Cryptography

Course Information

Arkady Yerukhimovich

August 26, 2024

Course Information

- Course Title: CS 4331 / 6331 - Cryptography
- Professor: Arkady Yerukhimovich
- Class Time: 12:45PM - 2:00PM on Mondays and Wednesdays
- Class location: Corcoran Hall 207
- Webpage: `https://gw-cs4331.github.io/`

Outline

1. What this course is about

2. Accessing Course Material

3. Expectations and Grading

4. Important Policies

What is Cryptography?

According to Wikipedia

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.

Why Study Cryptography?

- Cryptography is amazing
  - Can do things that seem impossible

Why Study Cryptography?

- Cryptography is amazing
  - Can do things that seem impossible
- Cryptography is useful
  - Widespread applications

Why Study Cryptography?

- Cryptography is amazing
  - Can do things that seem impossible
- Cryptography is useful
  - Widespread applications
- Cryptography is beautiful
  - Deep theory
  - Definitions for core concepts
  - Everything viewed through an adversarial lens

Why Study Cryptography?

- Cryptography is amazing
  - Can do things that seem impossible
- Cryptography is useful
  - Widespread applications
- Cryptography is beautiful
  - Deep theory
  - Definitions for core concepts
  - Everything viewed through an adversarial lens

Announcement

Crypto does not mean cryptocurrency

The Value of Cryptography

- Cryptanalysis (Bletchley Park)
  - shortened World War II by 2 years
  - saved millions of lives

The Value of Cryptography

- Cryptanalysis (Bletchley Park)
    - shortened World War II by 2 years
    - saved millions of lives
- Crypto is extensively used in
    - e-commerce
    - banking
    - data security and privacy
    - AES alone has contributed $250B to US economy

The Value of Cryptography

- Cryptanalysis (Bletchley Park)
  - shortened World War II by 2 years
  - saved millions of lives
- Crypto is extensively used in
  - e-commerce
  - banking
  - data security and privacy
  - AES alone has contributed $250B to US economy
- Definition of fundamental concepts
  - privacy
  - integrity
  - (machine) knowledge

What You Will Get Out of This Course

You will be able to:

- Understand key concepts of modern crypto
- Understand security guarantees provided by standard crypto primitives why these are needed by applications
- Know the main building blocks of modern crypto

What You Will Get Out of This Course

You will be able to:

- Understand key concepts of modern crypto
- Understand security guarantees provided by standard crypto primitives why these are needed by applications
- Know the main building blocks of modern crypto

You will **NOT** be able to:

- Design your own crypto schemes
- Implement crypto for real-world use

What You Will Get Out of This Course

You will be able to:

- Understand key concepts of modern crypto
- Understand security guarantees provided by standard crypto primitives why these are needed by applications
- Know the main building blocks of modern crypto

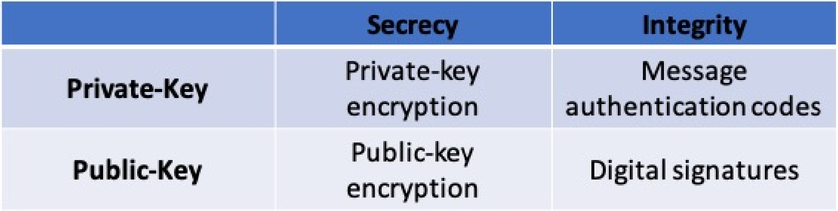
You will **NOT** be able to:

- Design your own crypto schemes
- Implement crypto for real-world use

Summary Course Goals

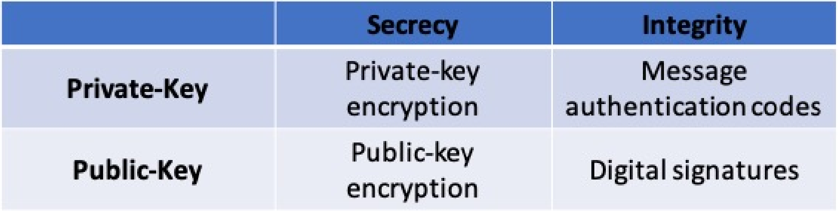
This course will not make you a cryptographer! But, it will teach you when you need to find one, and how to speak to them when you do.

What We Will Cover



	Secrecy	Integrity
Private-Key	Private-key encryption	Message authentication codes
Public-Key	Public-key encryption	Digital signatures

What We Will Cover

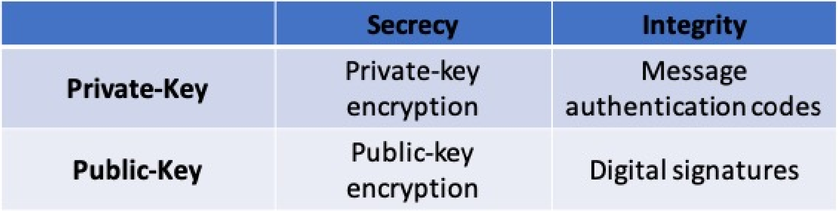


	Secrecy	Integrity
Private-Key	Private-key encryption	Message authentication codes
Public-Key	Public-key encryption	Digital signatures

Building Blocks:

- Pseudorandom Generators
- Pseudorandom Functions
- Hash Functions
- Number Theory

What We Will Cover



	Secrecy	Integrity
Private-Key	Private-key encryption	Message authentication codes
Public-Key	Public-key encryption	Digital signatures

Building Blocks:

- Pseudorandom Generators
- Pseudorandom Functions
- Hash Functions
- Number Theory

Key Concepts:

- Security definitions
- Adversarial mindset
- Proofs by reduction

Prerequisites

The main prerequisite for this class is *mathematical maturity*

- Be able to follow mathematical definitions, theorems, proofs
- Basic logic, probability (most things will be covered in class, but some background is helpful)

Recommended prerequisite courses:

- Undergrad: CS 2312 (Discrete II), CS 3313 (Foundations)
- Grad: CS 6212 (Algorithms)

Textbook

Textbook: "Introduction to Modern Cryptography, 2nd edition," by Katz and Lindell

- This book is strongly recommended
- eBook available for free from GW Library (https://wrlc-gwu.primo.exlibrisgroup.com/permalink/01WRLC_GWA/1piqqnm/alma99185917007604107)
- Make sure you get the 2nd edition
- Use of Chinese translation of textbook is not recommended

How to Contact Me

- The best way to contact me is
  - Via Piazza (details below and on website)
  - by email: arkady@gwu.edu
- Include CSCI 4331 or CSCI 6331 in the subject line

Outline

1. What this course is about
2. Accessing Course Material
3. Expectations and Grading
4. Important Policies

Lectures

Accessing Lectures:

- In person
- Zoom: Access through Blackboard→ Tools→ Zoom Meetings

Important:

- Zoom option is only for students who have a legitimate reason not to attend class in person.
- Main purpose for Zoom is to provide recordings for review

Office Hours

Office hours will be held twice a week. Times are TBD.

Office hours will be held in 4th floor common area

Discussions and Announcements

In Class:

- In class questions and discussion are an important part of this class
- They also count towards your participation grade
- Ask lots of questions!

Discussions and Announcements

In Class:

- In class questions and discussion are an important part of this class
- They also count towards your participation grade
- Ask lots of questions!

Piazza:

- Piazza is for questions and general discussion about lectures, homework, and anything you are curious about but didn't ask in class.
- Student are encouraged to answer each others' questions
- Homework assignments will be announced in Piazza
- Piazza link on course website

Discussions and Announcements

In Class:

- In class questions and discussion are an important part of this class
- They also count towards your participation grade
- Ask lots of questions!

Piazza:

- Piazza is for questions and general discussion about lectures, homework, and anything you are curious about but didn't ask in class.
- Student are encouraged to answer each others' questions
- Homework assignments will be announced in Piazza
- Piazza link on course website

Blackboard:

- Blackboard will be used for lecture videos and recordings only

Discussions and Announcements

In Class:

- In class questions and discussion are an important part of this class
- They also count towards your participation grade
- Ask lots of questions!

Piazza:

- Piazza is for questions and general discussion about lectures, homework, and anything you are curious about but didn't ask in class.
- Student are encouraged to answer each others' questions
- Homework assignments will be announced in Piazza
- Piazza link on course website

Blackboard:

- Blackboard will be used for lecture videos and recordings only

Gradescope:

- Gradescope will be used to collect and grade homework

Outline

1. What this course is about
2. Accessing Course Material
3. Expectations and Grading
4. Important Policies

Grading

Grade Breakdown

- Exam(s) - 40% (20% each)
- Research Project - 20%
- Homework - 30%
- Participation - 10%

Exam

There will be 2 exams in this class.

- Midterm – October 16th, in class
- Final – During finals week

Exam Policies:

- You will be allowed to bring one page (back-and-front) of notes.
- You may not work with others on the exam.
- You may not use outside resources on the exam.

Research Project

Project Description:

- Students will prepare a 20-minute recorded lecture on a crypto topic of their choice that is not covered in class, and share it online with the class.
- Students will post discussion questions for each others' lectures in Slack.
- We will have a "workshop" for students to answer questions about their projects.

Research Project

Project Description:

- Students will prepare a 20-minute recorded lecture on a crypto topic of their choice that is not covered in class, and share it online with the class.
- Students will post discussion questions for each others' lectures in Slack.
- We will have a "workshop" for students to answer questions about their projects.

Project Details:

- You may work in groups of up to 3 people
- Videos must be posted by end of day on November 22nd (this is the Friday before Thanksgiving)
- Final project workshop on December 4

Research Project

Project Description:

- Students will prepare a 20-minute recorded lecture on a crypto topic of their choice that is not covered in class, and share it online with the class.
- Students will post discussion questions for each others' lectures in Slack.
- We will have a "workshop" for students to answer questions about their projects.

Project Details:

- You may work in groups of up to 3 people
- Videos must be posted by end of day on November 22nd (this is the Friday before Thanksgiving)
- Final project workshop on December 4

Important

Start the project early, don't ruin your holiday.

Homework – “Specification Grading”

Each problem will be graded according to following rubric:

- E - Excellent: Demonstrates clear understanding
- M - Meets Expectations: Evidence of understanding but missing some details
- R - Needs Revision: Shows partial understanding but gaps remain
- N - Not Satisfactory: Fails to demonstrate understanding

Homework – “Specification Grading”

Each problem will be graded according to following rubric:

- E - Excellent: Demonstrates clear understanding
- M - Meets Expectations: Evidence of understanding but missing some details
- R - Needs Revision: Shows partial understanding but gaps remain
- N - Not Satisfactory: Fails to demonstrate understanding

Due Dates and Resubmissions:

- You will get 2 tries to answer each problem:
- To get an E, you must submit by due date
- If you get an R or N by due date, you may revise and resubmit to get up to M – only 1 resubmission per problem
- Resubmissions must happen at most 1 week after original deadline

Homework – "Specification Grading"

Each problem will be graded according to following rubric:

- E - Excellent: Demonstrates clear understanding
- M - Meets Expectations: Evidence of understanding but missing some details
- R - Needs Revision: Shows partial understanding but gaps remain
- N - Not Satisfactory: Fails to demonstrate understanding

Due Dates and Resubmissions:

- You will get 2 tries to answer each problem:
- To get an E, you must submit by due date
- If you get an R or N by due date, you may revise and resubmit to get up to M – only 1 resubmission per problem
- Resubmissions must happen at most 1 week after original deadline

Important

You must submit something by due date to be allowed to resubmit

Homework Details

Homework Details:

- Homework will come out (approximately) every week
- Homework is due (on Blackboard) by 12:45PM, on the due date (right before class).
- NO LATE HOMEWORK ACCEPTED – for initial submission
- Resubmissions can happen up to 1 week after deadline

Homework Details

Homework Details:

- Homework will come out (approximately) every week
- Homework is due (on Blackboard) by 12:45PM, on the due date (right before class).
- NO LATE HOMEWORK ACCEPTED – for initial submission
- Resubmissions can happen up to 1 week after deadline

Homework Policies:

- You may discuss general concepts with others, but do your homework yourself.
- You MUST write up your own answers. Do not copy from others.
  - Make sure you understand your answer
  - I may ask you to explain
- You MAY NOT use online resources: e.g. other course solutions, ChatGPT, chegg.com, etc.

Quizzes

- We will have quizzes during some of the lectures
- Quizzes are not graded, but will be part of class participation
- Quizzes give me a way to quickly assess how well you understand the material

Class Participation

Class participation score will consist of the following:

- Involvement during lecture and on Piazza
- Participation in quizzes
- Questions for classmates' projects

If you are sick or cannot participate a given week, please let me know.

Outline

1. What this course is about
2. Accessing Course Material
3. Expectations and Grading
4. Important Policies

Sharing Online Course Content

- Recordings of lectures MUST NOT be shared outside of class. These are only for students registered in the class.
- Lecture recordings made by other students MUST NOT be shared outside of class.
- Slides made by the professor may be downloaded and shared.

In Class Behavior

- Treat others with respect. We have students coming from diverse backgrounds, and I want everyone to feel welcome.
- Encourage others by asking questions and helping each other
- Do not disparage anybody

Important

Everyone will enjoy the class more if we treat each other with respect.

Enjoy the Class