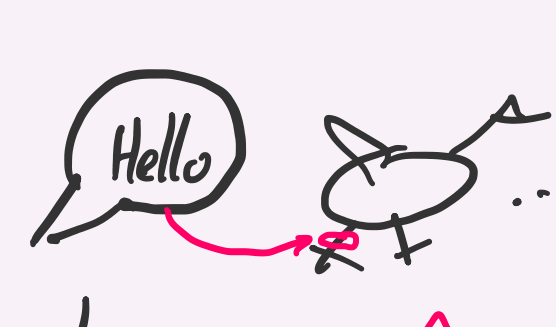
Our Protagonists:

Alice & Bob.

Plot:



Bob - - - - - - - - → Alice

intercepts pidgeon.

Antagonist: Eve (eavesdropper)

(reads this

gh 7 29 ∅ α ε . . .

Eve sees gibberis.

Bob keeps secret.

Alice can't read it either...

↑ Alice needs a process to recover "hello" from "gh7 29 ∅ α ε . . .".

---

m = message "plaintext"

c = gibberish "cipher text"

Situation

Eve c

Bob m ⇝(e) c ———→ Alice c ⇝(d) m

Goals

- c has enough structure so Alice can recover m.
- Eve shouldn't be able to recover m from c.

---

2 paradigms

1) Symmetric Encryption:

Alice & Bob meet in secret to discuss encryption scheme.

"Shared secret"

2) Public Key Encryption: (PKE)

Alice & Bob never meet safely away from eve.

↳ Internet Merchant Communication.

See examples of ① even today.

Main focus will be ②

* Surprising (to me) that PKE is possible!
* Math behind PKE is beautiful!!

Course Goal **

Describe & implement methods for Alice & Bob to securely communicate over an unsecured channel monitored by Eve.

---

2 perspectives

① Mathematics. Develop abstract theory including

* Abstract Algebra
* Number Theory
* Geometry
* Complex Numbers
* Probability Theory.

Definition / Theorem / Proof style.

Develop background as needed.

② Computation & Implementation.

* Coding up system
* Turn messages into numerical data.
* Write algorithms to encode it.

Structure

* Lectures twice a week, T, Th 5 - 6:30 PM

Lectures & You-Do problems

↳ Appear in HW.

* Course Capture.

⇝ Stay home if sick.

* Office Hours: TBA.

⇝ Depending restrictions & policy, may be online.

⇝ Available online.

⇝ Probably Masked up.

* Homework: 50% Grade.

⇝ Due Tuesdays (almost) every week.

* 2 parts
  - a) Written Part
    - ⇝ proofs
    - ⇝ Examples
    - ⇝ Turned in via PDF (Latex or handwritten)
  - b) Implementation Part
    - ⇝ Code up systems, algorithms
    - ⇝ CoCalc ⊛
    - ⇝ turn in on Gradescope.

* 2 projects: 30% grade
  - a) RSA
  - b) Elliptic Curve Crypto.

Communication Part.

We will send eachother secret messages using your implementations!

* Take-Home Final: 20%

COVID Addendum:

- Flexible me w/ you, you w/ me.
- Schedule might change.
- Might go online.

↳ Post lectures.

- Projects are dependent on covering relevant material... so due dates might change..

⚠ HW0 is due on Tuesday 8/31

Examples of Ciphers

Ex Caesar Cipher.

Courier delivers a message!

ђsgrd bjfp oj xεzym
enemy weak to south

⇝ Sends soldiers south, breaking through to a decisive victory!!

How?

Idea: shift alphabet!

a b c d e f g h..

f g h i j k l m...

Observations:

1) Rather easy to crack even w/o a computer.

↳ only 26 choices ⇐

2) Sender & reciever must securely meet to decide on code.

Axiom 1: Always assume Eve knows our general framework.

Fix condition 1

Ex Substitution Cipher.

a b c d e . . .

w e x m . . . .

~~Shift~~ permute the alphabet

Better 26! different ciphers

$26! = 26 \cdot 25 \cdots \approx 4 \cdot 10^{26}$

↑ choices for a

choices for b

Randomly guessing substitution won't decrypt message.

Axiom 2: Eve will always use the best tools at her disposal.

e.g. Substitution cipher is vulnerable to a probability analysis.

Vocab

Cryptography: Encoding messages & coming up w/ Ciphers.

Cryptanalysis: Attacking ciphers & searching for vulnerability.