Math 187A — Cryptography

Instructor: Sunny (Shishir Agrawal)

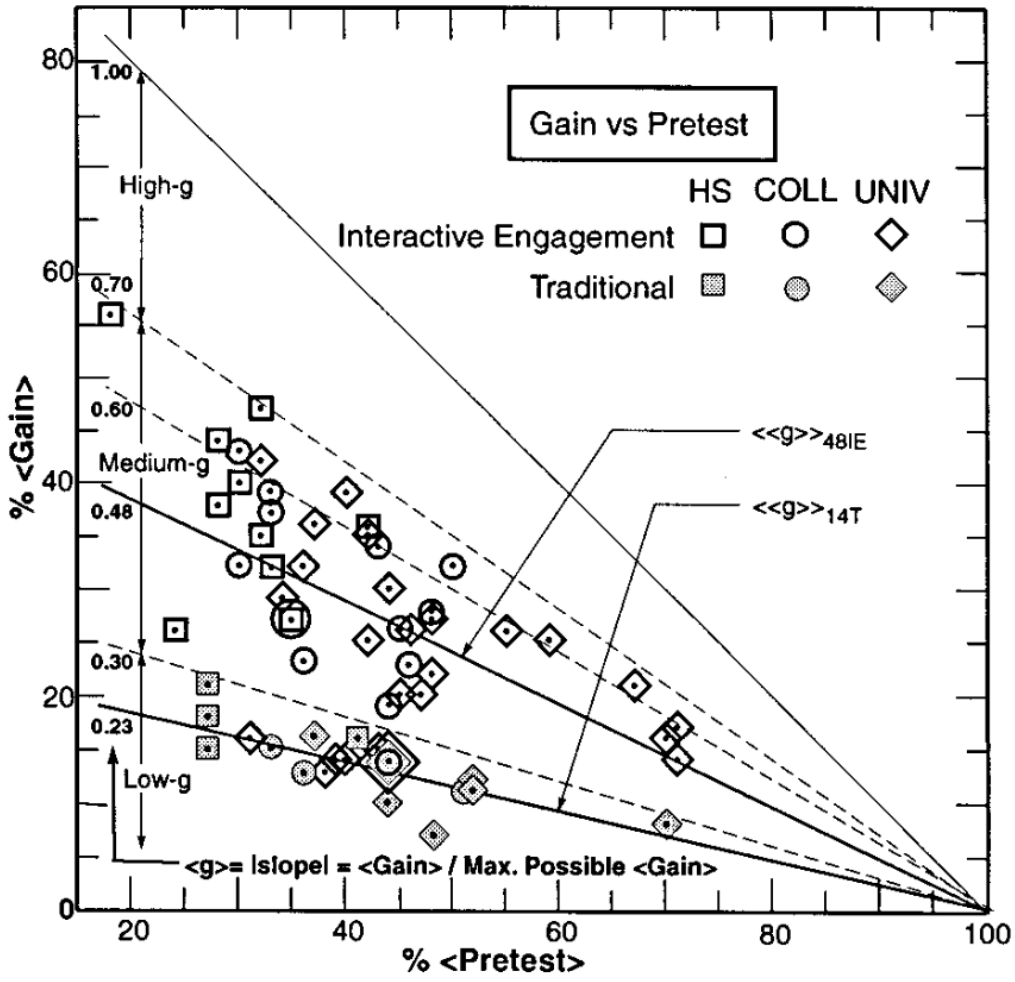
Common Ground

Turn to someone sitting near you who you don't already know. Take about 5 minutes to find at least *two* things that you have in common with your partner.

(Try to go beyond "We're both taking Math 187A this quarter," but it doesn't have to anything deeply personal.)

About Me

Pedagogy Data



Hake, doi:10.1119/1.18809

Class Structure

https://sagrawalx.github.io/teaching/wi23_math187a/

Cryptography

About techniques for secure communication.

Has a long history, and remains active through today.

Scytale

Cryptographic device mentioned in Ancient Greek texts as early as 600s BCE.

Encrypting “Keiser Augustin har sviktet...”
(Norwegian Bokmål for “Emperor Augustin has failed...”?)

Atbash Cipher

Used by Ancient Hebrew scholars as early as 500s BCE.

ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת

English alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Atbash Cipher

Used by Ancient Hebrew scholars as early as 500s BCE.

א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

English alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Try it! Encrypt a short message about something you did over winter break using the Atbash cipher. Then exchange your message with your neighbor and decipher.

Frequency Analysis

Manuscript on Deciphering Cryptographic Messages by Arab polymath Al-Kindi (800s CE).

Method for breaking all ciphers known up to that point, and many that have been used since!

Renaissance

Leon Battista Alberti (1404-1472) invented a cipher resistant to frequency analysis.

Johannes Trithemius (1462-1516) wrote the book *Polygraphia*.

Giovan Battista Bellaso (1505-??) invented the so-called Vignère cipher, which remained unbreakable for 300 years.

Course Outline

In the first part of this course, we'll look at how some of these "classical" ciphers work.

Course Outline

In the first part of this course, we'll look at how some of these "classical" ciphers work.

Then we'll spend some time talking about how these ciphers can be broken (including the Vignère cipher).

Course Outline

In the first part of this course, we'll look at how some of these "classical" ciphers work.

Then we'll spend some time talking about how these ciphers can be broken (including the Vignère cipher).

Then we'll move on to some "modern" cryptography.

Modern Cryptography

Begins with Claude Shannon's "A Mathematical Theory of Cryptography" (1949).

Modern Cryptography

Begins with Claude Shannon's "A Mathematical Theory of Cryptography" (1949).

Data Encryption Standard (DES) in 1975, replaced by Advanced Encryption Standard (AES) in 2001.

Modern Cryptography

Begins with Claude Shannon's "A Mathematical Theory of Cryptography" (1949).

Data Encryption Standard (DES) in 1975, replaced by Advanced Encryption Standard (AES) in 2001.

Public-key cryptography by Whitfield Diffie and Martin Hellman in 1976. (Equivalent system was described by GCHQ mathematician Malcolm Williamson in 1974, declassified in 1997).

Modern Cryptography

Begins with Claude Shannon's "A Mathematical Theory of Cryptography" (1949).

Data Encryption Standard (DES) in 1975, replaced by Advanced Encryption Standard (AES) in 2001.

Public-key cryptography by Whitfield Diffie and Martin Hellman in 1976. (Equivalent system was described by GCHQ mathematician Malcolm Williamson in 1974, declassified in 1997).

RSA cryptosystem by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. (Equivalent system was described by GCHQ mathematician Clifford Cocks in 1973, declassified in 1997).

Post-Quantum Cryptography

We already know quantum algorithms to break Diffie-Hellman, RSA, and other public-key cryptosystems!

Quantum computing hardware is rapidly improving and will soon catch up to the theory.

There is work being done on quantum-resistant public-key cryptography, but we will not touch on this.