Lecture 1

CS-466 Applied Cryptography

Adam O'Neill

Crypto Games!!!

Class Logistics

Class Logistics

Instructor: Adam O'Neill; adamo@cs.umass.edu

Office Hours: Tues & Thurs before class (roughly 2:45-3:45pm) or by appointment, LGRC 329A (Low-rise)

Course website: https://people.cs.umass.edu/~adamo/sp19466/index.html

TA: Albert Williams; abwillia@cs.umass.edu

Office Hours: Weds 2-3pm, LGRT 220 (High-rise)

Class Logistics

Grades: 50% problem sets, 25% midterm, 25% final

Final grades are are given according to equivalence classes via a formula which depends on the scores. **If you all do well you all get an A.**

For problem sets, you can discuss or use any resource but must list your collaborators/resources. Write your final solutions by yourself. Please typeset them. Turn in PDF via procedure detailed later.

Some Additional Resources

Bellare's courses
http://cseweb.ucsd.edu/~mihir/cse107/
http://cseweb.ucsd.edu/~mihir/cse207/

Rogaway's Courses
http://web.cs.ucdavis.edu/~rogaway/classes/127/winter19/

Boneh's Courses
http://crypto.stanford.edu/~dabo/courses/cs255_winter18/

Boneh-Shoup Book
https://crypto.stanford.edu/~dabo/cryptobook/

Katz-Lindell book
http://www.cs.umd.edu/~jkatz/imc.html

Reyzin Course
https://www.cs.bu.edu/~reyzin/teaching/f14cs538/

How to do well in this course

- Don't focus on your grade, just try your best
- Be adventurous, quizzical
- Think of the class as telling a story
- Try to make your thoughts rigorous and precise, in the language of mathematics

http://cseweb.ucsd.edu/~mihir/education.html

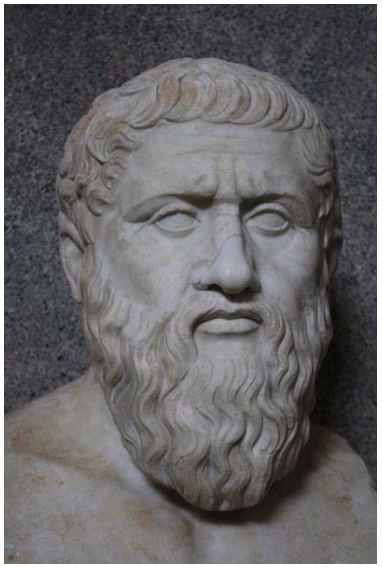
What’s cryptography?

What's Cryptography?

One viewpoint (Goldreich):

How to communicate and compute in the presence of an adversary.

Cryptography is a part of science in the same way as math or physics.



What's Cryptography?

Another viewpoint (Bellare/Rogaway):

There is no such thing as **Cryptography**, really.

There are only CRYPTOGRAPHERS.

How many can you name?

What's Cryptography?

Another viewpoint (Bellare/Rogaway):

Cryptography is socially constructed.

Cryptography is alive, not a textbook!

See http://web.cs.ucdavis.edu/~rogaway/papers/cc.pdf

The analogy to art

There is no such thing as **Art**, really.

There are only ARTISTS.

The Story of Art
E. H. Gombrich












How many can you name?

What does this mean?

There is no such thing as “secure encryption scheme” ontologically

But still we need a definitions that are

- Precise
- Useful

Security Mindset

Put on your adversary hat!

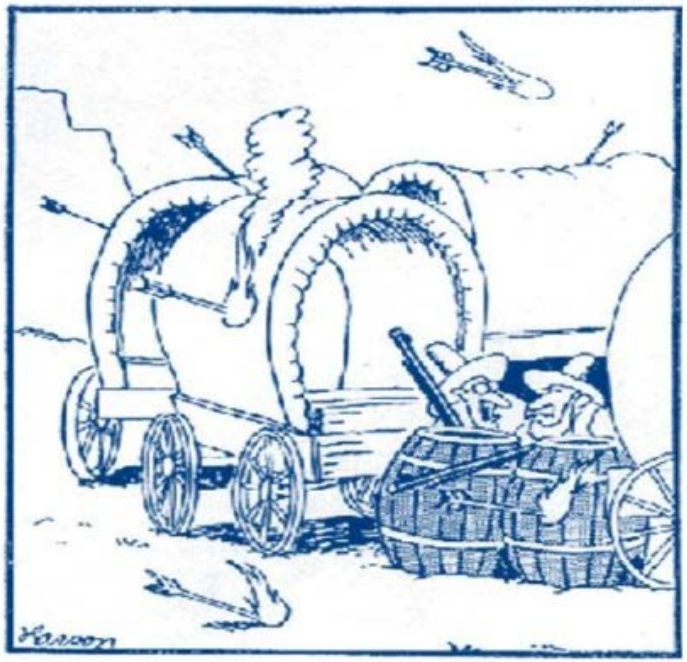
Ask what the risks and threats are. How might the system be attacked?

Be critical of security claims.

Our system is secure because it uses 128-bit keys!

How are they being used? What is the threat model? Do you have a security proof?

Coloring outside the lines



"Hey! They're lighting their arrows!
Can they do that?"

© Marc Sniukas - Doujak Corporate Development

Some goals and uses

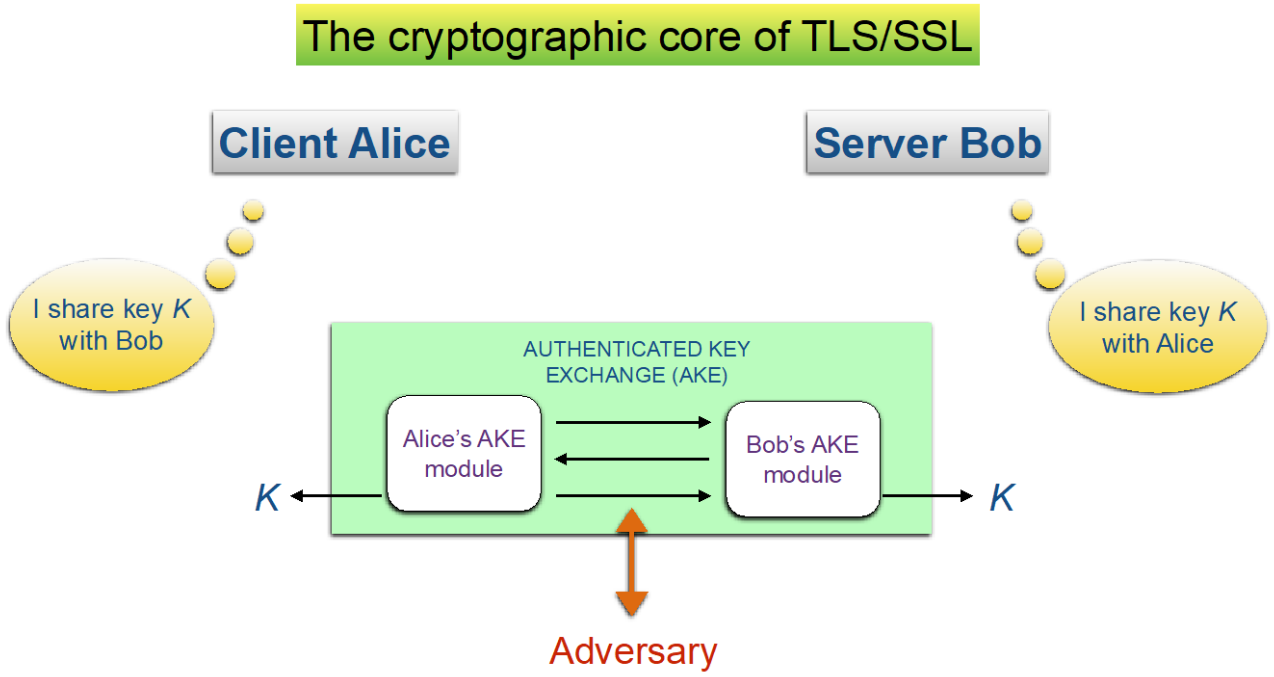
Who Uses Crypto?

You probably did, today!

- TLS/SSL protocol (used for Gmail, Facebook, YouTube…)
- 10000+ apps use crypto… most incorrectly ☹

https://www.cs.ucsb.edu/~chris/research/doc/ccs13_cryptolint.pdf

SSL/TLS



K is a fresh, authentic session key
Adversary cannot influence or know *K*

SSL/TLS

TLS/SSL Vulnerabilities

Vulnerability	crypto	Implementation/ Usage
FREAK	x	
Re-negotiation	x	
Version Rollback		x
BEAST	x	
Padding Oracle	x	
Lucky 13	x	
Poodle	x	x
Heartbleed		x
RC4	x	
AllYourSSLsAreBelongToUs		x

Many different TLS/SSL Implementations: OpenSSL, GnuTLS, cryptlib, JSSE, RSA BSafe, SChannel, …

Issues: Cipher suites, re-negotiation, side-channels, buffer overflows, bad randomness, …

Lots of bad crypto in TLS/SSL, often for historic and legacy reasons.

Secure Channels: Ideal

Secure Channels: Real

Security goals

The question of identity

On the Internet, nobody knows you are a dog.

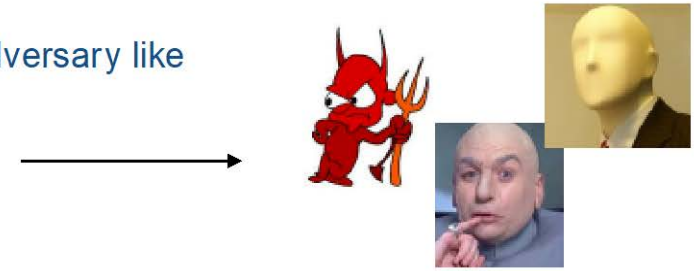
Example applications

Crypto beyond secure channels

Why does it matter?

Adversaries are real!

Academic cryptographers often represent the adversary like this



Instead think of the adversary as a well-funded, technically capable and highly motivated entity with lots of computing power.

Does it matter to you?

Eric Schmidt, CEO
Google, 2009

If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.

Glenn Greenwald

If you have nothing to hide then give me the passwords to ALL your email accounts, your text and chat histories, …

https://www.youtube.com/watch?v=pcSlowAhvUk

20 minute video of TED talk

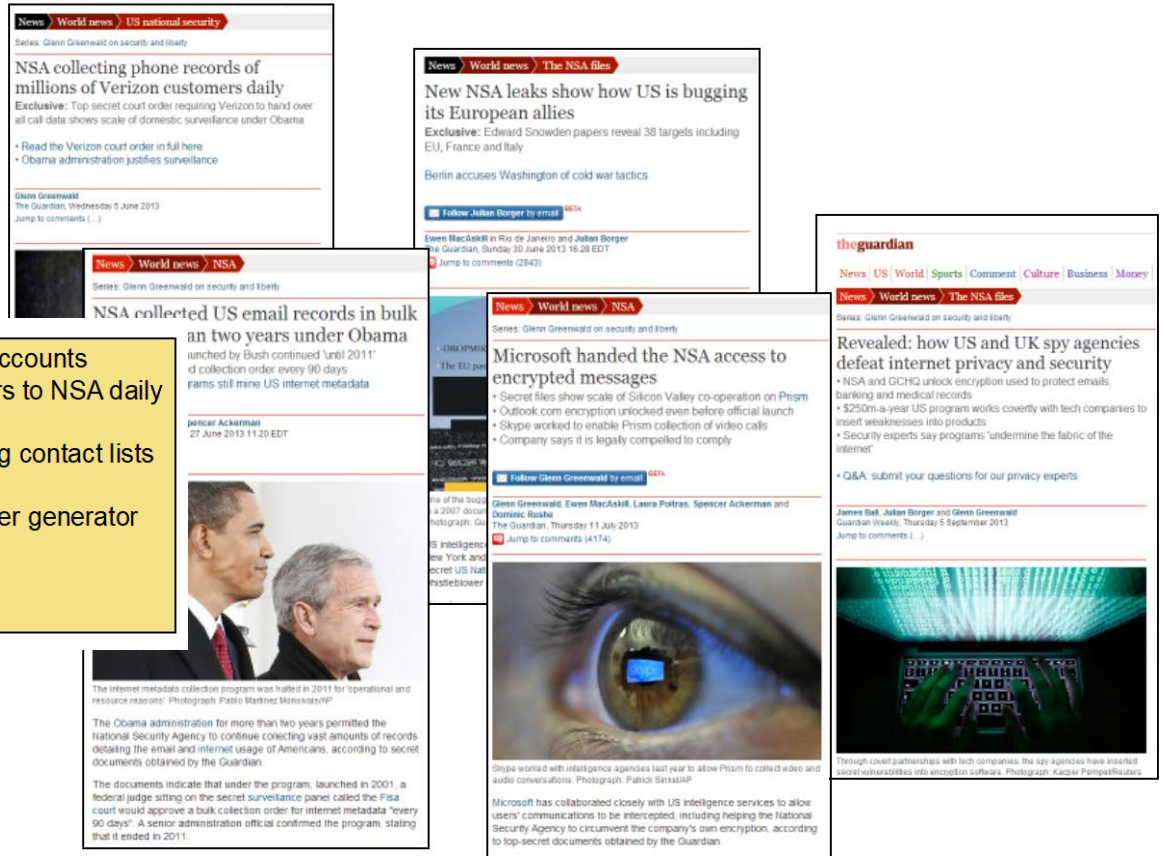
The Chronicle of Higher Education
Why privacy matters even if you have nothing to hide
http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

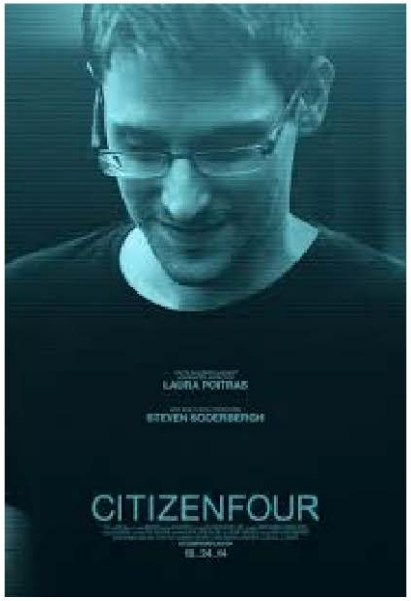
Bruce Schneier The Value of Privacy
Privacy protects us from abuses by those in power … We keep private journals, sing in the shower … privacy is a basic human need.
https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html

http://zeroknowledgeprivacy.org/library/why-privacy-matters/

Snowden revelations

Court-approved NSA access to Google and Yahoo accounts
Verizon hands phone records of millions of customers to NSA daily
Extensive wiretapping, tapping undersea cables
Harvesting of millions of email and instant-messaging contact lists
Tracking and mapping location of cellphones
Backdoor planted in Dual_EC_DBRG random-number generator
Paying corporations to adopt NSA-broken standards
Sophisticated malware
…

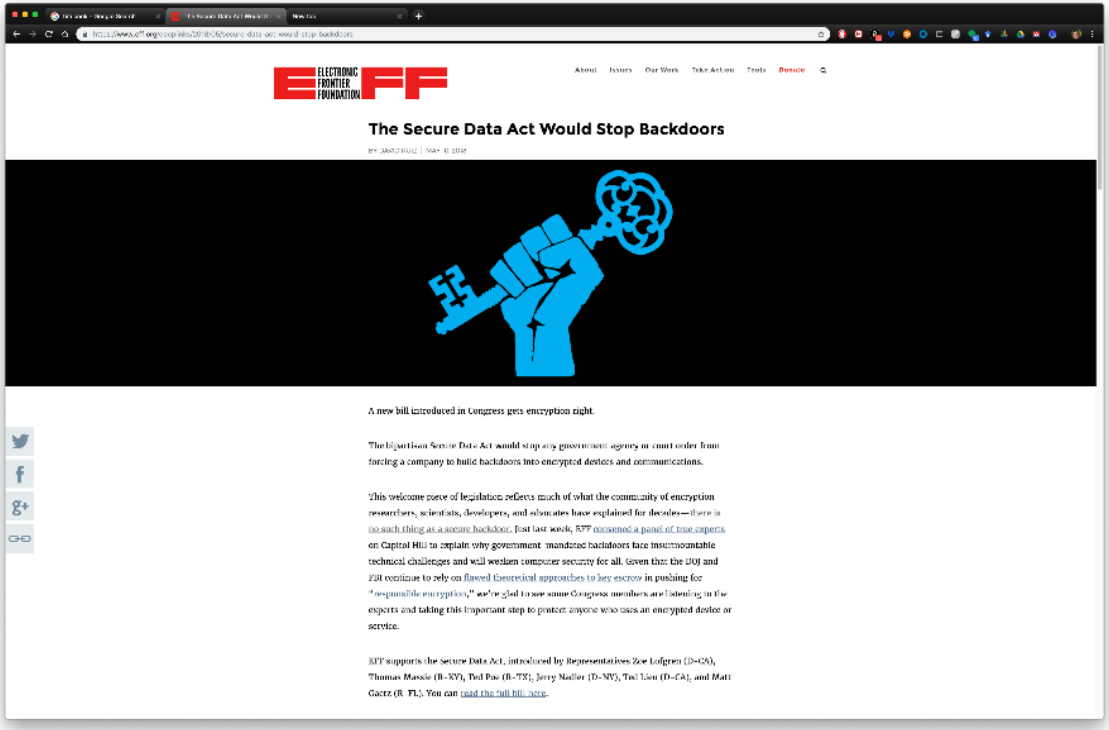




Laura
Poitras

See the movie!

Read the news!


ELECTRONIC FRONTIER FOUNDATION
About Issues Our Work Take Action Tools Donate
The Secure Data Act Would Stop Backdoors
A new bill introduced in Congress gets encryption right.
This welcome piece of legislation reflects much of what the community of encryption researchers, scientists, developers, and advocates have explained for decades—there is no such thing as a secure backdoor. Just last week, EFF convened a panel of true experts on Capitol Hill to explain why government-mandated backdoors face insurmountable technical challenges and will weaken computer security for all. Given that the DOJ and FBI continue to rely on flawed theoretical approaches to key escrow in pushing for "responsible encryption," we're glad to see some Congress members are listening to the experts and taking this important step to protect anyone who uses an encrypted device or service.
EFF supports the Secure Data Act, introduced by Representatives Zoe Lofgren (D-CA), Thomas Massie (R-KY), Ted Poe (R-TX), Jerry Nadler (D-NY), Ted Lieu (D-CA), and Matt Gaetz (R-FL). You can read the full bill here.

Backdoors

Backdoors: The Debate

Mandatory backdoors

https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval

"Manhattan project"

https://www.cbsnews.com/news/democratic-debate-transcript-clinton-sanders-omalley-in-new-hampshire/

No backdoors

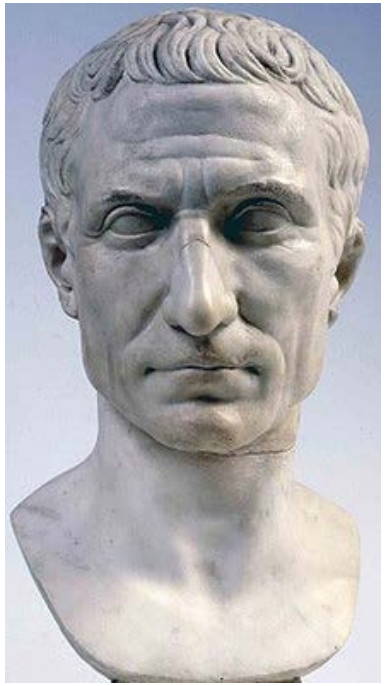
https://www.apple.com/customer-letter/

https://www.eff.org/deeplinks/2018/05/secure-data-act-would-stop-backdoors

Just the same debate with newer technology?
https://en.wikipedia.org/wiki/Clipper_chip

Modern Cryptography

Cryptography is very old…

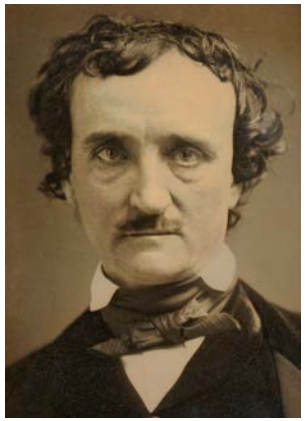


https://en.wikipedia.org/wiki/Timeline_of_cryptography

Pre-modern cryptography

Based mainly on "linguistic" ideas (see next lecture). Ad hoc deploy-then-patch or replace.

Edgar Allen Poe (an amateur cryptographer):



"human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

Is this true?

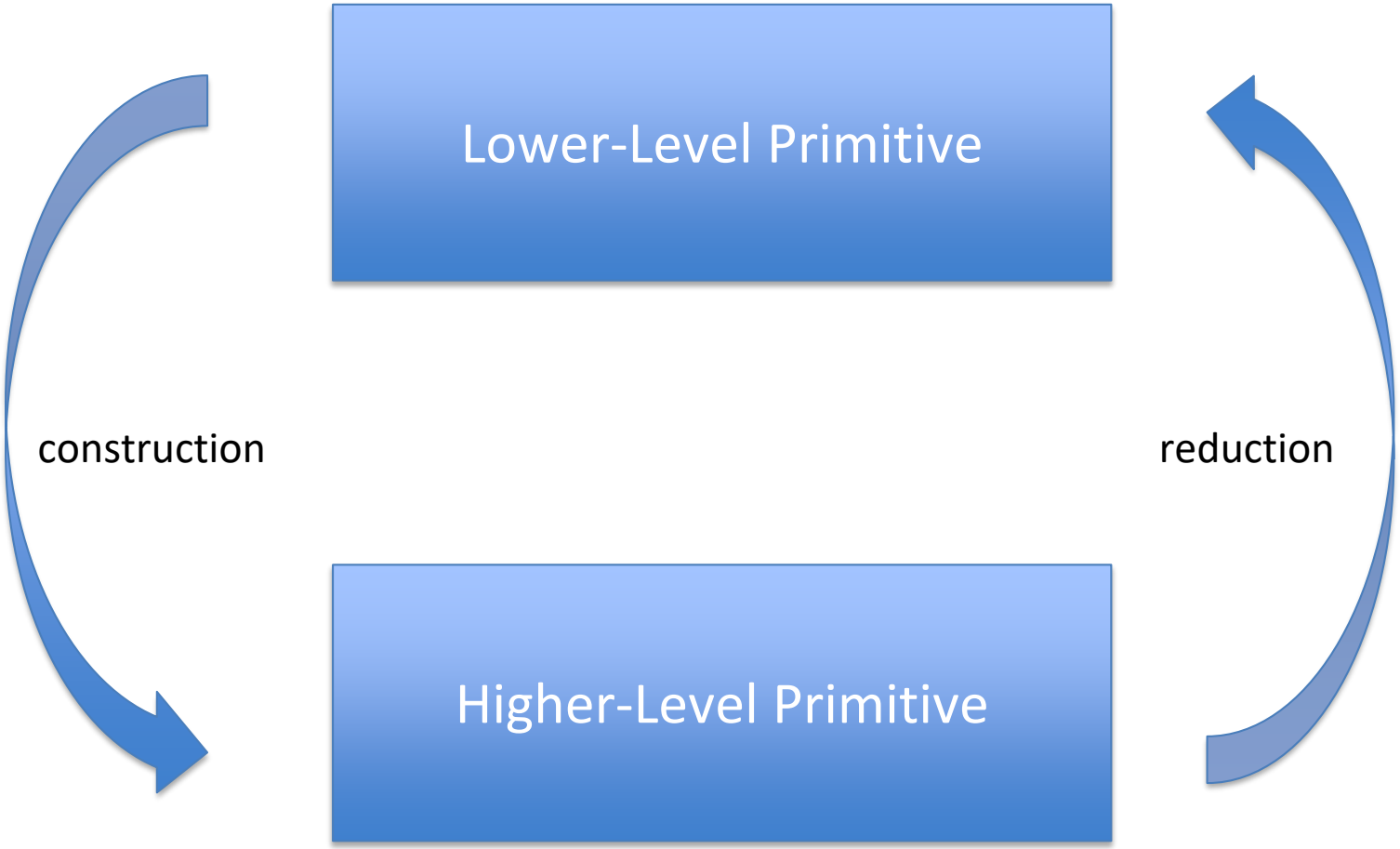
Modern Cryptography

- Deals with how to formalize and provably achieve desired properties.
- Security proofs for practical schemes are typically reductions… we will see why.
- Steps: Syntax definition, security definition, construction, reduction.

Secure Channels Revisited

Computational Hardness

Provable Security



Why is this the Right Approach?

- Ad-hoc design is subject to bug-then-patch cycle. Very dangerous and costly.
- "Testing is not possible in this setting, there are an infinite number of adversarial strategies.
- Doesn't make sense to try to design a secure encryption scheme without first asking what "secure" even means.

Why is this the Right Approach?

- Ad-hoc design is subject to bug-then-patch cycle. Very dangerous and costly.

- Doesn't make sense to try to design a secure encryption scheme without first asking what "secure" even means.