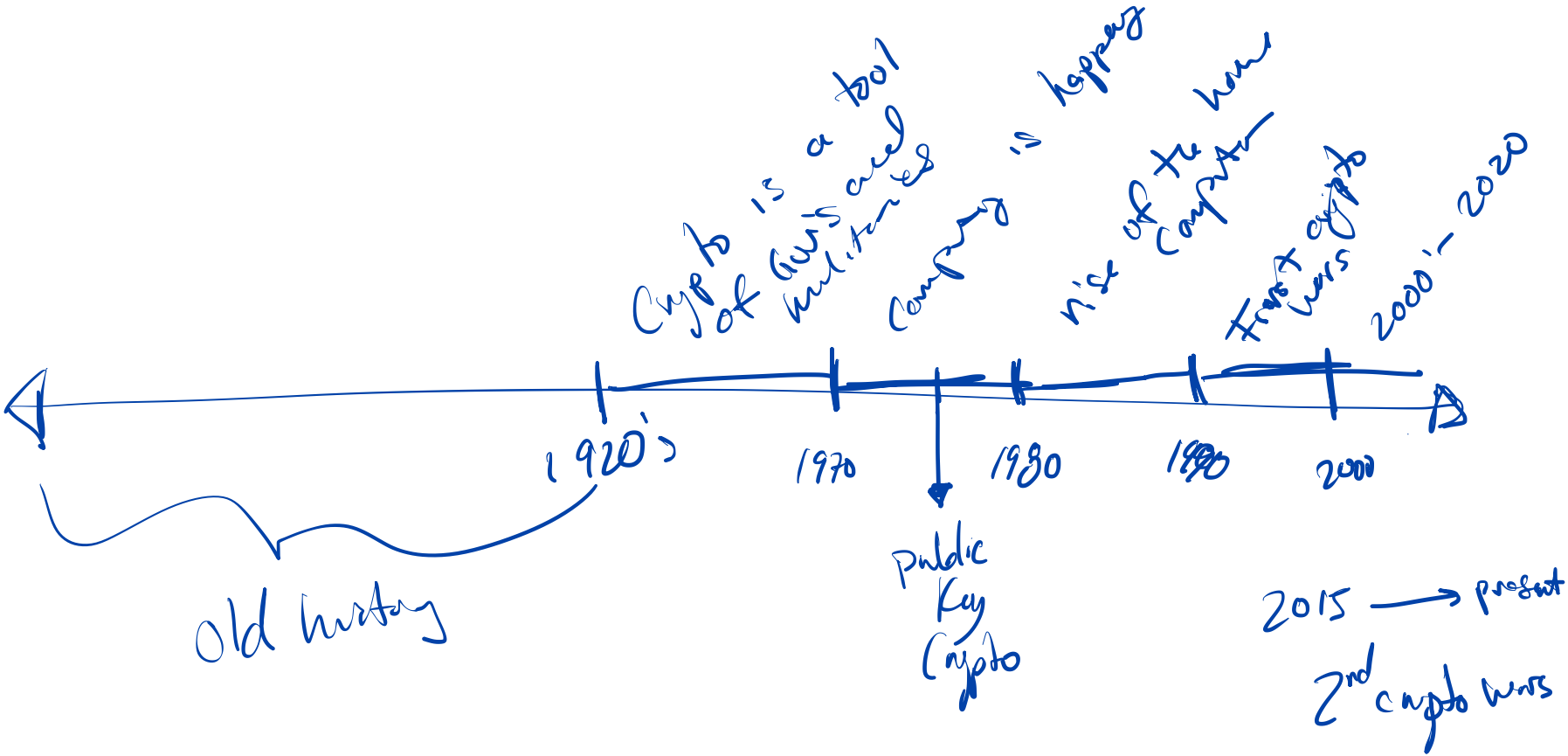
CS558 Network Security

Lecture 22: History of Encryption

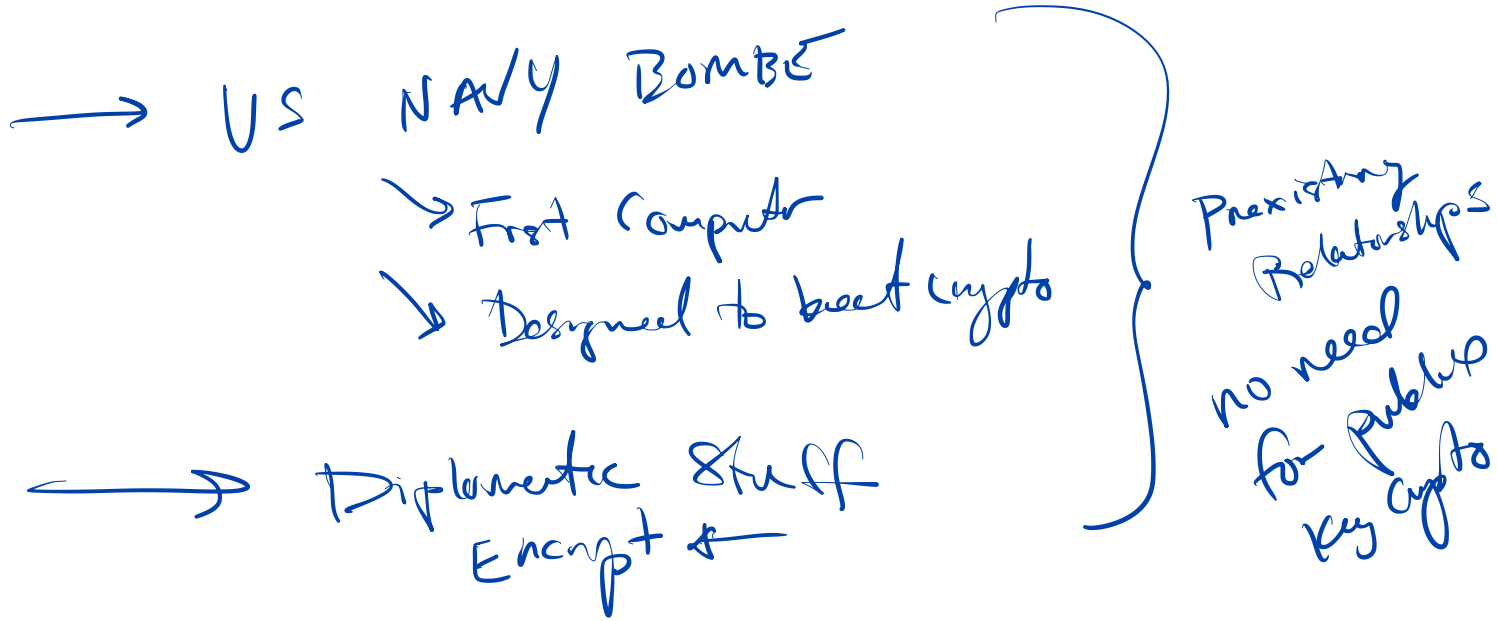
BOSTON UNIVERSITY

I AM NOT A LAWYER. NOTHING I SAY IS LEGAL ADVICE

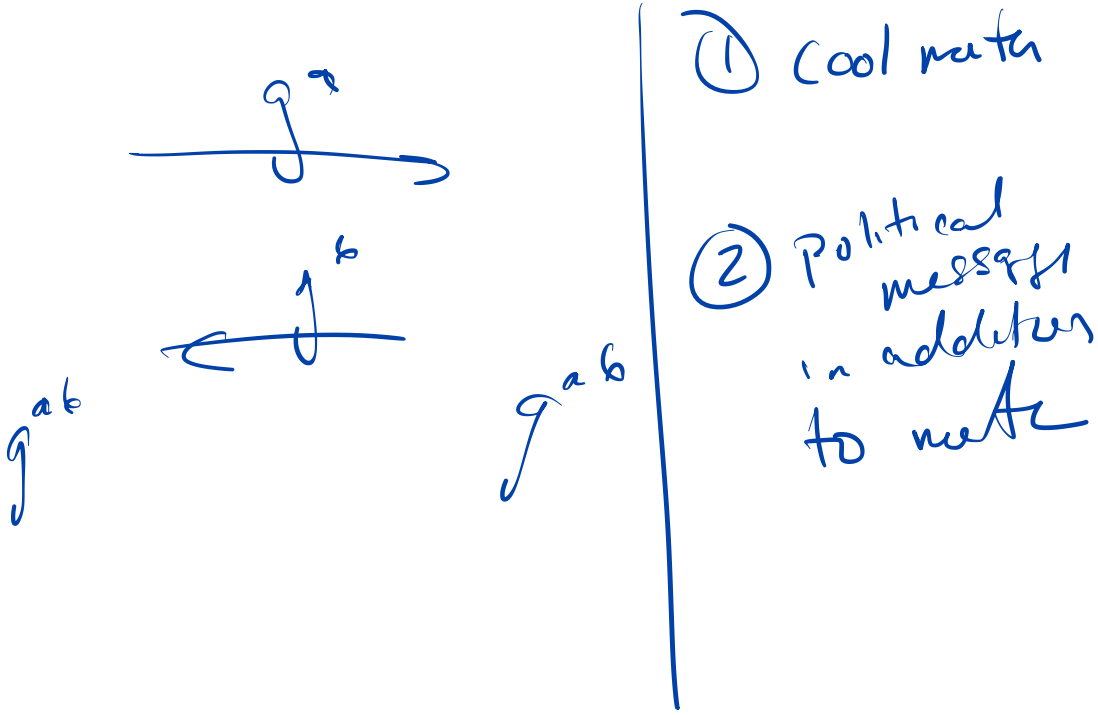
BOSTON UNIVERSITY

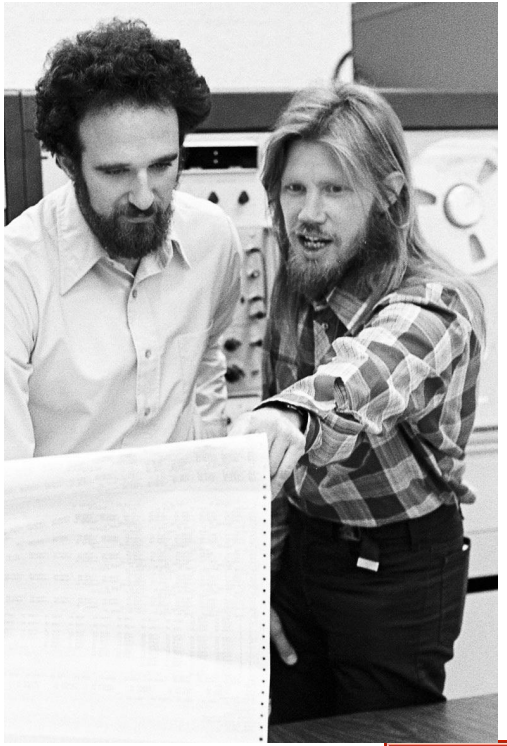


Pre 1970's -- Crypto for Military



1970's -- Genesis of Public Key Cryptography





1980's and 1990's -- Rise of computing and internet

→ US Gov Backs Creation of Crypto

→ Business start using Crypto

Need for cryptography as businesses

US Support of Cryptography to protect Business

Law Enforcement & Intelligence Agencies start getting nervous

1990's -- Things Get Spicy

- Fights over Export Grade Encryption
- Key Escrow and the Clipper Chip (1993)
- CALEA (1993)
- Section 230 (we'll discuss later this class)

Export Grade Cryptography (until ~1996)

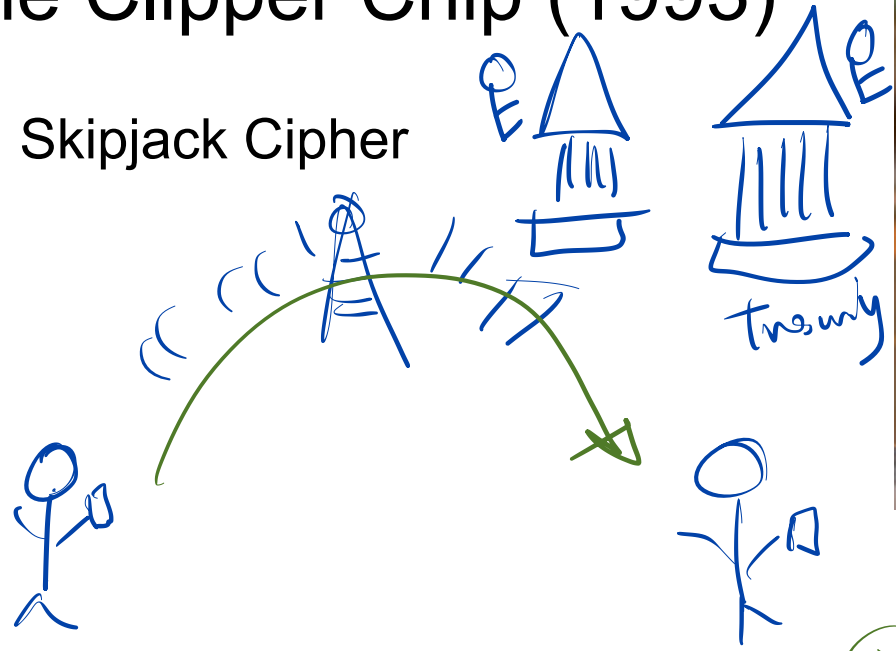
- Applied Crypto Textbook (Schneier, Karn)

- Bernstein vs United States

- Philip Zimmerman (Creator of PGP)

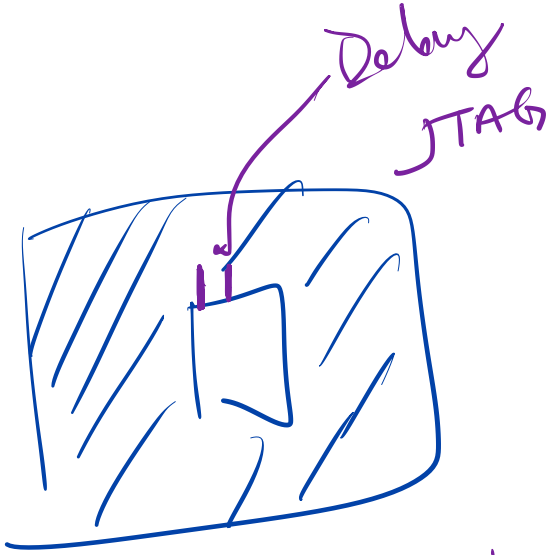
The Clipper Chip (1993)

- Skipjack Cipher



① want Security/ Privacy for individuals

② not too much S.t. Law Enforcement can't get in



Shows that the proposal is broken

Matt Blaze

CALEA -- Communications Assistance for Law Enforcement Act

- “Requires a telecommunications carrier to ensure that its equipment, services, or facilities that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of: (1) isolating and enabling the Government, pursuant to a court order or other lawful authorization, to intercept all of the subscriber's wire and electronic communications over such facilities concurrently with their transmission or at any later time acceptable to the Government”

- “Exempts information services”

The End of Crypto Wars 1

- “Strong” Encryption is legal
- CALEA ensures government access to telecommunications data
- Law Enforcement continues to grumble

Fast Forward: up to 2015

- Encryption becomes widely deployed and default

- All Writs Act of 1789

"may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law"

BOSTON UNIVERSITY

Apple vs FBI

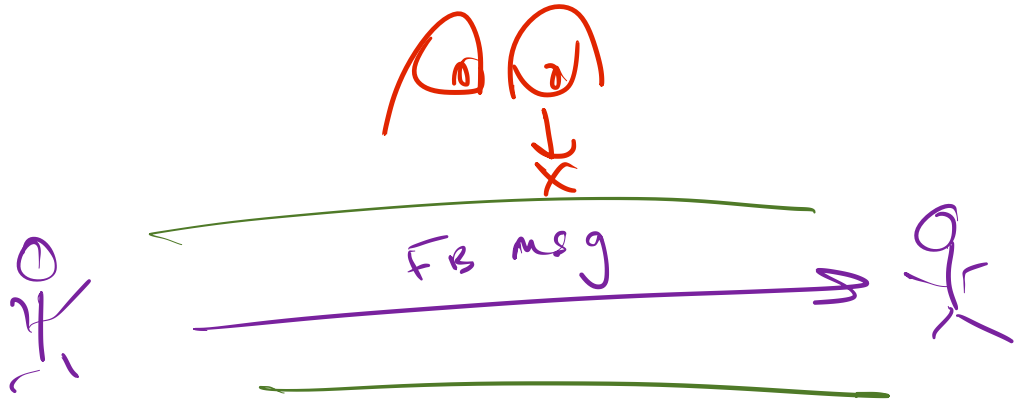
- Brooklyn drug case

  "It would be absurd to posit that the authority the government sought was anything other than obnoxious to the law."

- San Bernardino Shooting Case

- Resolution unknown, as cases were dropped

Encryption in Motion (Encrypted Messaging)



Clipper Chip

Key Escrow

Backdoors

[Warrant-proof Encryption]

Section 230 of the Communications Act (1996)

SESTA-FOSTA (2018)

- Stop Enabling Sex Traffickers Act
- allow states and victims to Fight Online Sex Trafficking Act

modifies Section 230

EARN IT Act (2019)

- Carve-out Section 230 Exception for CSAM
- Lawful Access to Encrypted Data Act

BOSTON UNIVERSITY

Congress / Bills / S. 3538 (117th)

S. 3538: EARN IT Act of 2022

Track S. 3538 | Call or Write Congress | Add to List

Overview | Summary | Cosponsors | Details | Text | Study Guide

A bill to establish a National Commission on Online Child Sexual Exploitation Prevention, and for ot

The bill's titles are written by its sponsor.

Sponsor and status

Lindsey Graham

Sponsor. Senior Senator for South Carolina. Republican.


S. 3538

IN THE SENATE OF THE UNITED STATES

A BILL

Read Text »

Last Updated: Jan 31, 2

Length: 53 pages

Introduced Jan 31, 2022
117th Congress (2021–2023)

Status **Ordered Reported** on **Feb 10, 2022**

The committees assigned to this bill sent it to the House or Senate as a whole for consideration on February 10, 2022.

Other activity may have occurred on another bill with identical or similar provisions.

Cosponsors 21 Cosponsors (11 Republicans, 10 Democrats)

Prognosis 16% chance of being enacted according to Skopos Labs (details)

Source Congress.gov

History

JUL 2, 2020 — Earlier Version — Ordered Reported
This activity took place on a related bill, S. 3398 (116th).

JAN 31, 2022 — **Introduced**
Bills and resolutions are referred to committees which debate the bill before possibly sending it on to the whole chamber.
Read Text »

FEB 10, 2022 — **Ordered Reported**
A committee has voted to issue a report to the full chamber recommending that the bill be considered further. Only about 1 in 4 bills are reported out of committee.

If this bill has further action, the following steps may occur next:

BOSTON UNIVERSITY

Where are we today?

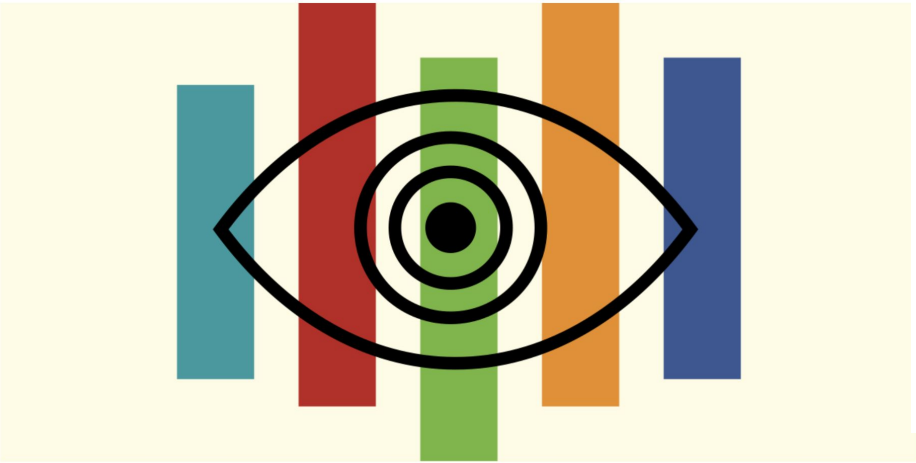
- Encryption is broadly legal, but under threat
- “Tech-lash” fueled concerns about the power of Big Tech proving cover
- ***We have no idea what is going to happen next***

ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action Tools Donate

India's Draconian Rules for Internet Platforms Threaten User Privacy and Undermine Encryption

BY KATITZA RODRIGUEZ AND KURT OPSAHL | JULY 20, 2021



Australia passes controversial anti-encryption law that could weaken privacy globally

Companies are required to give access to encrypted communications

By Jon Porter | @JonPorty | Dec 7, 2018, 8:38am EST

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.

SHARE

Illustration by Alex Castro / The Verge

BOSTON UNIVERSITY

WhatsApp and Signal unite against online safety bill amid privacy concerns

Encrypted chat apps sign open letter warning of 'unprecedented threat to safety and security' of UK citizens

Age checks, trolls and deepfakes: what's in the online safety bill?

WhatsApp and Signal are concerned the online safety bill could in effect outlaw end-to-end encryption. Photograph: Yui Mok/PA

The rival chat apps WhatsApp and Signal have joined forces in a rare show of unity to protest against the online safety bill, which they say could