## Math 187A — Cryptography

## Instructor: Sunny (Shishir Agrawal)

(ロ)、(型)、(E)、(E)、 E) の(()

## **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/sp24\_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..."?)

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

#### **Atbash Cipher**

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

אבגדה וזחט יכלמנסעפצקרשת תשרקצפעסנמלכיטח זוהדגבא 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.

אבגדה וזחט יכלמנסעפצקרשת תשרקצפעסנמלכ יטח ז והדגבא 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 spring break using the Atbash cipher. Then exchange your message with your neighbor and decipher.

#### **Frequency Analysis**

Manuscript on Decriphering 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! ناسه الده مناء المروضة ملكلان تشتر امرة مره الكام مع وعمر ما يعرف مد بلاما الدهار معام وعلم والحرف بلوطوع منام مناطق من مع تعلين منارع مسلوم إلى مواصل ملكوم لا من من معالما مسير وملام و المروسية من معالم المدارين وتحد ولعالم المواصل المسلوم المواليم الم مسم الإمار مع والحاص والمروم والصع وحد ولعام والمع المع المواليم المج مسم الإمار مع والحاص والمروم الصع وحد ولعام والمع المع من مع

الااداء والجداله والعالم وصلوا بدعلم مدمحد والمسه ع

دنسالا الاستسبس الرحسين وسالا الاستسبس تلحير الدري استرابا مع الأوساس المحد محالة مار عن علم المراجز من وكما مكون التدارا المعليه مارم المحلسلا المراجز المعارين مع الملك ماليون الموارين المحالة المعام عالما المار ومسترارين المحالين المحالة المعارين المعارين المعالية

▲□▶ ▲□▶ ▲□▶ ▲□▶ □ のQで

### 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.

AVTREALPHABET, PAR							
requel Honorus, furnomine incoards, delen-							
in the magic							
ann i	noj suld oj	dano) ata-	nate day				dui Shur
2	b	C	a	e	I	g	n
y	4	m	m	2	r	y	X
q1	k	1 4	m	n	0	Р	PP
nIJ	Cun	Y.	Ma	The	m	12	In
r	S	t	u	x	Y	Z.	82
m	¥	V4	fre	nu	Min	ul	Tig

### **Course Outline**

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

### **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).

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三 のへぐ

### **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).

▲□▶ ▲□▶ ▲□▶ ▲□▶ ■ ●の00

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

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

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ 三三 - のへぐ

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.

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).

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

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.