EECS 498/598: Encrypted Systems
Winter 2022
Lecture 1

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Introductions
    - Who are your course staff? Who are you all?
- Course policies and syllabus
- Motivation and course overview

About Me

- Only my second semester as a professor !
- Postdoc NYU, PhD Cornell (2020), undergrad at Indiana
- Worked as a cryptography engineer
- website: https://web.eecs.umich.edu/~paulgrub/
- he/him/his pronouns
- Research: applied cryptography, security, systems
  - Managing encrypted data, searchable encryption, authenticated encryption, attacks, provable security, etc…
- Outside of work:
  - Reading about history, pandemics, social issues, politics…
  - watching sitcoms (currently: Brooklyn 99)
  - playing Switch

About Our GSI

Chad Sharp
cmsharp@umich.edu

- PhD student in CSE
  - Advised by Chris Peikert
- Works on cryptography
  - Post-quantum crypto
  - fully-homomorphic encryption

About You!

Go around the room and introduce yourself to us:

- Name, preferred pronouns
- one thing you want to get out of this class, or a topic you’re excited about
- an interesting fact about yourself

Agenda for this lecture

- Introductions
  - Who are your course staff? Who are you all?
- Course policies and syllabus
- Motivation and course overview

Course Setup

- Hybrid between research seminar and lecture-based course
  - Tuesday and Thursday, 3:30-5:30pm FXB 1024
- Each lecture has two parts:
  - Student presentation + class discussion for the assigned papers
  - Brief overview (from Paul or Chad) of the topics of the next lecture
- Paul and Chad will have office hours throughout the week.
  - Paul’s OH time: TBD
  - Chad’s OH time: TBD
- If you need to email the course staff, include [EECS598W22] in the subject line

Student Deliverables

- Paper reviews
- Presentations
- Research project

Paper Reviews

- Each lecture will have a list of assigned papers
  - Papers *must* be read before their corresponding lecture
- Before each lecture, students will write and submit a 2-3 paragraph review of each assigned paper
  - “Before” = by noon on the day of the lecture
- Write reviews like research paper reviews for a conference:
  - explain main ideas of paper
  - outline core contributions
  - comments on quality, novelty, future directions, etc.
  - See https://people.inf.ethz.ch/troscoe/pubs/review-writing.pdf

Presentations

- Each student* will be responsible for writing and delivering a presentation about one of the sets of assigned papers
  - * Depending on numbers, teams of 2 may be allowed
  - Powerpoint/Keynote encouraged but not required
  - Students will have some choice in which papers they get (process TBD)
- Chad and I will prepare some concrete guidance
- Submit outline of presentation one class in advance
- The student* will also lead a discussion of the papers
  - During and/or after presentation
  - Prepare several questions in advance

Research Projects

- Throughout the semester, students will work in teams of at most 3 on a research project related to the course material
- Three sub-deliverables:
  - project proposal
  - mid-semester progress report
  - final submission
- Goal: produce a polished research artifact (writeup+code) that could appear at a top research conference

Grading

- Your final grade will have three components:
  - 50%: Research project
  - 25%: Paper reviews, in-class participation, and **attendance**
  - 25%: Presentation, leading discussions
- All research project submissions *must* be typeset in LaTeX.
- Paper reviews can be in any (digital) format

Course Materials

- Lecture notes: https://github.com/pag-crypto/EECS598-winter22
- (tentative) Lecture schedule: https://docs.google.com/document/d/1ydSlUtJQzSKNMh2o2o2tHIrO1ivoVvX9TMapHWxZ7UA/edit?usp=sharing
- Canvas: https://umich.instructure.com/courses/515831/
- Piazza: https://piazza.com/umich/winter2022/eecs498598
- No required textbook, but you'll likely find the optional textbooks useful

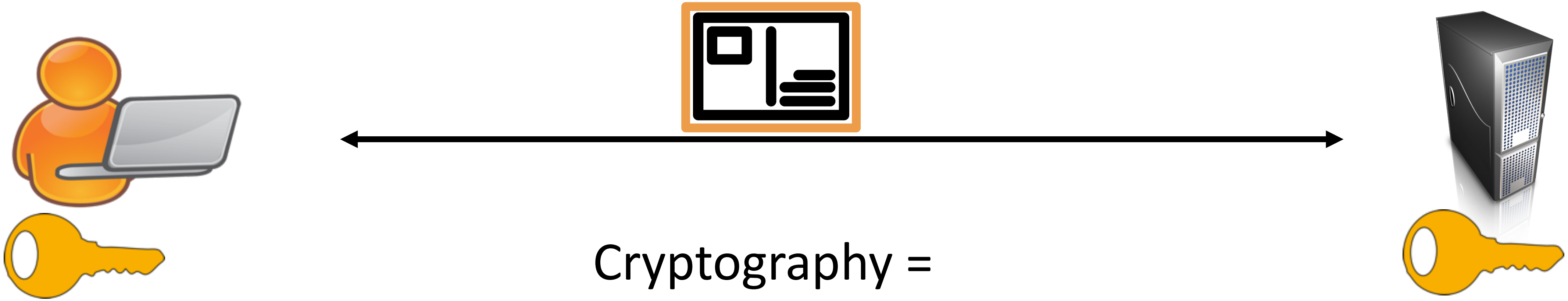
Agenda for this lecture

- Introductions
  - Who are your course staff? Who are you all?
- Course policies and syllabus
- Motivation and course overview

Motivating our topic of study

The title of this class is “Encrypted Systems”.

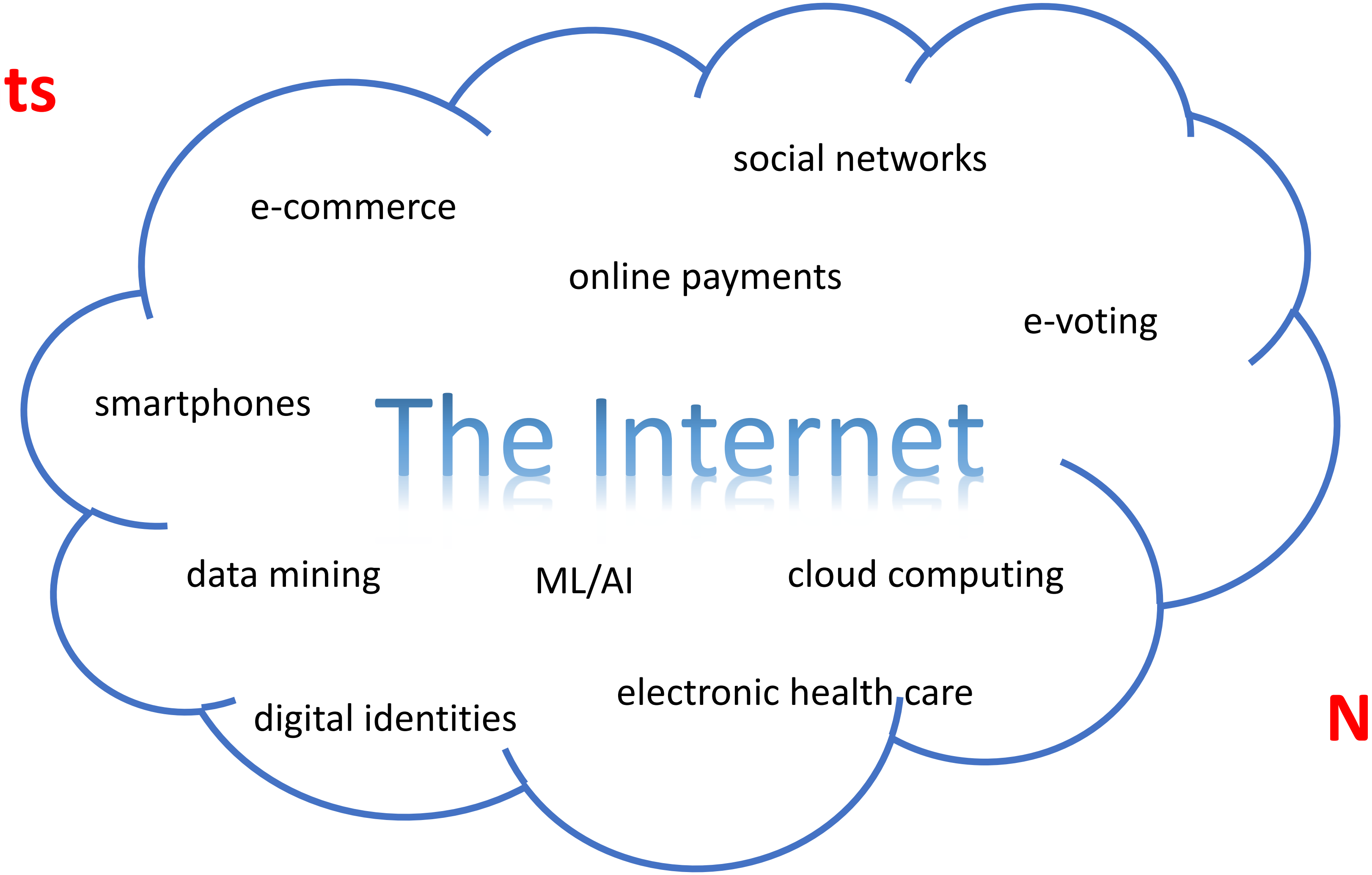
What is an encrypted system?



Cryptography =
hiding communication contents

Motivating our topic of study

New threats



social networks

e-commerce

online payments

e-voting

smartphones

The Internet

data mining

ML/AI

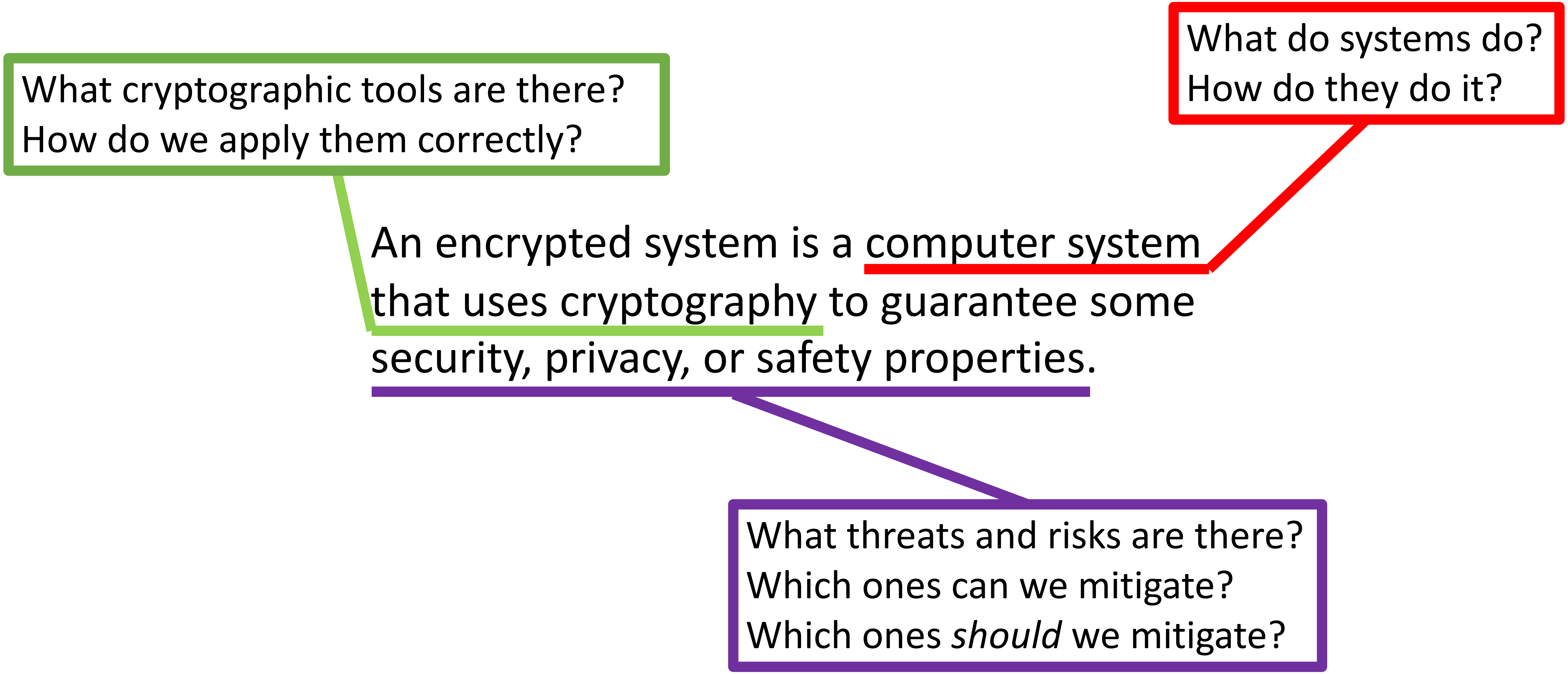
cloud computing

electronic health care

digital identities

New risks

Motivating our topic of study



What cryptographic tools are there?
How do we apply them correctly?

What do systems do?
How do they do it?

An encrypted system is a computer system that uses cryptography to guarantee some security, privacy, or safety properties.

What threats and risks are there?
Which ones can we mitigate?
Which ones *should* we mitigate?

Course Topics

- **Secure channels:**
  - E2E-encrypted messaging apps. Group messaging
- **Encrypted data management:**
  - Searchable encryption, oblivious RAM, private information retrieval.
  - Encrypted databases and key-value stores. leakage-abuse attacks
- **Distributed ledgers:**
  - Blockchain protocols, distributed consensus, verifiable random functions.
  - Cryptocurrencies and smart contracts.
- **Authentication, authorization, key management:**
  - Digital signatures and variants (blind, aggregate, multi-, group, ring, etc.). Public-key infrastructure, certificate transparency, anonymous credentials
- **Zero-knowledge proofs, verifiable computation, trusted hardware:**
  - classical and modern zero-knowledge proof systems, including zkSNARKs.
  - payment privacy in cryptocurrencies, zero-knowledge middleboxes
- **Privacy and applications**
  - Oblivious pseudorandom functions, private set intersection, mix networks. Anonymous communication, private measurement, online advertising, voting

Each unit has two parts:

1. study cryptographic tools
2. examine how encrypted systems are built with them

Expected Prerequisites

- Cryptography
  - definitions and proofs
  - PRFs, PRPs, AEAD, PKE, key exchange, signatures
- Security/Systems
  - threat models
  - core “abstractions” (e.g. access control)
  - software basics

Next week’s classes will be a very quick review of these prerequisites

Final thoughts

- This is a brand-new class! Exciting, but need to be flexible.
- Feedback on what is (or isn’t) working is always appreciated
- Policies, setup or course content may be tweaked