DS 593: Privacy in Practice

Introduction

Instructor: Alishah Chator

data privacy
Shift

PRIVACY

Personal Introduction

So What Exactly is This Course About?

- Privacy!
  - What does it mean?

- In Practice!
  - What does it look like?

So What Exactly is This Course About?

- Maybe different from other courses you have taken in CDS
- The focus is on critically analyzing the technology and policies around us
- Structure is inspired by social science based classes

Motivation

- Designing a class I wish I could have taken ☺

- Privacy shows up everywhere but it is also tricky to unpack
    - Relies on complex protocols and technologies
    - Governed by obscure laws and regulations
    - Privacy-marketed tools can require a lot of technical expertise
    - Often is framed in opposition to other social goods
        - i.e. safety
    - Unclear how much the average person should care

Syllabus!

- https://docs.google.com/document/d/1zVg4laCQYZsfp5VupwMLzGoBdkWzrjZPmom77diM-bY/edit?usp=sharing

Framing Questions

- What is the cost of data?
  - Especially the non-financial cost

- What does it mean to give user’s agency
  - Ability to reason about the technologies around them intuitively
  - And then ability to make usage decisions based on that

- When is **techno-solutionism** appropriate
  - There are many ways to solve problems: technically, legally, socially, etc

- Much of what I am talking about may not seem like it is privacy

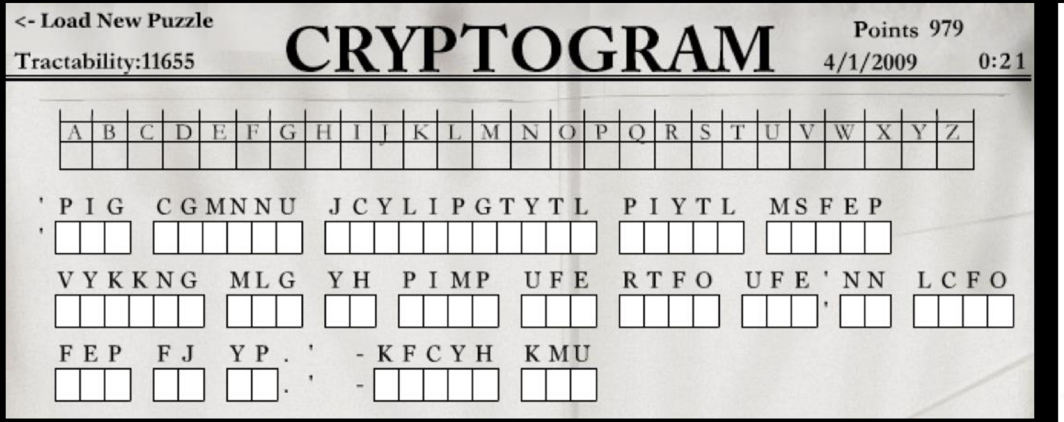
- This class is going to be using an extremely broad notion of privacy

- We will unpack this more next week

History of Security and Privacy

The Boring Context-free History of Privacy Technologies

Caesar Cipher – Antiquity



<- Load New Puzzle

Tractability:11655

CRYPTOGRAM

Points 979

4/1/2009

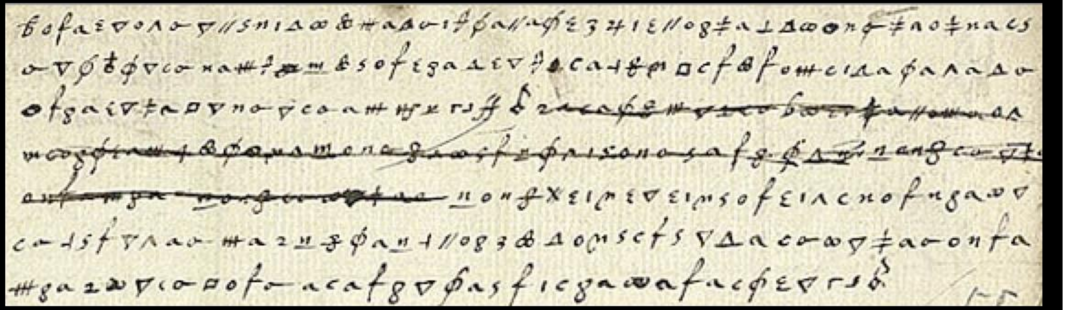
0:21

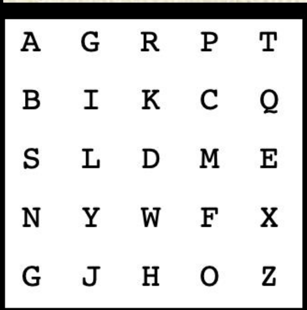
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

'PIG CGMNNU JCYLIPGTYTL PIYTL MSFEP

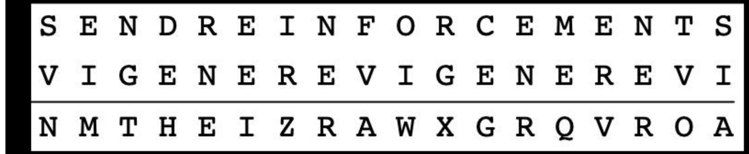
VYKKNG MLG YH PIMP UFE RTFO UFE'NN LCFO

FEP FJ YP.' -KFCYH KMU

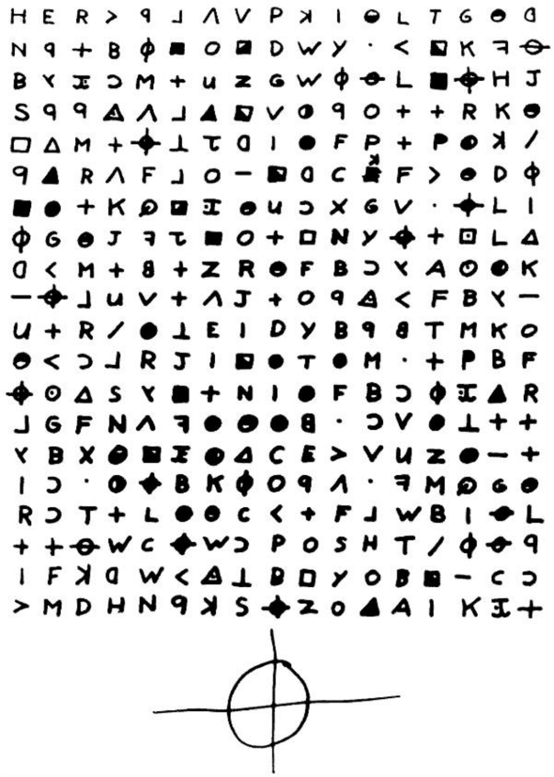




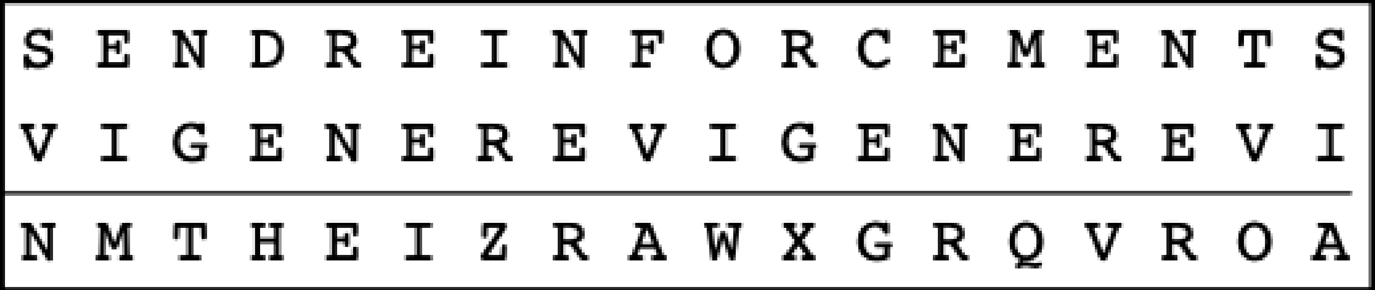
A	G	R	P	T
B	I	K	C	Q
S	L	D	M	E
N	Y	W	F	X
G	J	H	O	Z



S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A

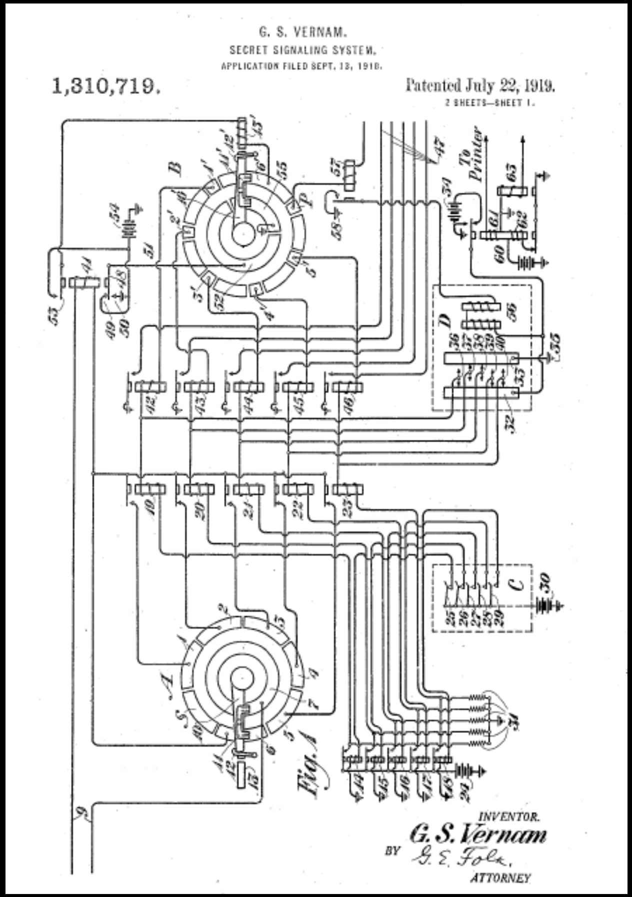


Vigenère Cipher - ~1500



S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A

One Time Ciphers – early 1900s



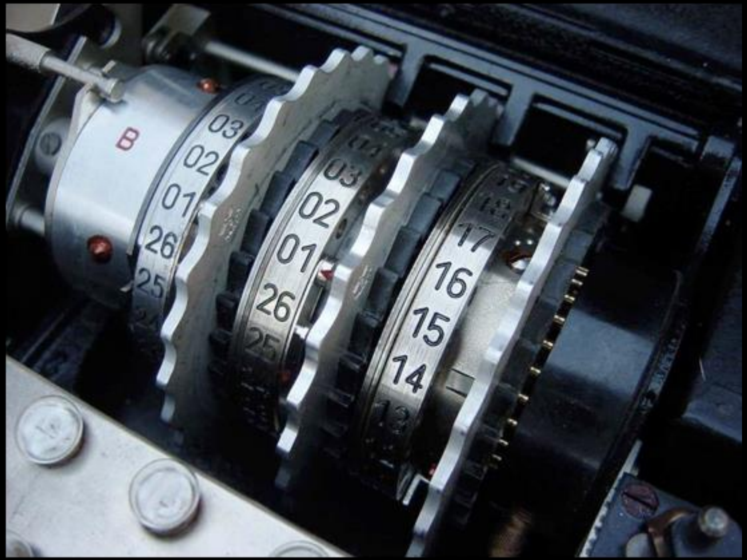
G. S. VERNAM.
SECRET SIGNALING SYSTEM.
APPLICATION FILED SEPT. 13, 1918.

1,310,719.

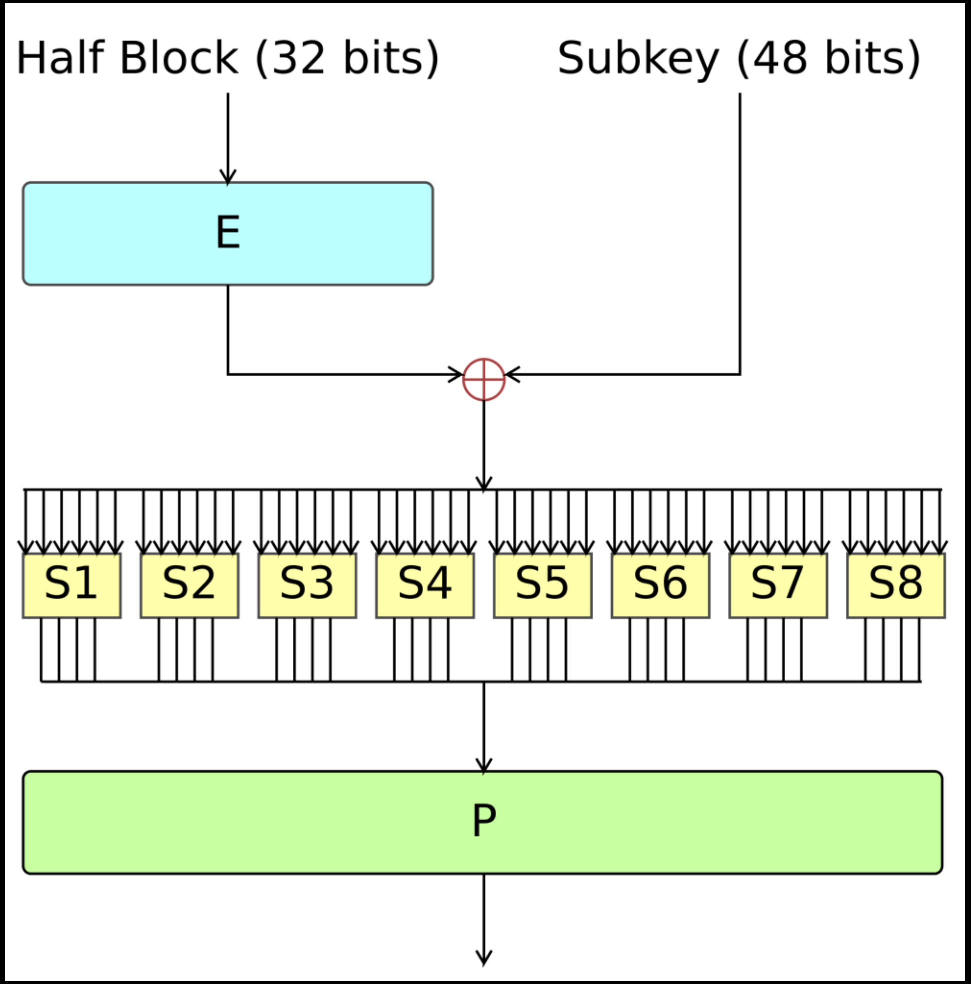
Patented July 22, 1919.
2 SHEETS—SHEET 1.

INVENTOR.
G. S. Vernam
BY G. E. Folk,
ATTORNEY

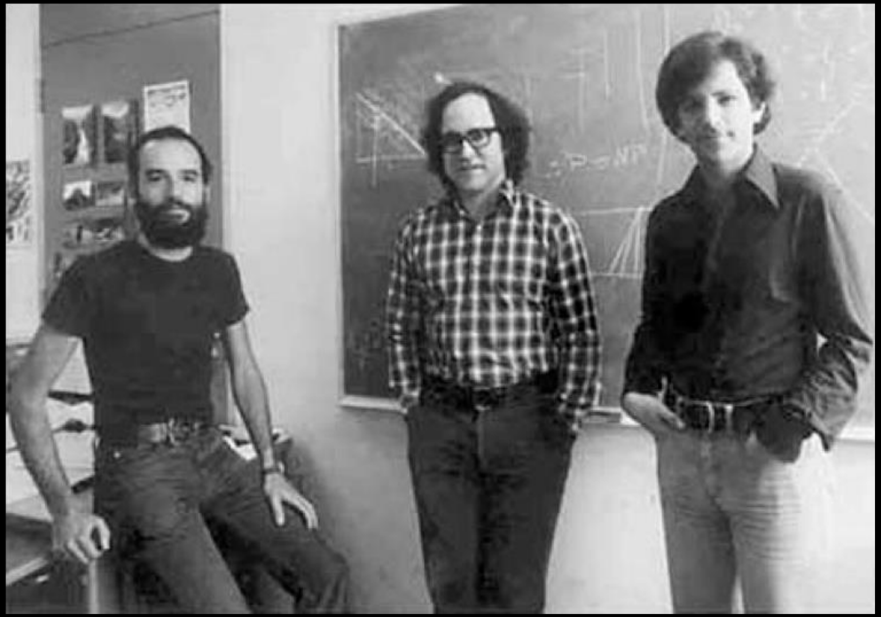
Mechanical/Rotor Ciphers – 1920s



Block Ciphers – 1970s



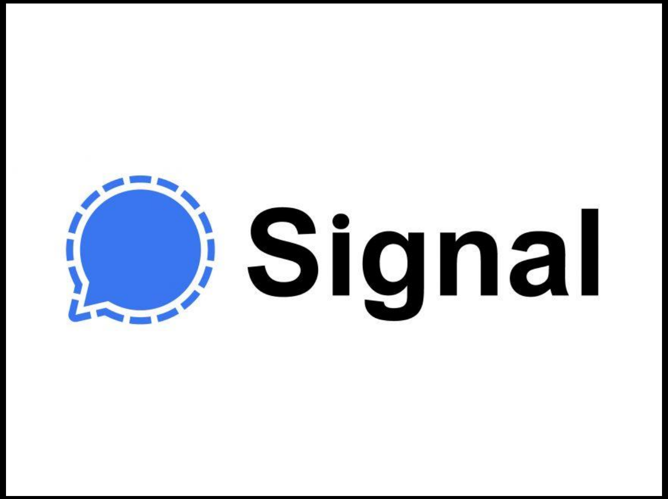
Public Key Cryptography – Late 1970s

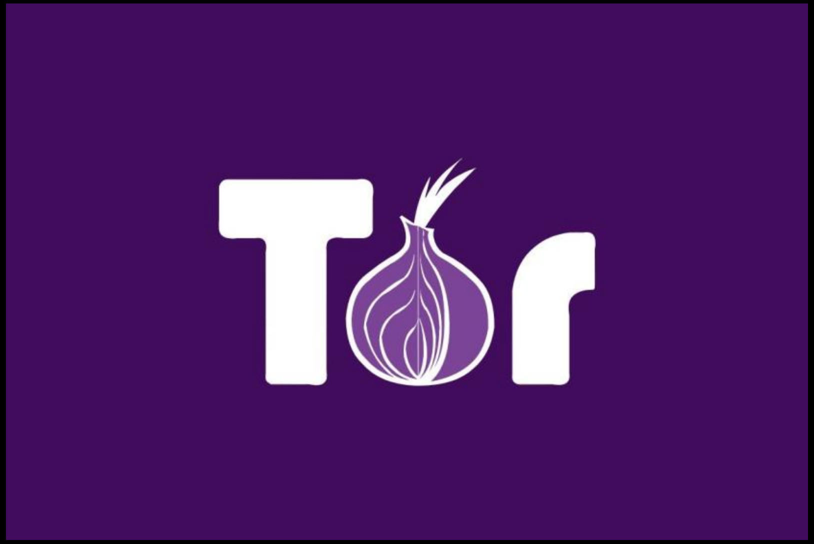


Internet and SSL – ~1990s

HTTP
+
SSL
=
HTTPS

Now





Next time

- Let’s add some context
  - Historical
  - Modern