Welcome to CMSC/MATH/ENEE 456: Cryptography

August 31, 2020

Today: Admin, Intro to Crypto, Shift Cipher

August 31, 2020

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Admin

August 31, 2020

Necessary Administrative

Course Webpage:
https://www.cs.umd.edu/users/gasarch/COURSES/456/F20/index.html

Necessary Administrative

Course Webpage:
https://www.cs.umd.edu/users/gasarch/COURSES/456/F20/index.html

Course Zoom Site:
https://umd.zoom.us/my/gasarch

Necessary administrative stuff

- Gradescope: you will **post HW** there.
- Gradescope: we will **grade HW** there.
- Regrade Requests due within a week of the HW being graded.
- Grades on Elms.
- Piazza is great for asking questions.

TAs

- Yuang Shen (he goes by Eric)
- Zan Xu
- Josh Twitty
- Their office hours and mine (on Zoom) are on policy part of website.
- Their emails and mine are on policy part of website.

What You Need For This Class

- Discrete math, probability, modular arithmetic, algorithms, misc math.
- Mathematical maturity.
- Ability to write **short** to middle-sized programs. (This is not a course like **Operating systems** where the project is a large part of the course intellectually and for the grade.)

How to Get the Most Out of This Class

1. Read notes and slides before class. (**Caution** Some of the slides are in progress. They will be labeled as such. You should not read those, they may contain false information.)

2. Ask questions on Piazza and/or bring questions to class.

3. This course will be taped so can catch up or review. **Caution**

How to Get the Most Out of This Class

1. Read notes and slides before class. (**Caution** Some of the slides are in progress. They will be labeled as such. You should not read those, they may contain false information.)

2. Ask questions on Piazza and/or bring questions to class.

3. This course will be taped so can catch up or review. **Caution**

   3.1 If cut class and DO watch videos in sync, fine.
   3.2 If cut class and INTEND to watch videos in sync, **not fine**.
   3.3 Tape might not always work.

HWs/exams

- HWs most weeks.

HWs/exams

- HWs most weeks.
- Due Monday **before** class begins. But see next item.

HWs/exams

- HWs most weeks.
- Due Monday **before** class begins. But see next item.
- **Dead Cat Policy:** Can submit HW Wed **before** class without penalty.

HWs/exams

- HWs most weeks.
- Due Monday **before** class begins. But see next item.
- **Dead Cat Policy:** Can submit HW Wed **before** class without penalty.
- **WARNING:** YOU have already been given an extension, HW solutions will be posted on Wed, so NO extensions past that.

HWs/exams

- HWs most weeks.
- Due Monday **before** class begins. But see next item.
- **Dead Cat Policy:** Can submit HW Wed **before** class without penalty.
- **WARNING:** YOU have already been given an extension, HW solutions will be posted on Wed, so NO extensions past that.
- We will keep track of your lateness NOT for grade, but for recommendation letters.

Textbook

Required Text None.
Recommended Text None.

Textbook

Required Text None.
Recommended Text None.
There will be notes, slides, and recordings of lecture online.

How to contact Prof or TAs

- email: Please put "456" in subject line.
- Office hours
- Piazza
- We are around A LOT outside of office hours. Its not as though we're going anywhere!

Intro To Cryptography

August 31, 2020

Crypto Is...

- Crypto is amazing.
  - Can do things that initially seem impossible. Example: Alice and Bob can establish a secret key without meeting.
- Crypto is important. Example: Secure financial transactions.
  - It impacts us every day Example: The last time you used a credit card you used crypto.
- Crypto is fun! Example: Making and breaking codes!

Crypto Is Not...

Crypto Is Not...

James Bond

Crypto Is Not...

James Bond

- James Bond is fictional.

Crypto Is Not...

James Bond

- James Bond is fictional.
- James Bond is a drunk.
  See article on course website: *License to Swill*.

Crypto Is Not...

James Bond

- James Bond is fictional.
- James Bond is a drunk.
  See article on course website: *License to Swill*.
- James Bond's Villains are stupid.
  See video on course website *Goodbye Mr. Bond*.

Crypto Is Not...

James Bond

- James Bond is fictional.
- James Bond is a drunk.
  See article on course website: *License to Swill*.
- James Bond's Villains are stupid.
  See video on course website *Goodbye Mr. Bond*.

Seriously: Spying depends a lot more on **Math** than on **Fancy Tuxedos**.

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

1. More of an art. Not much Mathematics.

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

1. More of an art. Not much Mathematics.
2. WWII: They used people good at crossword puzzles (see course website for an article on this).

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

1. More of an art. Not much Mathematics.
2. WWII: They used people good at crossword puzzles (see course website for an article on this).
3. Turing and others brought math into it, but not much math compared compared to **Modern**.

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

1. More of an art. Not much Mathematics.
2. WWII: They used people good at crossword puzzles (see course website for an article on this).
3. Turing and others brought math into it, but not much math compared compared to **Modern**.

Modern: (1976-today)

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

1. More of an art. Not much Mathematics.
2. WWII: They used people good at crossword puzzles (see course website for an article on this).
3. Turing and others brought math into it, but not much math compared compared to **Modern**.

Modern: (1976-today)

1. Lots of Math. Lots of Rigor.

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

1. More of an art. Not much Mathematics.
2. WWII: They used people good at crossword puzzles (see course website for an article on this).
3. Turing and others brought math into it, but not much math compared compared to **Modern**.

Modern: (1976-today)

1. Lots of Math. Lots of Rigor.
2. The notion of **Provably Secure** important.

Classical VS Modern Cryptography

Classical: (1900 BC?–1975)

1. More of an art. Not much Mathematics.
2. WWII: They used people good at crossword puzzles (see course website for an article on this).
3. Turing and others brought math into it, but not much math compared compared to **Modern**.

Modern: (1976-today)

1. Lots of Math. Lots of Rigor.
2. The notion of **Provably Secure** important.

Note: The cutoff of 1975–1976 is approximate since **History of Crypto** is hard and sometimes secret.

We Begin With Classical Cryptography

Why study Classical Cryptography?

We Begin With Classical Cryptography

Why study Classical Cryptography?

- Learn Math that will be used for Modern Crypto (e.g., Mod arithmetic).

We Begin With Classical Cryptography

Why study Classical Cryptography?

- Learn Math that will be used for Modern Crypto (e.g., Mod arithmetic).
- Shows why unprincipled approaches are dangerous (unprincipled means **not-rigorous**, not **immoral**).

We Begin With Classical Cryptography

Why study Classical Cryptography?

- Learn Math that will be used for Modern Crypto (e.g., Mod arithmetic).
- Shows why unprincipled approaches are dangerous (unprincipled means **not-rigorous**, not **immoral**).
- Illustrates why things are more difficult than they may appear.

We Begin With Classical Cryptography

Why study Classical Cryptography?

- Learn Math that will be used for Modern Crypto (e.g., Mod arithmetic).
- Shows why unprincipled approaches are dangerous (unprincipled means **not-rigorous**, not **immoral**).
- Illustrates why things are more difficult than they may appear.
- Simple examples of what will later be advanced concepts.

The Course's Main Scenario

August 31, 2020

Alice, Bob, and Eve

Alice, Bob, and Eve

- Alice sends a message to Bob in code.

Alice, Bob, and Eve

- Alice sends a message to Bob in code.
- Eve overhears it.

Alice, Bob, and Eve

- Alice sends a message to Bob in code.
- Eve overhears it.
- Alice and Bob want Eve to **not** be able to decode it.

Alice, Bob, and Eve

- Alice sends a message to Bob in code.
- Eve overhears it.
- Alice and Bob want Eve to **not** be able to decode it.

This can mean one of two things:

Alice, Bob, and Eve

- Alice sends a message to Bob in code.
- Eve overhears it.
- Alice and Bob want Eve to **not** be able to decode it.

This can mean one of two things:

- Eve does not have enough information to decode it. So even if Eve had unlimited computing power she could not decode. This is **Information-Theoretic Security**.

Alice, Bob, and Eve

- Alice sends a message to Bob in code.
- Eve overhears it.
- Alice and Bob want Eve to **not** be able to decode it.

This can mean one of two things:

- Eve does not have enough information to decode it. So even if Eve had unlimited computing power she could not decode. This is **Information-Theoretic Security**.
- Assuming Eve can't factor quickly (or some other computational limitation) then Eve cannot break the code. This is **Computational Security**.

The First Step in Any Cipher: Spaces

Alice wants to encode:

Cryptography is an important part of security

The First Step in Any Cipher: Spaces

Alice wants to encode:

Cryptography is an important part of security

She uses SHIFT-BY-1 to get:

The First Step in Any Cipher: Spaces

Alice wants to encode:

Cryptography is an important part of security

She uses SHIFT-BY-1 to get:

Dszquphsbiz jt bo jnqpsubou qbsu pg tfdvsjuz

The First Step in Any Cipher: Spaces

Alice wants to encode:

Cryptography is an important part of security

She uses SHIFT-BY-1 to get:

Dszquphsbiz jt bo jnqpsubou qbsu pg tfdvsjuz

Without any fancy math Eve knows that the second and third word are two letters long. Thats information she can use!

The First Step in Any Cipher: Spaces

Alice wants to encode:

Cryptography is an important part of security

She uses SHIFT-BY-1 to get:

Dszquphsbiz jt bo jnqpsubou qbsu pg tfdvsjuz

Without any fancy math Eve knows that the second and third word are two letters long. Thats information she can use!

Alice needs to hide spacing information. What to do?

The First Step in Any Cipher-Blocks of Five

Alice wants to encode

The First Step in Any Cipher-Blocks of Five

Alice wants to encode

Cryptography is an important part of security

The First Step in Any Cipher-Blocks of Five

Alice wants to encode

Cryptography is an important part of security

She break the message into blocks of 5:

Cryto graph yisan impor tantp artof secur ity

and then codes it.

The First Step in Any Cipher-Blocks of Five

Alice wants to encode

Cryptography is an important part of security

She break the message into blocks of 5:

Cryto graph yisan impor tantp artof secur ity

and then codes it.

Because of blocks-of-5, spaces will not give anything away.

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.
   Map everything to Capitals.

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.
   Map everything to Capitals.
2. Punctuation leaks information.

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.
   Map everything to Capitals.
2. Punctuation leaks information.
   Get rid of all punctuation.

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.
   Map everything to Capitals.
2. Punctuation leaks information.
   Get rid of all punctuation.
3. What to do about numbers?

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.
   Map everything to Capitals.
2. Punctuation leaks information.
   Get rid of all punctuation.
3. What to do about numbers?
   Just like letters- alphabet is 36 characters.

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.
   Map everything to Capitals.
2. Punctuation leaks information.
   Get rid of all punctuation.
3. What to do about numbers?
   Just like letters- alphabet is 36 characters.
   More generally, we will take into account alphabet size.

The First Step in Any Cipher-Other Issues

I want to encode:

Are my TAs for CMSC/MATH/ENEE 456 awesome? YES!

1. Capital and small letters leak information.
   Map everything to Capitals.
2. Punctuation leaks information.
   Get rid of all punctuation.
3. What to do about numbers?
   Just like letters- alphabet is 36 characters.
   More generally, we will take into account alphabet size.

Note: We assume $a, \ldots, z$ unless otherwise noted.

BILL, TURN OFF RECORDING

BILL TURN OFF RECODING!!!