Instructor

• Instructor: Ryan Henry

- henry@indiana.edu
- http://homes.soic.indiana.edu/henry
- LH 330E

• Office hours: Fridays @ 10:30 - 11:30
  (or by appointment)

- Alas, Ryan is stuck in Washington DC today ;-(

Ryan Henry
Associate Instructor (AI)

- Instructor: Swami Ramesh
  - swamivr@indiana.edu
  - LH 330A

- Office hours: Fridays @ 13:30 - 14:30 (or by appointment)
Required textbook

Introduction to Modern Cryptography (2nd edition)

Jonathan Katz and Yehuda Lindell

Chapman & Hall/CRC Cryptography and Network Security Series

November 2014
The course website is the official source for:
- assignments,
- lecture slides,
- important announcements,
- supplemental material,
- etc.

Please check the course website frequently!

Also, Canvas: https://iu.instructure.com/courses/1600125
Lectures (presumably you've already figured this out)

Tuesdays and Thursdays

@ 13:00-14:15

in Ballantine Hall (BH) 322
Should I interrupt with questions during lectures?

A: Only if you want answers (in other words: YES, PLEASE DO!)
Grading and assessment

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Component</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>written assignments</td>
<td>8 assignments at 10% each</td>
</tr>
<tr>
<td>20%</td>
<td>in-class quizzes</td>
<td>4 quizzes at 5% each</td>
</tr>
<tr>
<td>10%</td>
<td>participation</td>
<td></td>
</tr>
<tr>
<td><strong>110%</strong></td>
<td>total</td>
<td>(Lowest assignments automatically be dropped)</td>
</tr>
<tr>
<td>Grade</td>
<td>Percentage</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>A+</td>
<td>97%</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>93%</td>
<td></td>
</tr>
<tr>
<td>A-</td>
<td>90%</td>
<td></td>
</tr>
<tr>
<td>B+</td>
<td>87%</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>83%</td>
<td></td>
</tr>
<tr>
<td>B-</td>
<td>80%</td>
<td></td>
</tr>
<tr>
<td>C+</td>
<td>77%</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>73%</td>
<td></td>
</tr>
<tr>
<td>C-</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td>D+</td>
<td>67%</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>63%</td>
<td></td>
</tr>
<tr>
<td>D-</td>
<td>60%</td>
<td></td>
</tr>
</tbody>
</table>
Homework

• One assignment assigned every second Tuesday*
  - Due before Tuesday lecture two weeks later

• Mostly written with some coding problems

  - **ASK FOR HELP EARLY!**
    - We will stop providing help starting 10 days after
      assignment is distributed!

  * with a few exceptions – see the calendar
Homework (sample timeline)

week N:
Sun Mon **Tue** Wed Thu **Fri** Sat

assignment distributed

week N+1:
Sun Mon Tue Wed Thu **Fri** Sat

office hours

last day for help!!

week N+2:
Sun Mon **Tue** Wed Thu Fri Sat

assignment due

(next assignment distributed)

Ryan Henry
Q: By a show of hands, who here knows \textsc{LaTeX}? 
- If your hand is not up, good news: you get to learn \textsc{LaTeX}!!

- Written portion of assignments must be typeset using \textsc{LaTeX}
- We will give you the \textsc{LaTeX} source for every assignment
- SoIC has a site license for Share\textsc{LaTeX}
When do we start talking about cartography?

A: Umm ... Never!
(this class is about cryptography!)
Huh!? No maps??

Well what in the @#$%★‽! is “cryptography”? 
What in the @#%★?! is Cryptography?
And, more generally, what is this course all about?
What is this class all about?

- Short answer: The theoretical foundations of modern cryptography
- Cryptography $\subseteq$ mathematics
  - No specific background is assumed, but "mathematical maturity" will help
  - We will cover the necessary math as we go!
What is this class all about?

FIELDS ARRANGED BY PURITY

MORE PURE

Sociology is just applied psychology.
Psychology is just applied biology.
Biology is just applied chemistry.
Which is just applied physics. It's nice to be on top.
Oh, hey, I didn't see you guys all the way over there.

On the other hand, physicists like to say that physics is to math as sex is to masturbation.

https://xkcd.com/435/
What is this class all about?

• Cartography, for starters
• But also:
  - particulars of deployed encryption schemes
  - specific “hard” problems
  - how to implement, use, or break specific cryptographic software

ADVICE: Don’t try to implement crypto yourself!
I will make you write lots of proofs

statement 1
statement 2
statement 3
⋮
statement n

I don't see why statement 2 follows from statement 1

NO MARKS FOR YOU!

Peggy (the prover)

Victor (the verifier)
I will make you write lots of proofs

Victor is very thorough yet very lazy
- will catch every mistake you make…but
- cannot be bothered to supply missing details

A perfectly valid complaint for Victor:

“I don’t understand!”
(or even, “This is poorly written”)

Victor (the verifier)
Ryan Henry
So it's all math and proofs? (See ya-I'm dropping!)

NO!! WAIT!

It's not just any math and proofs...it's super important, super cool math and proofs!
"Core" crypto

- Key establishment
- Secure communication

confidentiality/integrity
More advanced crypto

- Digital signatures

Bob signed this message
More advanced crypto

- Digital signatures
- Anonymous communications

Who am I talking to???
More advanced crypto

- Digital signatures
- Anonymous communications
- Oblivious computation

What am I computing for Bob??
More advanced crypto

- Digital signatures
- Anonymous communications
- Oblivious computation
- Anonymous digital currencies

Who just paid for that widget?
Cryptographic protocols

- End-to-end verifiable elections
  (as if anybody ever suspected an election was rigged!)
Cryptographic protocols

- End-to-end verifiable elections
  (as if anybody ever suspected an election was rigged!)

- Secure multiparty computation

\[ f(x_1, x_2, x_3, x_4, x_5) \]
Crypto magic

- Group signatures
- Commitment schemes
- Homomorphic encryption
- Oblivious transfer
- Deniable messaging
- Differential privacy
- Zero-knowledge proofs
- Multiparty computation
- Proofs of data possession
- Secret sharing
- Private information retrieval
- Verifiable outsourced computation

And a whole lot more...
Modern cryptography == Science

• Three steps in modern crypto

1. propose a precise threat model
2. propose a construction
3. prove that breaking construction is “equivalent” to solving an intractable problem (or impossible)
That's all for today, folks!

Thursday's lecture: Discrete probability 101