g , a primitive root mod p , with $2 \leq g \leq p-2$

Secretly generate:

- Alice and Bob choose secret integers $0 \leq x, y \leq p-2$ respectively
- Eve picks her own secret integer, z



MiTM Diffie-Hellman

Publicly choose:

a secure large prime p

g , a primitive root mod p , with $2 \leq g < p$

$$K_{EA} := g^{xz} \pmod{p}$$

$$K_{EB} := g^{yz} \pmod{p}$$

Secretly generate:

- Alice and Bob choose secret integers $0 \leq x, y \leq p-2$ respectively

- Eve picks her own secret integer, z

$$A := g^x \pmod{p}$$

$$E := g^z \pmod{p}$$

$$K_{EB} := E^y \pmod{p}$$

$$K_{EA} := E^x \pmod{p}$$

$$E := g^z \pmod{p}$$

$$B := g^y \pmod{p}$$



Tor protocol, cont'd

- once session keys are agreed upon with DH, encrypt for the exit node, then encrypt the result for the relay node, and finally encrypt the result for the guard node
- send the layered result to the guard node
- guard node decrypts, gets the next hop and sends it on, then the middle key decrypts, ...
- on way back, each node uses the session key agreed on with the client OP, and passes to its neighbor in the circuit



Tor strengths and weaknesses

- Strengths
 - widespread adoption
 - low latency
 - easy to run nodes, easy to use as a client: adds to security
 - bridges, pluggable transports for censorship circumvention
 - fingerprint resistance (Tor Browser)
 - Applications ecosystem (SecureDrop, Briar, Ricochet, OnionShare, Tails, ...)
- Weaknesses
 - traffic analysis by a global/pervasive passive adversary
 - end-to-end timing attacks
 - content is revealed to exit node
 - blockable exit nodes



Who runs exit nodes?

- Universities
 - MIT+, Michigan, CMU, UNC, Karlsruher IT, Stanford, Clarkson, U. Washington, Utah+, Caltech, RIT+, Bowdoin, Northeastern+, Princeton
- Bad people too! (Why might they do that?)
- Not Arizona :-(
 - yet (-:



Who runs hidden services?

- Propublica, Duckduckgo, Facebook, Scihub, Riseup, Protonmail, Debian, Whonix, The Intercept, Wikileaks, Securedrops for The Freedom of the Press Foundation, The Guardian, The Associated Press, NY Times, USA Today, Washington Post, etc., TORCH (these are all onion links)
- A bunch of people with illegal stuff
- Hidden services are easy to set up (demo)
 - even inside firewalled networks

Privacy and Decentralization I

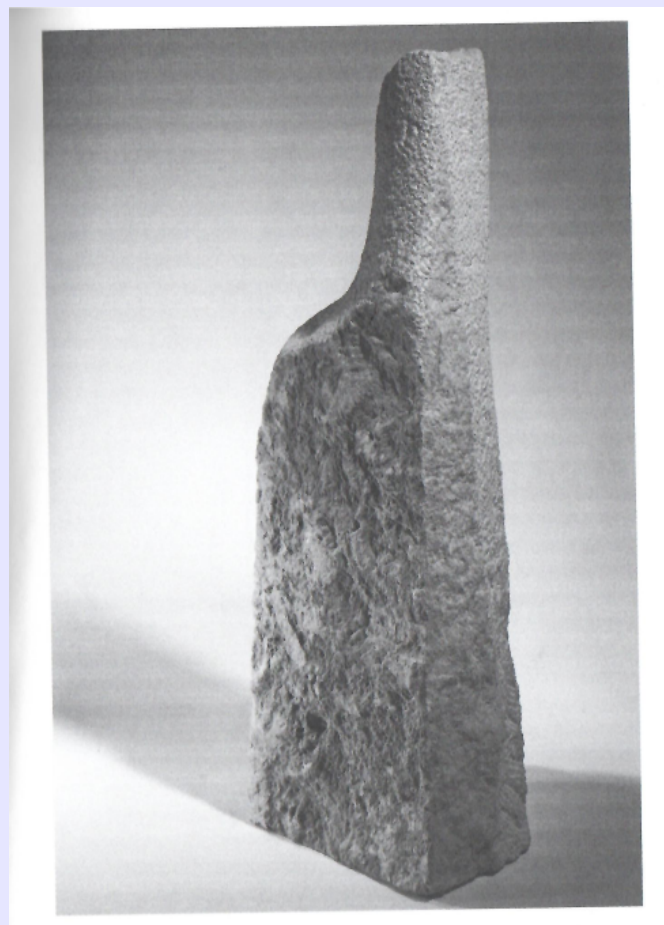


- The tools you choose to use influences your practice
 - What happens when your tools are services, provided by another party?





- How do you ensure that practice influences your use and choice of tools?



Batya Friedman, *Value Sensitive Design*

- Zoom was not made for education, but for business management

Good video communication will attract top talent and encourage flexible working conditions

Arguably, all of these tips fall under the primary use for video communication — to connect people who are not in the same physical space.

"I was the first employee [in Australia] a couple of years ago, and we wouldn't have been able to grow as quickly as we [did] to the 80-odd people we have across Asia without using tools such as Zoom," Michael says.

"Being remote and having that connection

From an employer's perspective, removing live has the potential to increase access to t

 **Multi-platform management:** The average organization uses more than one conferencing system and seeks a management solution that is "fluent" in multiple platforms

 **Legacy conferencing system migrations:** How can an organization most effectively utilize legacy hardware systems and still achieve end user satisfaction using new UC platforms?

 **Actionable Meeting Room Analytics:** Deriving analytics such as room utilization and room availability which lead directly to actionable 'fix it' guidance for IT.

 **Zoom Room troubleshooting:** ...and Microsoft Teams Room (MTR), and Skype Room Systems (SRS) troubleshooting too-providing 24x7 answers to multiple end user issues

 **Software & Hardware Symbiosis:**





- e-learning and ed-tech has been a thing for a while now
- COVID-19 has been a boon
- Big part of the sell with ed-tech is to increase efficiencies through use of analytics available online (or via other technologies)



- Zoom went from 10M to 300M users, partly by removing the limited use restriction for educational uses
- Zoom is valued at 29x its revenue in the last year
 - Free users cost; they will need to convert them to something valuable.
 - What is a common model for providing “free” services on the Internet?



COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

USER DATA



The nice thing about students working on-line is that you get a much better overview of their study behavior. As I aggregate over 260 active s



from Gürses, Rectanglez-R-Us



- Third-party service providers are available *now*, in the short term
 - useful when a pandemic forces many students online
- What are the long-term implications of that transition?



Principal agent problems

- Zoom bombs: Zoom is a global organization, so the needs of individual institutional licensees are not paramount.
- For a while, response to Zoom bombs was: “we’ll do some, and the rest is your responsibility” until the clamor was too loud



- Downsides of the Zoom licensing model?
- “Unbundling of institutions:” pressure to grow for Zoom resulting in hollowing out of various parts of Universities?
- “Context collapse”
- What is this new abstraction of the classroom, that takes place on commercial services like Zoom, or Facebook, or Google Docs, and who is it available to?
- Zoom security “sucks”



Tools and Self-Determination

- *Who should decide on the tools that are used?*
Should faculty, students and staff decide for themselves? For which tools? What happens if something goes wrong?
- (What is “predatory inclusion?”)