Topic 0
Welcome to CO 487/687 Applied Cryptography!

Douglas Stebila

CO 487/687: Applied Cryptography
Fall 2024

Today's lecture

1. Uses of cryptography
2. Overview of cryptography
3. Administrative info

You used cryptography in the last 10 minutes

(Yes, you!)

You locked your car

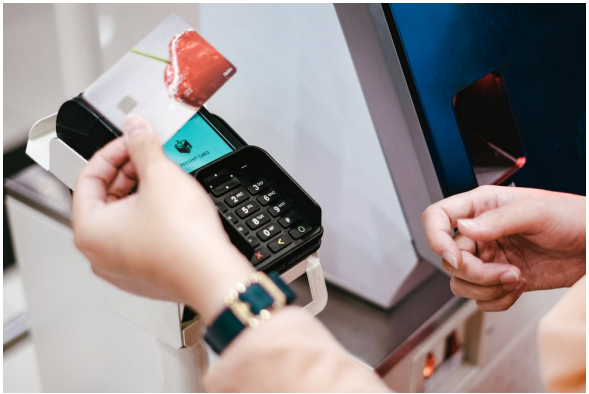
- cryptographically protected protocol between remote and car to ensure only authorized people can lock/unlock the car
  - symmetric key cryptography
  - message authentication code
  - challenge-response protocol

https://commons.wikimedia.org/wiki/File:Remote_central_locking.jpg

You listened to music over Bluetooth

- encrypted connection to protect privacy
- authentication to prevent someone from hijacking your headphones

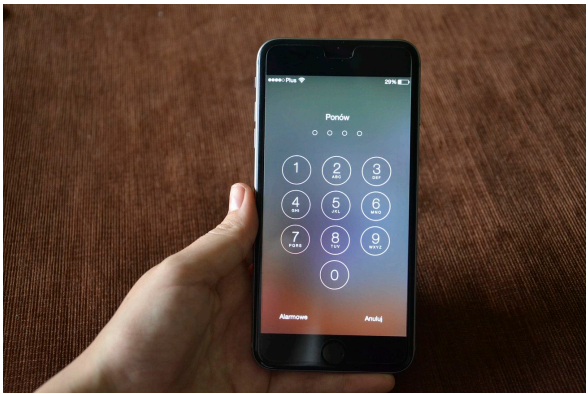
https://www.pexels.com/photo/man-wearing-white-headphones-listening-to-music-901236/



You bought a coffee at Tim Horton's and paid via tap

- encryption of credit card number and other data between card & bank and bank & merchant

https://thenounproject.com/photo/close-up-of-a-hand-with-gift-card-at-payment-machine-4dyaAb/



You unlocked your phone using a PIN

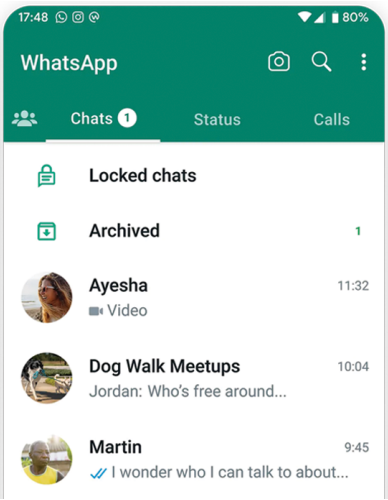
- hash function used to check your entered PIN against the stored PIN hash

https://www.rawpixel.com/image/5920814

You browsed some posts Instagram

- server-to-client authentication using public key certificates with digital signatures
- encrypted connection to protect privacy
- integrity protection to prevent tampering of transmitted data

https://www.pickpik.com/instagram-app-login-splash-screen-logo-iphone-79388



You sent a chat message on WhatsApp

- end-to-end encryption between users
- "ratcheted" key agreement to derive new encryption keys for each message
- authenticated encryption to provide confidentiality and integrity
- uses the "Signal protocol"

https://www.whatsapp.com/privacy

You installed a software update from the app store

- digitally signed by developer and app store to prevent malware from being installed

https://www.macrumors.com/2018/03/20/apple-tightening-rules-on-whats-new-text-app-store/

You were connected over wi-fi

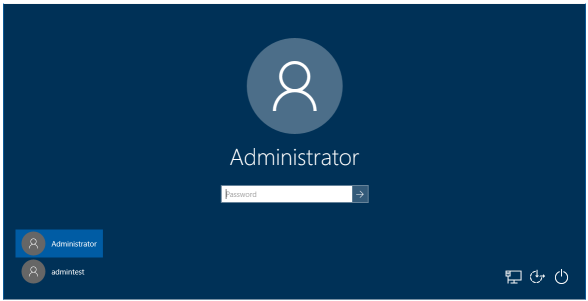
- encrypted authentication protocol to protect your wi-fi login password
- encryption between phone and base station to protect privacy
- integrity protection to prevent tampering

https://www.rawpixel.com/image/400416/wifi-connection

You were connected over mobile data

- key installed on your SIM card
- authentication between phone and base station to control access
- encryption between phone and base station to protect privacy
- integrity protection to prevent tampering

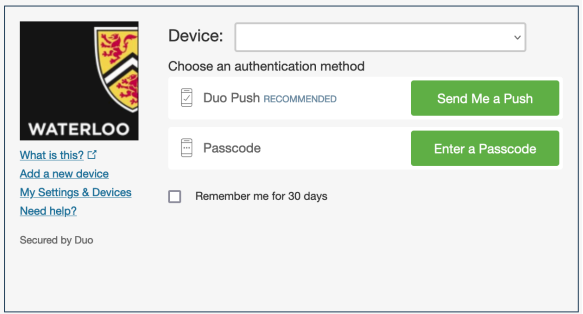
https://www.wallpaperflare.com/monte-brione-cell-towers-radio-masts-garda-mountain-italy-wallpaper-gbovl



You logged in to your computer using your password

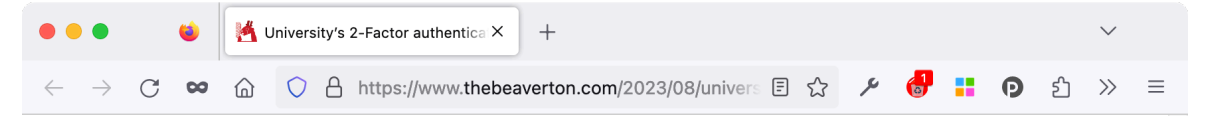
- hash function used to check entered password against stored password hash
- key derivation function used to derive encryption key to unlock hard drive disk encryption

Source: Technet



You logged in to UW LEARN

- Duo computed a one-time password using a hash function and pre-shared key
- (Actually this changed in 2024, but we'll study the previous version.)



EDUCATION

University's 2-Factor authentication stymies hacker trying to do other people's homework

1 WEEK AGO *by* DEREK SCHULTZ [e]

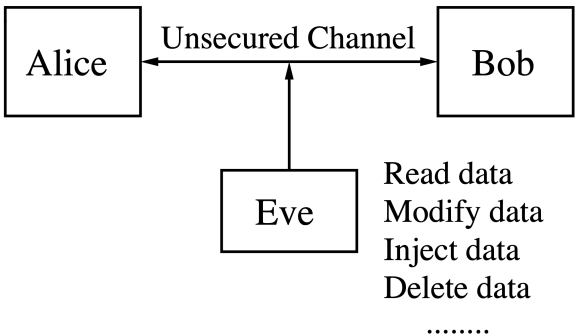
CALEDON, ON — A local hacker's nefarious plot to maliciously log into a first-year student's account and do their algebra was frustrated this week, thanks to the foresight of administrators who require 2-factor authentication on literally everything.

https://www.thebeaverton.com/2023/08/universitys-2-factor-authentication-stymies-hacker-trying-to-do-other-peoples-homework/

Overview of cryptography

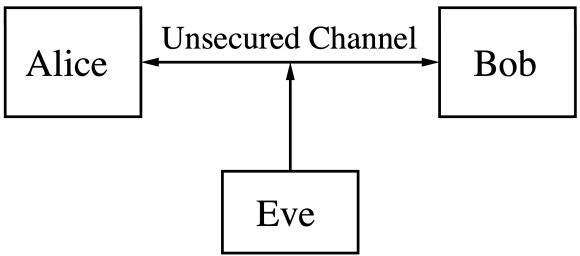
What is Cryptography?

Cryptography is about securing communications in the presence of malicious adversaries.



Fundamental Goals of Cryptography

- Confidentiality: Keeping data secret from all but those authorized to see it.
- Integrity: Ensuring data has not been altered by unauthorized means.
- Authentication: Corroborating the source of data or identity of an entity.
- Non-repudiation: Preventing an entity from denying previous commitments or actions.



Fundamental Goals of Cryptography

- Confidentiality: Keeping data secret from all but those authorized to see it.
- Integrity: Ensuring data has not been altered by unauthorized means.
- Authentication: Corroborating the source of data or identity of an entity.
- Non-repudiation: Preventing an entity from denying previous commitments or actions.

States of information

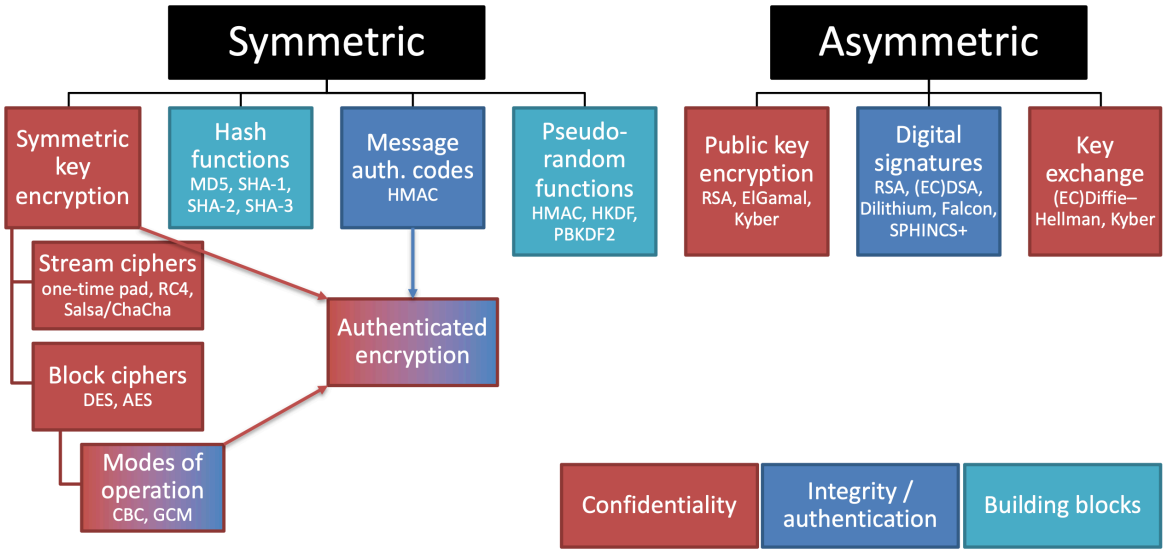
- Data at rest
- Data at transit
- Data while processing

Main parts of the course

1–3:
Cryptographic
Building Blocks

4:
Applications

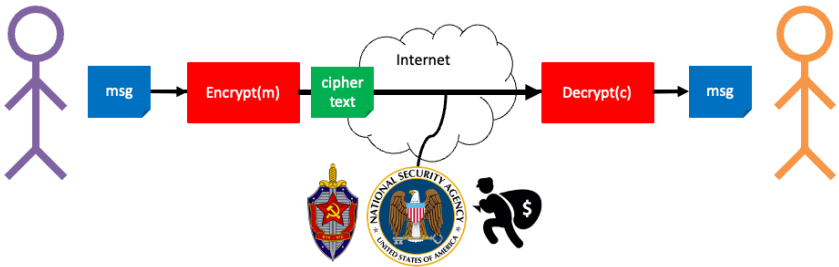
Sections 1–3: Cryptographic Building Blocks



Section 4: Applications

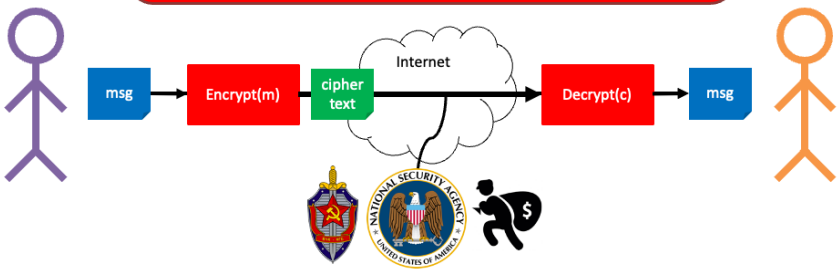
Key management	Secure channels	Other applications
• PKI • X.509 certificates	• TLS • SSH • Signal	• Bitcoin • Zero knowledge

Encryption using a secret function

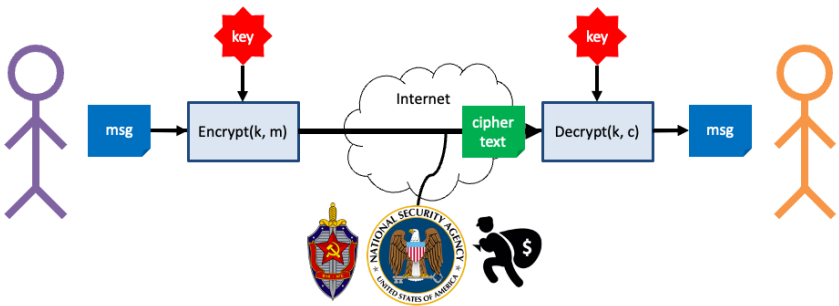


Encryption using a secret function

Relying on a secret function violates Kerckhoff's principle of avoiding security by obscurity



Symmetric encryption



Man-in-the-middle (MITM) attack on symmetric encryption:
What if an active adversary modifies transmissions?

Authenticated encryption

Authenticated encryption

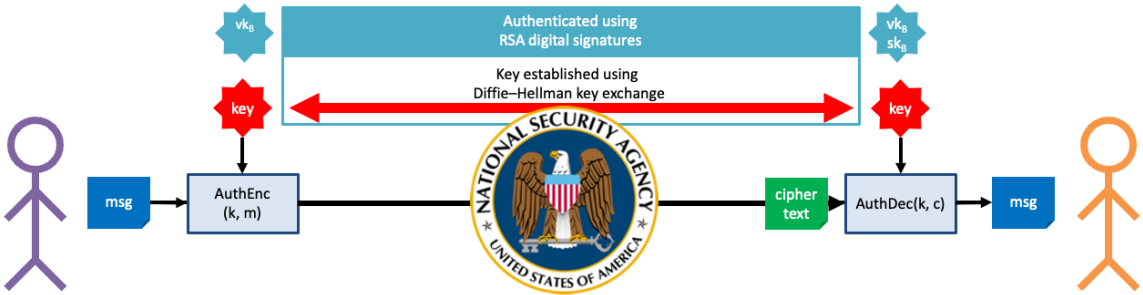
Key exchange + authenticated encryption

Man-in-the-middle attack on key exchange:

What if an active adversary impersonates Alice and Bob to each other?

Building a secure channel: attempt 5

Authenticated key exchange + authenticated encryption



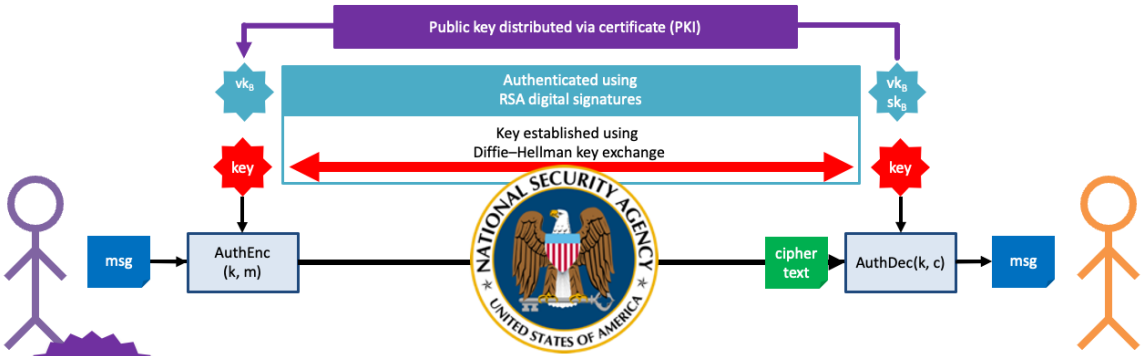
Building a secure channel: attempt 5

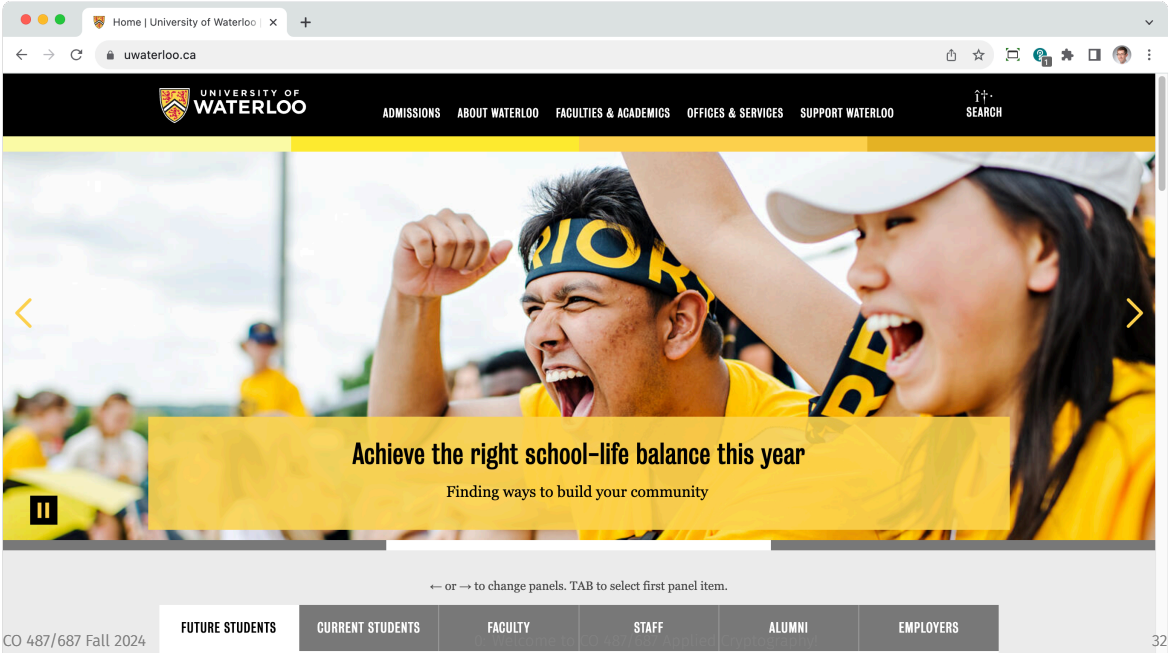
Man-in-the-middle attack on authenticated key exchange

What if an active adversary replaces Alice's public key?

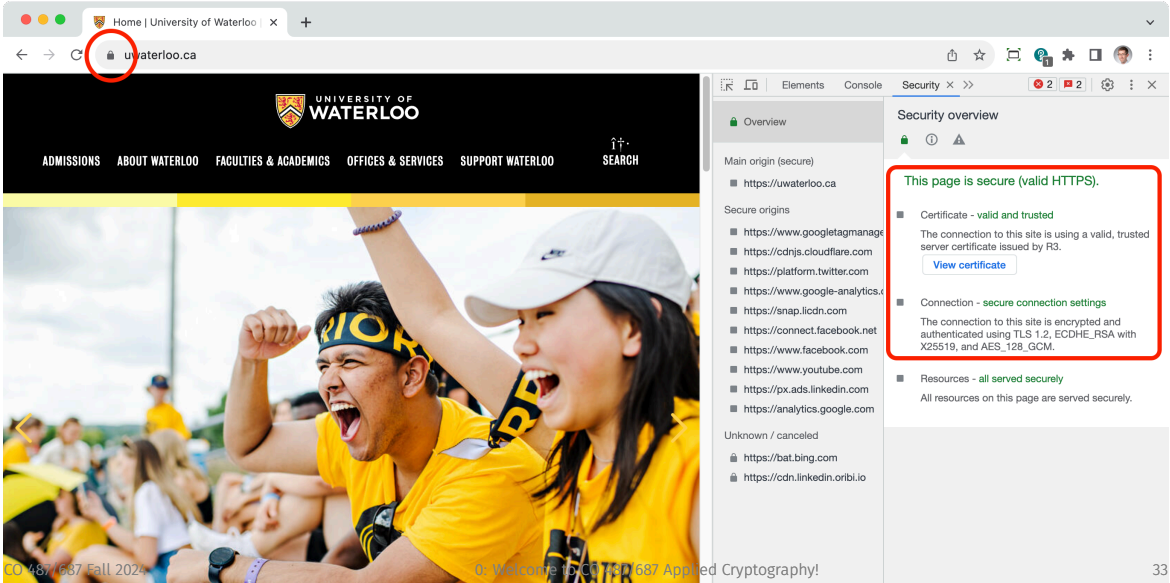
Building a secure channel: attempt 6

Certified authenticated key exchange + authenticated encryption




Home | University of Waterloo
uwaterloo.ca
UNIVERSITY OF WATERLOO
ADMISSIONS
ABOUT WATERLOO
FACULTIES & ACADEMICS
OFFICES & SERVICES
SUPPORT WATERLOO
SEARCH
Achieve the right school-life balance this year
Finding ways to build your community
← or → to change panels. TAB to select first panel item.
FUTURE STUDENTS
CURRENT STUDENTS
FACULTY
STAFF
ALUMNI
EMPLOYERS

Transport Layer Security (TLS) protocol



Cryptography is multi-disciplinary

- Mathematics: Design and analysis of problems that are believed to be hard (e.g. integer factorization)
- Computer science: Design and analysis of cryptographic protocols whose security relies on the hardness of the underlying mathematical problem
- Engineering: Efficient and secure implementation of the protocols in hardware and software

Cryptography $\neq$ Security

- Cryptography provides some mathematical tools that can assist with the provision of cybersecurity services. It is a small, albeit an essential, part of a complete security solution.
- Security is a chain
  - Weak links become targets; one flaw is all it takes.
  - Cryptography is usually not the weakest link. However, when the crypto fails the damage can be catastrophic.

Cryptography in Context

Information security a.k.a. cybersecurity is comprised of the concepts, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.

Cybersecurity includes many things:

Computer security

- Security models and policies
- Secure operating systems
- Virus protection
- Auditing mechanisms
- Risk analysis
- Risk management

Network security

- Internet protocols and their security
- Viruses and worms
- Denial-of-service (DoS) attacks
- Firewalls
- Intrusion detection systems
- Wireless communications

Software security

- Detecting and preventing buffer overflows
- Programming languages and compilers
- Specifying and enforcing security policies
- Digital rights management
- Code obfuscation
- Software tamper resistance
- Trusted computing

Administrative information

Teaching team

Instructor: Prof. Douglas Stebila

Teaching assistants:

- Santiago Estupinan
- Youcef Mokrani
- Josephine Reynes
- Fernanda Rivera Omana
- Camryn Steckel
- Nic Swanson

About the Course

- Coverage will favour breadth at the expense of depth
  - For depth, try the recommended and optional readings
  - See also: CO 485 (Mathematics of Public-Key Crypto)
  - See also: CS 458 (Computer Security and Privacy)
- This course is not a traditional textbook course!
  - Attending the lectures is strongly recommended.
  - There are no good sources of “practice questions”
  - Your job: Identify and understand the important (technical and non-technical) concepts presented in class
- Optional textbooks:
  - Paar, Pelzl, Güneysu. Understanding Cryptography, 2nd edition. Free access via UW’s library subscription. See links on LEARN or course outline.
  - Stinson. Cryptography — Theory and Practice, 4th edition.
- Recommended readings are posted on LEARN

4+8+7 things to remember from CO 487

CO 487/687

Dr. Douglas Stebila

UNIVERSITY OF WATERLOO

Fall 2024

Related courses

Other courses at Waterloo that deal with security:

- Combinatorics and Optimization:
  - CO 481: Introduction to quantum information processing
  - CO 485: Public-key cryptography
- Computer science:
  - CS 436: Networks and distributed computer systems (non-majors)
  - CS 453: Software and Systems Security
  - CS 456: Computer Networks (CS majors)
  - CS 459: Privacy, Cryptography, Network and Data Security
- Electrical and computer engineering:
  - ECE 254: Operating systems and systems programming
  - ECE 409: Cryptography and system security
  - ECE 419: Communication system security
  - ECE 458: Computer security

Course websites

- LEARN
  - Course outline
  - Slides, assignments & solutions, handouts, sample exams.
  - Recommended and optional readings
- Piazza: for questions about course material.
- Crowdmark: for assignment submission.

Assessment

- Assignments: submitted via Crowdmark.
  - due: Sep 26, Oct 10, Oct 31, Nov 14, Nov 28
- Final: during final exam period, Registrar-scheduled

Grading scheme (CO 487)

- 50% assignments
- 50% final
- 2% bonus Piazza contributions

Remark requests: within 7 days. Make a private post on Piazza.

Grading scheme (CO 687)

Whichever of the following two formulas is higher (automatically calculated):

- 40% assignments
- 40% final
- 20% project
- 2% bonus Piazza contributions

Project: Proposal due Oct. 31, final report due Dec. 12. See details on LEARN.

Late/missed assignments

- Must submit self-declared short-term absence on Quest or Verification of Illness Form (VIF) that covers the due date of the assignment
- Grants you choice of:
  - Extend deadline for the assignment by 72 hours
  - Have entire weight of the assignment shifted to the final exam
- Must submit additional CO 487 form online telling me which of these you choose

Academic integrity

Assignments:

- Can collaborate with other students in the course
- You must write up your own solutions and acknowledge any sources you use or people you work with.
- Can ask general questions on Piazza but avoid discussing specific solutions in public posts.
- Cannot ask questions on other online bulletin boards, chat groups, or consult solutions from past offerings of the course.
- Some assignment questions may be flagged as “no collaboration” for which you are expected to work independently as in exam settings.

See course outline for additional policies and details.

Office hours and Piazza

- Office hours: Schedule to be confirmed, see LEARN.
  - Instructor office hours: Mondays 4–5pm
  - TA office hours: to be announced; more scheduled during assignment due date weeks
- Piazza: monitored periodically through the day; don't expect instant instructor responses.
  - Up to 2% will be available as a bonus for positive contributions on Piazza, such as asking good questions or helping answer questions.
  - Use Piazza's "endorsement" mechanism – "good question", "helpful", etc. – to flag good contributions.

Covid guidelines

- Recommend you stay up-to-date with vaccinations; booster shots available around town and on campus in a few weeks.
- Respect those who choose to wear a mask and consider wearing a mask in situations where you'll be in close contact with others.
- If you are sick, stay away.
  - Lecture slides and videos from 2020 on LEARN.
  - Use self-declared short-term absence or VIF.

Should You Take This Course?

CO 487 is an elective course for everyone.

So, it is intended to be interesting, fun, relevant, and not-too-difficult*.

- * What does “not-too-difficult” mean?
  - Breadth, not depth.
  - No heavy algebra, no deep proofs.
  - But lots of different concepts
    - Understand the relationship between different concepts
    - Understand their different use cases
    - Realize what’s more important and what’s less important
    - Be creative in the techniques and tools you use
    - Some problems will be open-ended

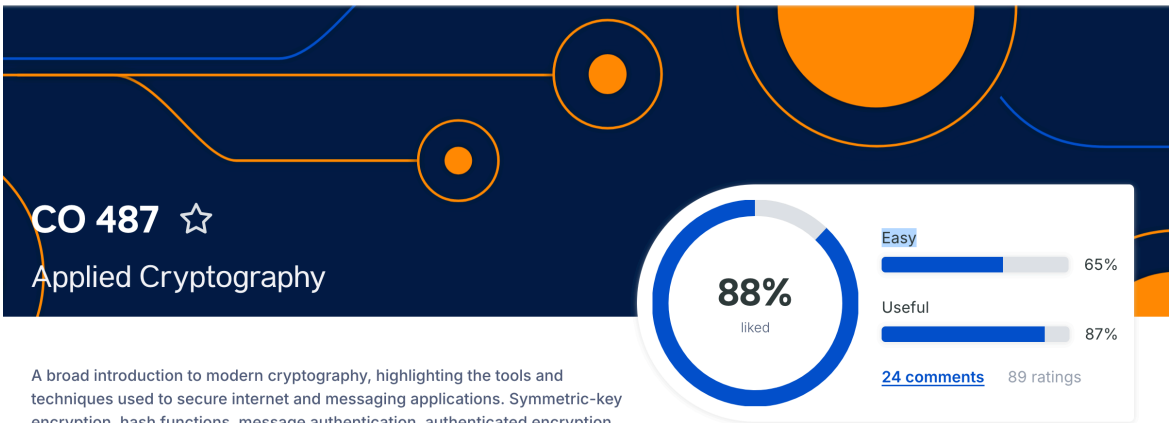
Should You Take This Course?

Assumed knowledge:

- Some elementary number theory (e.g. MATH 135)
- A bit of probability (e.g. STAT 230)
- A bit of programming (e.g. CS 136)
  - Some assignment problems will require that you be able to write computer programs, in Python or a language of your choice.

Not used in this course:

- Calculus
- Other areas of C&O:
  - combinatorics / graph theory (MATH 239)
  - optimization (CO 250)
  - quantum computing (CO 481)
  - coding theory (CO 331)



A broad introduction to modern cryptography, highlighting the tools and techniques used to secure internet and messaging applications. Symmetric-key encryption, hash functions, message authentication, authenticated encryption, public-key encryption and digital signatures, key establishment, key management. [Offered: F,W]

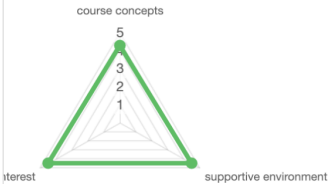
Course Stats

learning outcomes received an average score of **4.3**

graded work received an average score of **4.1**

outcomes assessed received an average score of **4.3**

Professor Stats



course concepts received an average score of **4.3**

supportive environment received an average score of **4.5**

interest received an average score of **4.5**

Should You Take This Course?

Does not seem to be a CO course, would not recommend if you like taking theory courses

*— Combinatorics & Optimization student 7 months ago, taught by **Douglas Stebila***

Easy

Useful

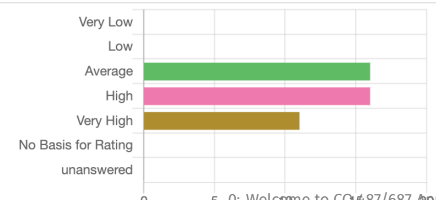
Liked

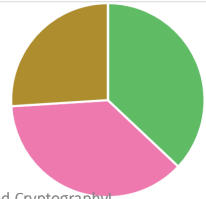
suggested changes:

Don't tell people this class is 'easy' because the assignments are anything but haha

workload

The course workload demands were...





Why I like cryptography

- At the intersection between math and computer science
- Important real world problems
- Always evolving

In a single day at a cryptography conference, I can hear talks on:

- Algebraic geometry and elliptic curve isogenies
- Hacking a Tesla via its car remote and driving away with it
- Facebook's plans to prevent abuse on encrypted chats
- Whether Apple and Google's COVID exposure notification apps are sufficiently private
- Updates on encryption policy from US Congressional interns