

Instructor: Dawid Wu (dwu4@cs.utexas.edu)

TA: TBD

Overarching goal of cryptography: securing communication over untrusted networks

Alice $\xrightarrow{\quad}$ Bob
↓

third party should not be able to

- 1) eavesdrop of communication (confidentiality)
- 2) tamper with the communication (integrity)

Today: secure communication on web (https://...)

TLS protocol (transport layer security)

two components: handshake (key exchange)

record layer (confidentiality + integrity)

protecting data at rest: disk encryption

Most of this course: study mechanics for protecting confidentiality + data

- Encryption schemes for confidentiality
- Signature schemes for message integrity
- Key exchange for setting up shared secrets

End of this course: protecting communication \Rightarrow protecting computation

- Two users want to learn a joint function of their private inputs
 - \hookrightarrow training models on private (hidden) data
 - \hookrightarrow comparing two DNA sequences privately
 - \hookrightarrow private auction to determine winner without revealing bids
 - \hookrightarrow private voting mechanisms (can identify winner of election without revealing individual votes)
- We can show the following remarkable theorem:

"Anything that can be computed with a trusted party can be computed without!"

Logistics and administrivia:

← course is primarily a theory course - we will assume familiarity with reductions and mathematical proofs!

- Course website: <https://www.cs.utexas.edu/~dwu4/courses/fc23>
- See Ed Discussion for announcements, notes will be posted to course website (1-2 days after lecture)
- Homework submission via Gradescope (enroll via Canvas) ← one of these is programming assignment (Python)
- Course consists of 5 homework assignments (worth 70%) and two in-class exams (worth 30%)
- Five late days for the semester: use in 24-hour increments, max 72 hours (3 late days) for any single assignment
- Some office hours will also be available on Zoom

This semester: lectures will be recorded using Lectures Online

Please participate virtually if you are feeling unwell

Still broken by frequency analysis

- e is the most frequent character ($\sim 12\%$)
- q is the least frequent character ($\sim 0.10\%$)

Can also look at digram, trigram frequencies

- Vigenere cipher (late 1500s) - "polyalphabetic substitution"
key is short phrase (used to determine substitution table):

m = HELLO

k = CAT

Encrypt (k, m):

HELLO	
+ CATCA	← repeat the key
KFFPP	

↑
interpret letters as number between 1 and 26
addition is modulo 26

if we know the key length, can break using frequency analysis
otherwise, can try all possible key lengths $l = 1, 2, \dots$

↳ general assumption: keys will be much shorter than the message (otherwise if we have a good mechanism to deliver long keys securely, then can use that mechanism to share messages directly)

- Fancier substitution ciphers: Enigma (based on rotor machines)
but... still breakable by frequency analysis

Today: encryption done using computers, lots of different ciphers

- AES (advanced encryption standard; 2000)

"block cipher"

- Salsa (2005) / ChaCha (2008)

"stream cipher"