



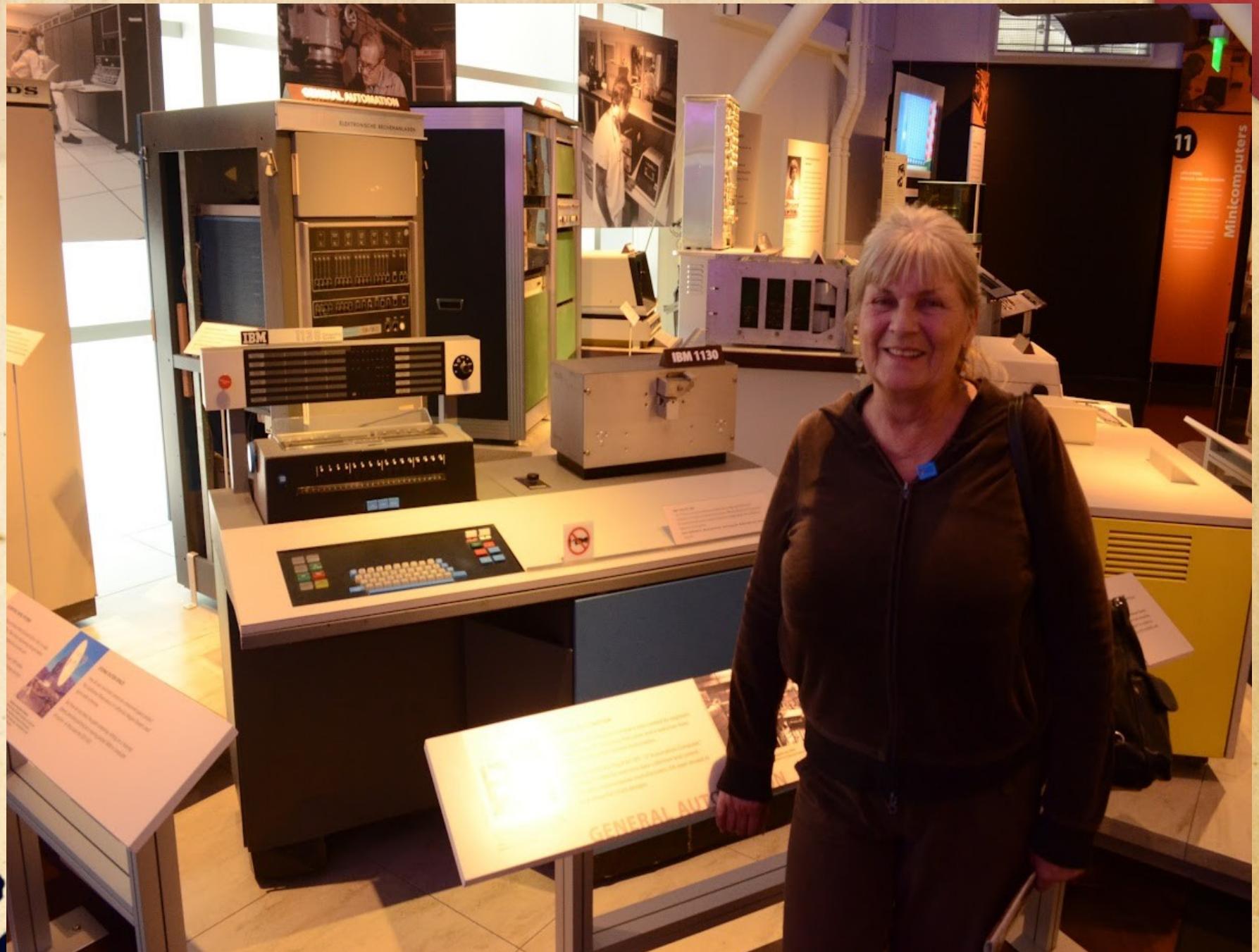
CSE 548 Spring 2026

Jed Crandall

jedimaestro@asu.edu

A bit about me...

- Associate Professor, SCAI *and* Biodesign Center for Biocomputation, Security, and Society
- Research is about Internet Freedom, including:
 - Internet censorship and censorship evasion
 - Machine-in-the-middle attacks, adversarial networking
 - Privacy, forensics, and a few other things





https://commons.wikimedia.org/wiki/File:Apple_II_typical_configuration_1977.png



Welcome to Debian Linux 1.1!

This is the Debian Linux Boot Disk. On most systems, you can go ahead and press <ENTER> to begin installation. You will probably want to try doing that before you try anything else. If you run into trouble, or if you already have questions, press the function key <F1> for quick installation help.

WARNING: You should completely back up all of your hard disks before proceeding. The installation procedure can completely and irreversibly erase them! If you haven't made backups yet, remove the floppy from the disk drive and press <RESET> or <Control-Alt-Del> to get back to your old system.

Debian Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. For copyright information, press <F5>.

This boot floppy installs the Linux kernel version 2.0.0.

Press <F1> for help, or <ENTER> to boot!

boot: _

https://archive.org/details/debian_1.1



Plagiarized from
<https://sites.psu.edu/thedepweb/2015/09/17/captain-crunch-and-his-toy-whistle/>

<https://archives.phrack.org/issues/7/3.txt>

==Phrack Inc.==

Volume One, Issue 7, Phile 3 of 10

=====

The following was written shortly after my arrest...

\/\The Conscience of a Hacker/\/

by

+++The Mentor+++

Written on January 8, 1986

=====

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

<https://archives.phrack.org/issues/7/3.txt>

==Phrack Inc
Volume One, Issue 7, Ph

=====The following was written shortly after my

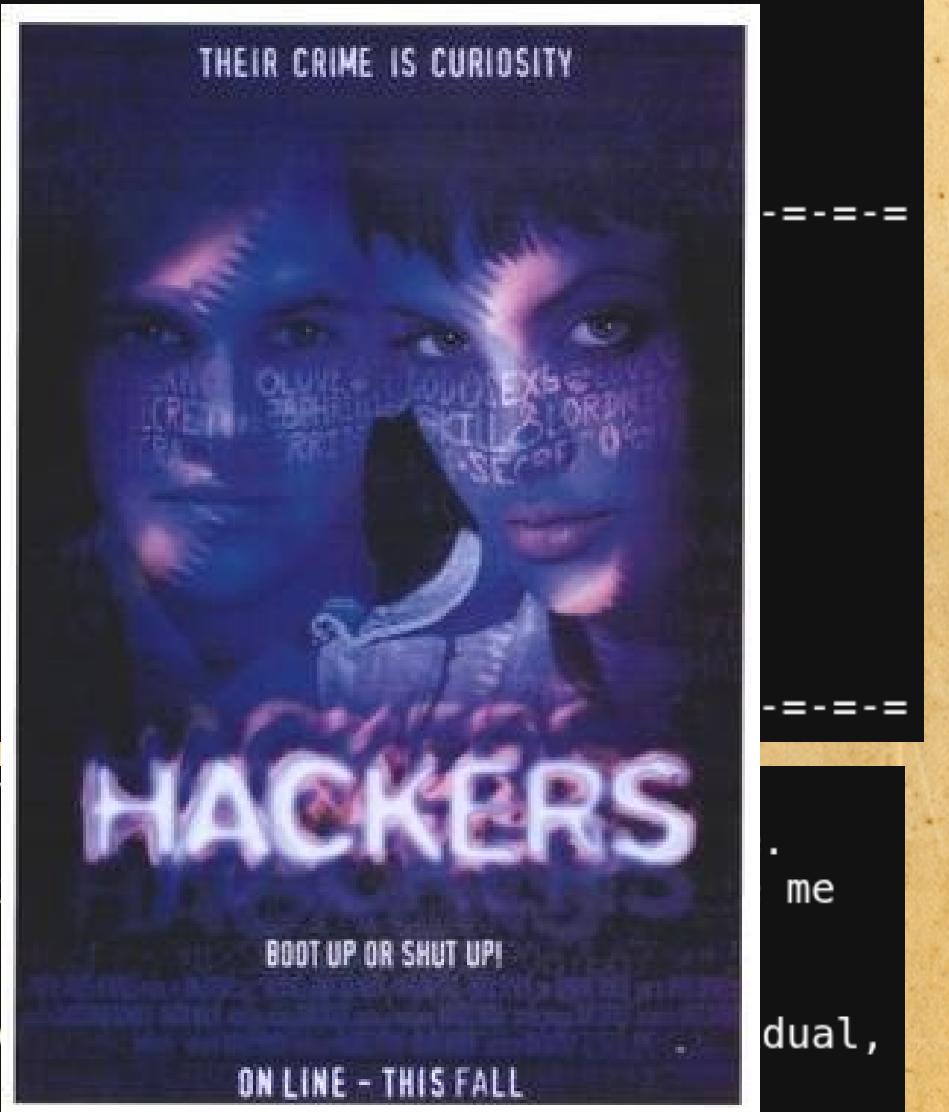
\\\The Conscience of
by

++The Mento

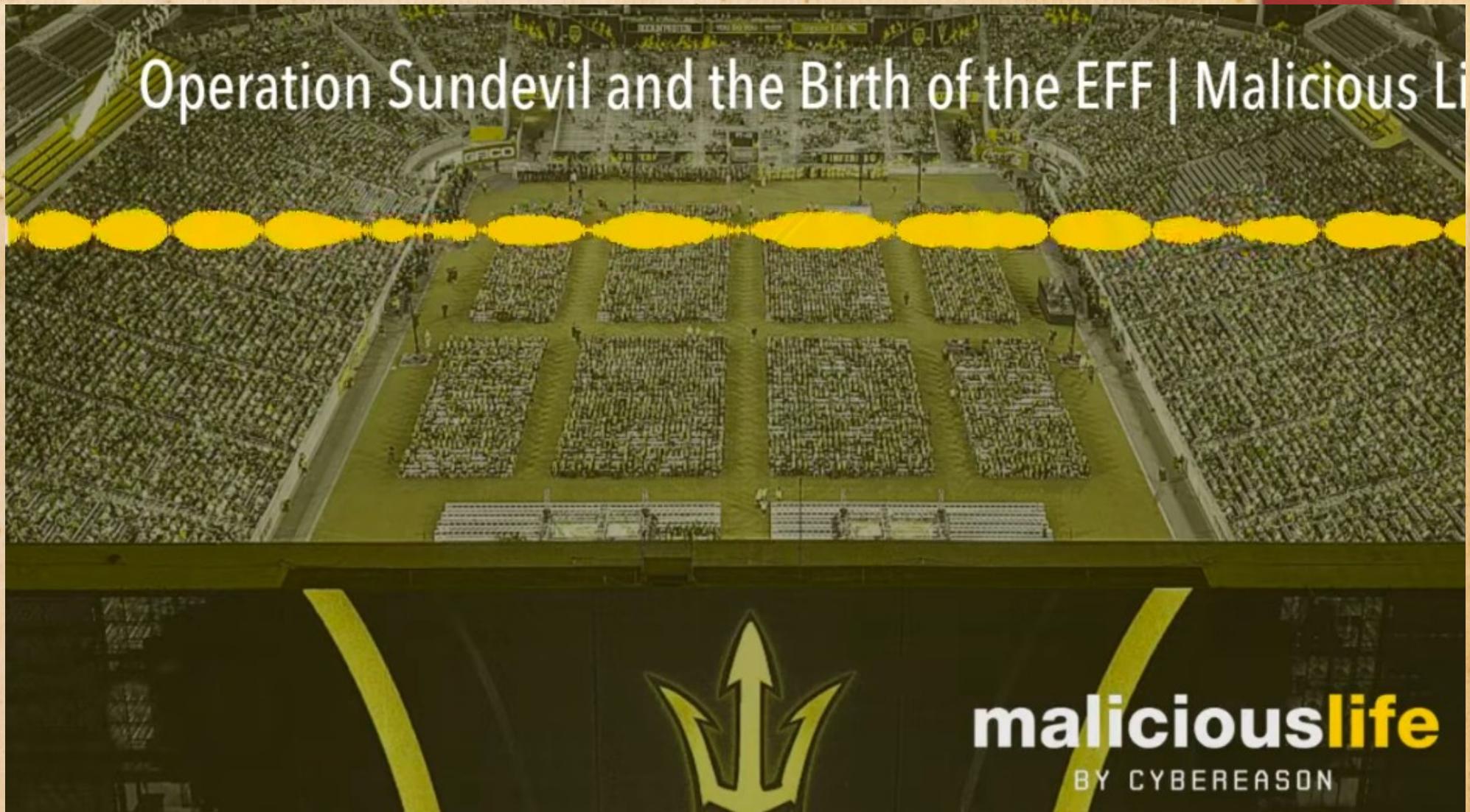
Written on Januar

=====Yes, I am a criminal. My crime is
that of judging people by what they say and
My crime is that of outsmarting you, someth-
for.

I am a hacker, and this is my manife
but you can't stop us all... after all, we'



Operation Sundevil and the Birth of the EFF | Malicious Life



maliciouslife
BY CYBEREASON

https://www.youtube.com/watch?v=Mookr_VrhyU



Thought experiment

- Imagine that people are selected in a lottery every day (could be you, a family member, a friend, a coworker, a journalist whose work you admire...)
 - All of their crypto on all of their devices is compromised or disabled in some way
 - They're not informed
 - Potential attackers *are* informed
 - Criminal organizations, competing companies, malicious individuals, former romantic partners, governments, ...



“How many of you have broken no laws this month? That's the kind of society I want to build. I want a guarantee - ***with physics and mathematics, not with laws*** - that we can give ourselves real privacy of personal communications.”

— John Gilmore



This semester is all about the relationship you (and the people and organizations you care about) have with the ISPs that connect us to the Internet.



Why study “Advanced Network Security?”

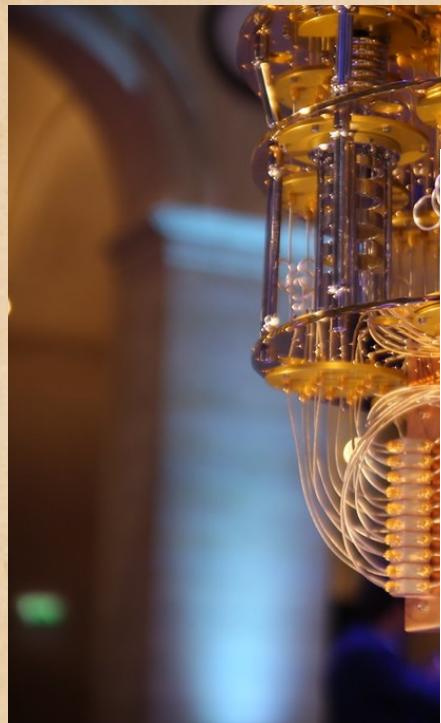


Why study “Advanced Network Security?”

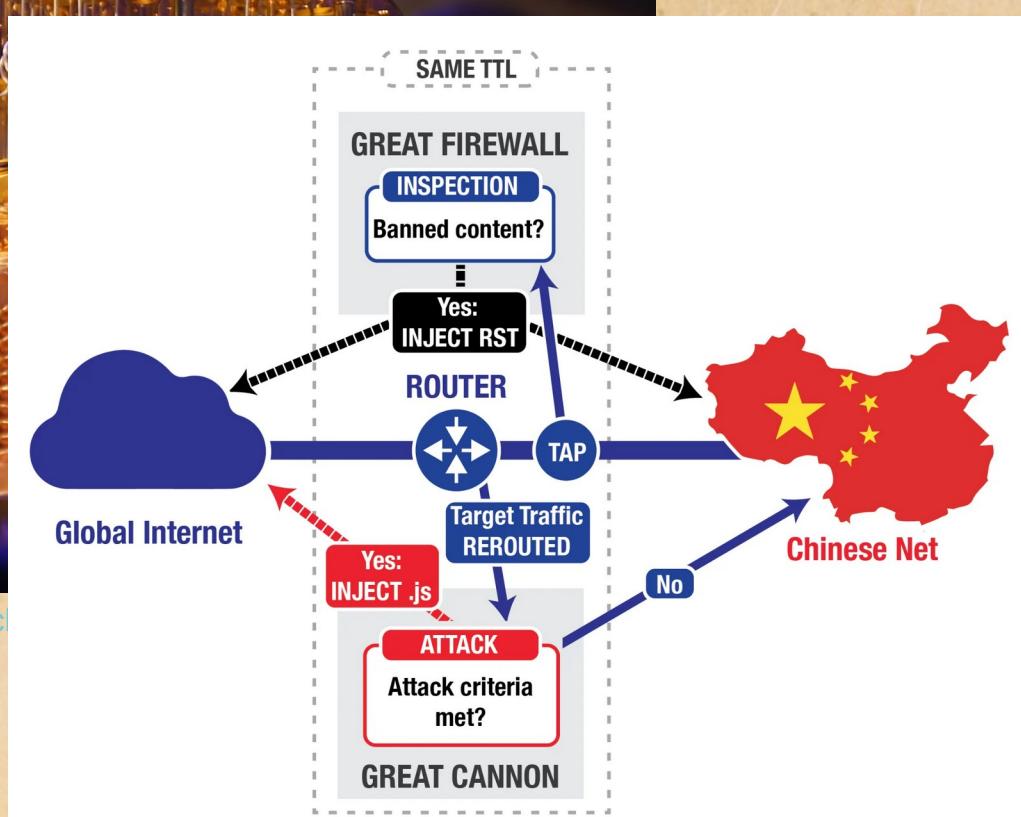


<https://www.flickr.com/photos/feuilllu/46700983592>

Why study “Advanced Network Security?”

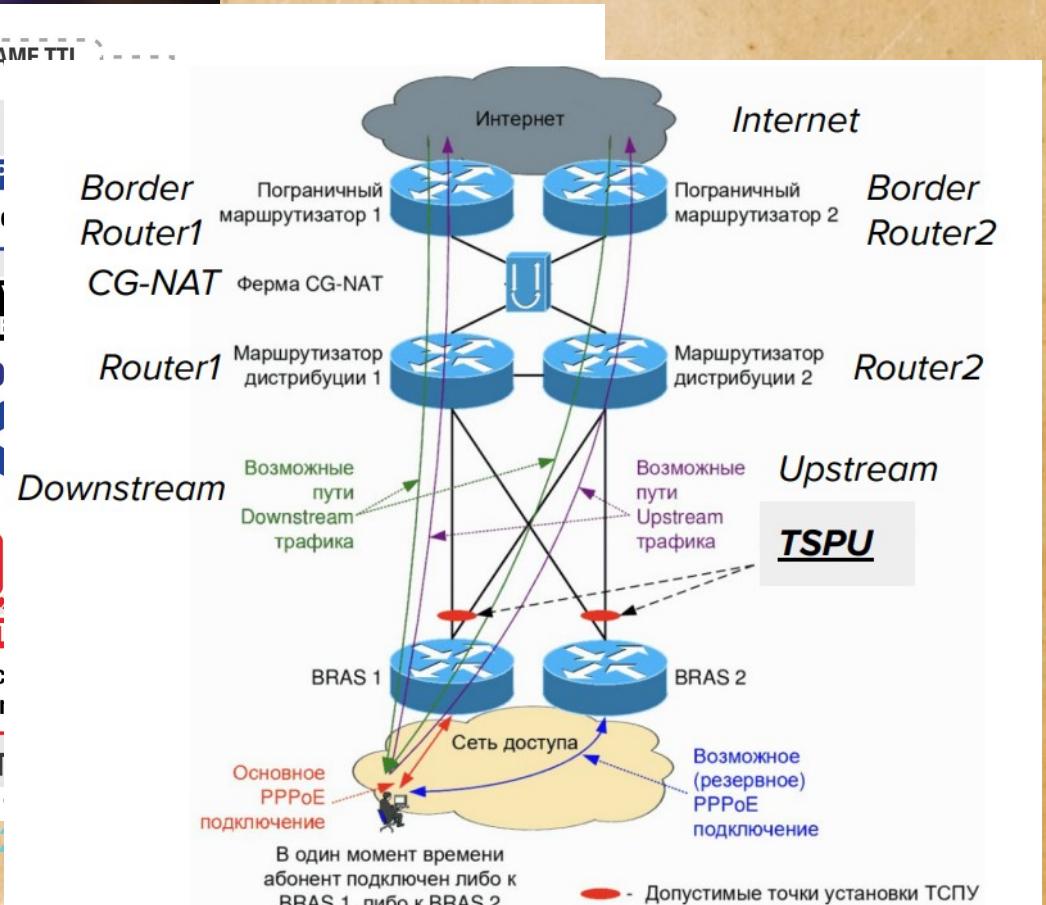
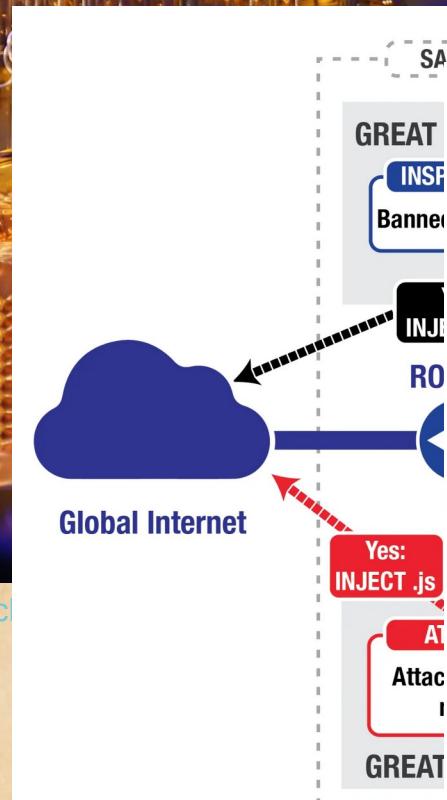
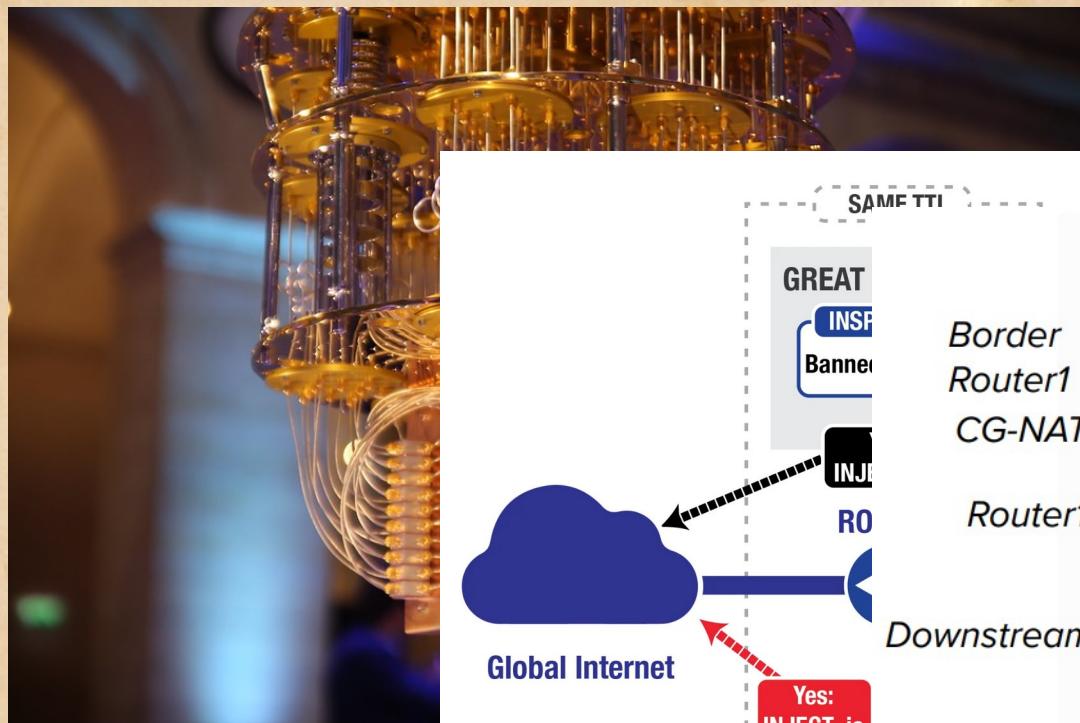


<https://www.flickr.com/photos/131000000@N00/14311300333/>



<https://citizenlab.ca/2015/04/chinas-great-cannon/>

Why study “Advanced Network Security?”



<https://ensa.fi/papers/tspu-imc22.pdf>

Russian Trusted Root CA

Identity: Russian Trusted Root CA

Verified by: Russian Trusted Root CA

Expires: 02/27/2032

▼ Details

Subject Name

C (Country): RU

O (Organization): The Ministry of Digital Development and Communications

CN (Common Name): Russian Trusted Root CA

Issuer Name

C (Country): RU

O (Organization): The Ministry of Digital Development and Communications

CN (Common Name): Russian Trusted Root CA

Issued Certificate

Version: 3

Serial Number: 10 00

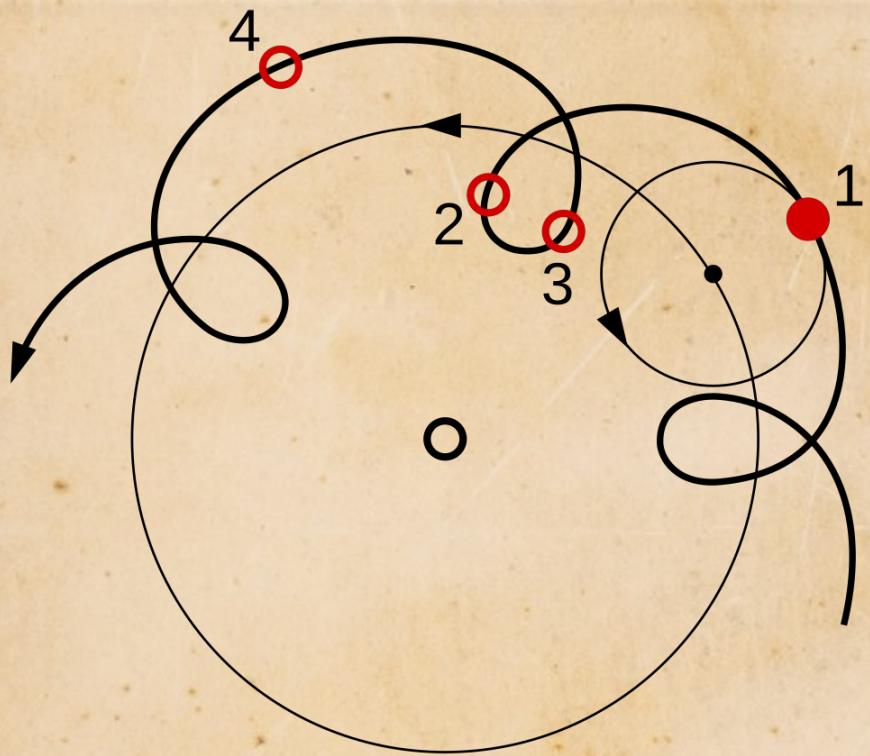
Not Valid Before: 2022-03-01

Not Valid After: 2032-02-27

Certificate Fingerprints

SHA1: 8F F9 15 CC AB 7B C1 6F 8C 5C 80 99 D5 3E 0E 11 5B 3A EC 2F

MD5: 7F BB 1F BB D1 29 47 E7 28 DC BF A4 56 8C 64 CD

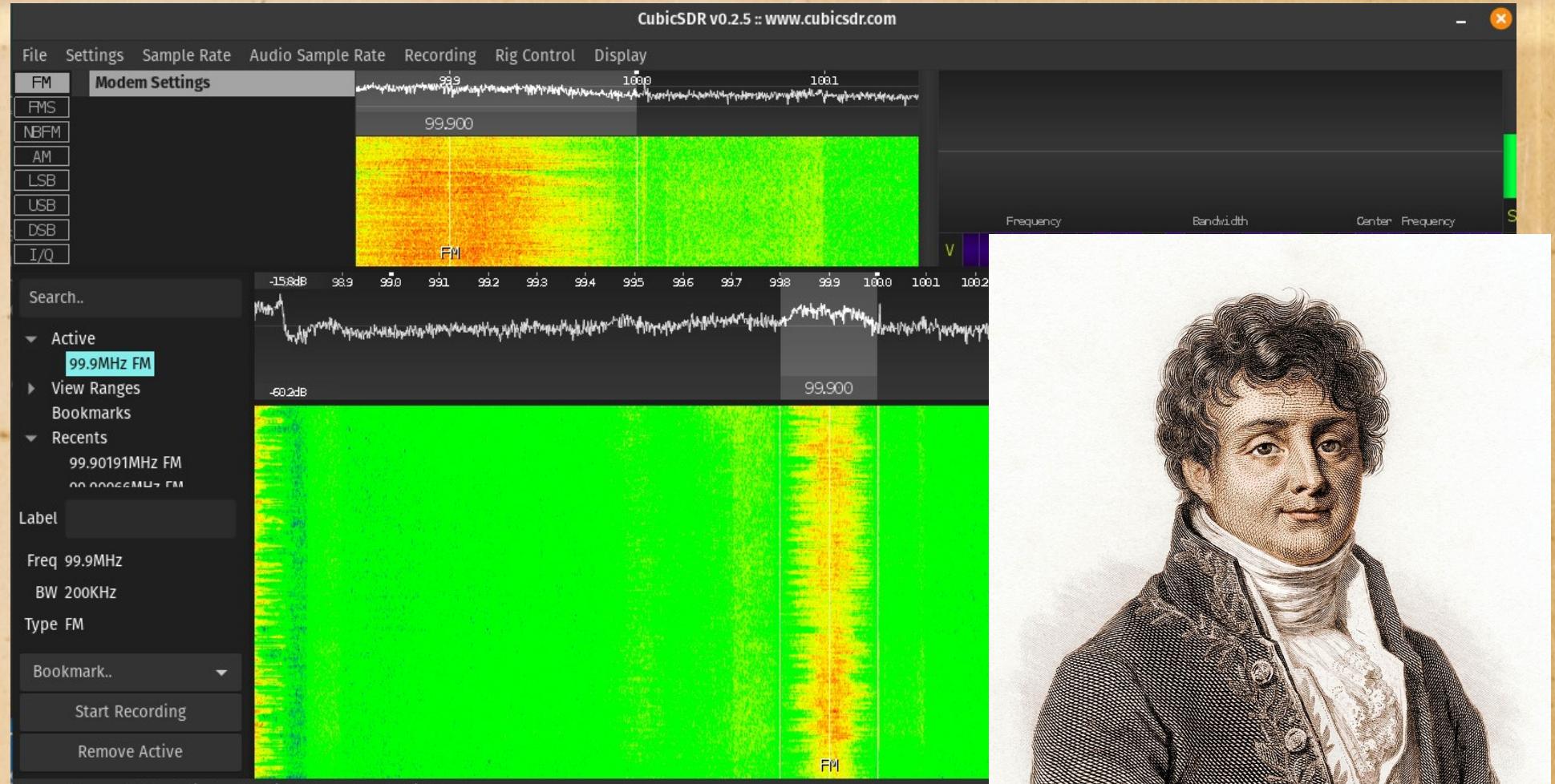


https://en.wikipedia.org/wiki/Deferent_and_epicycle

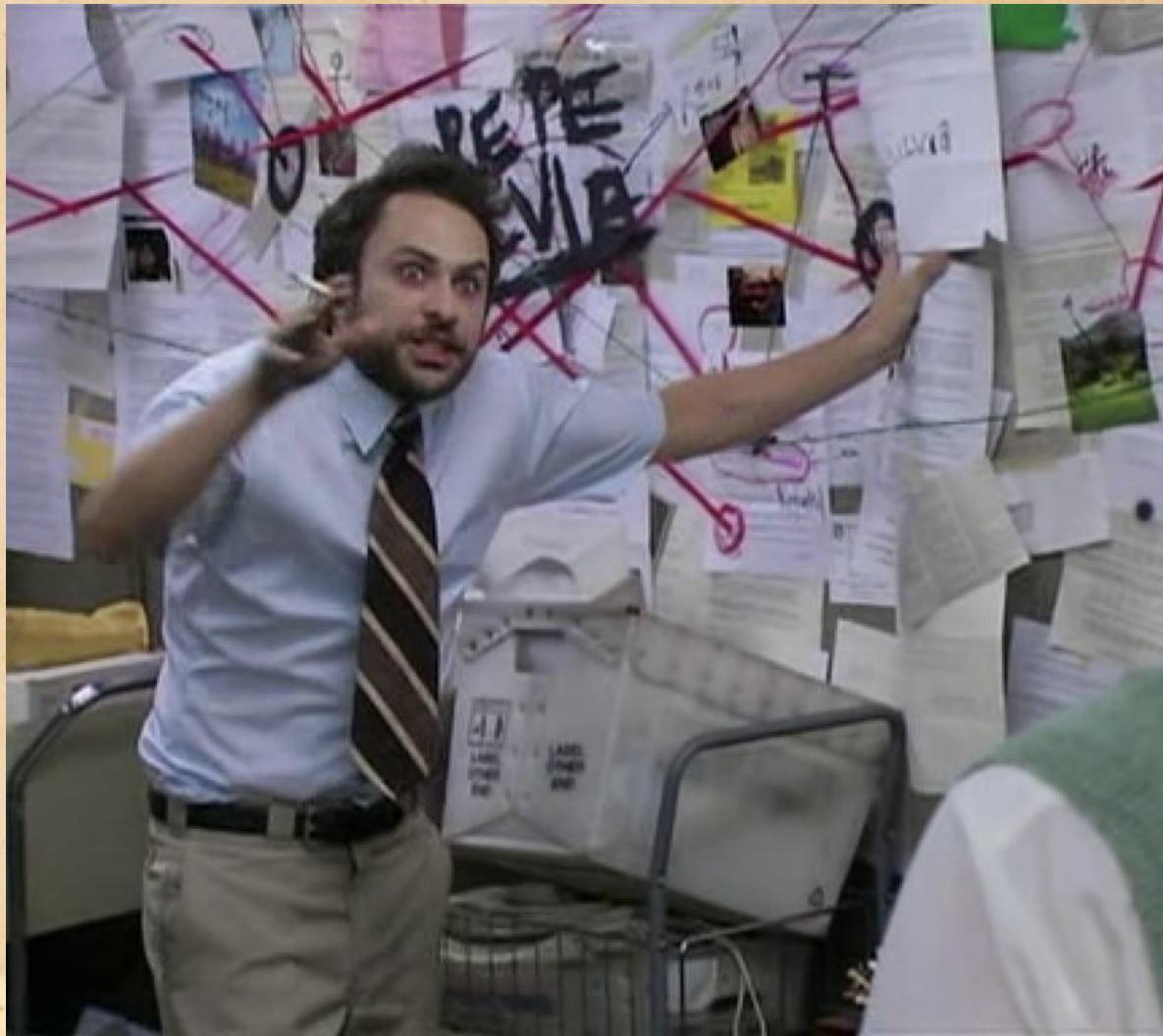


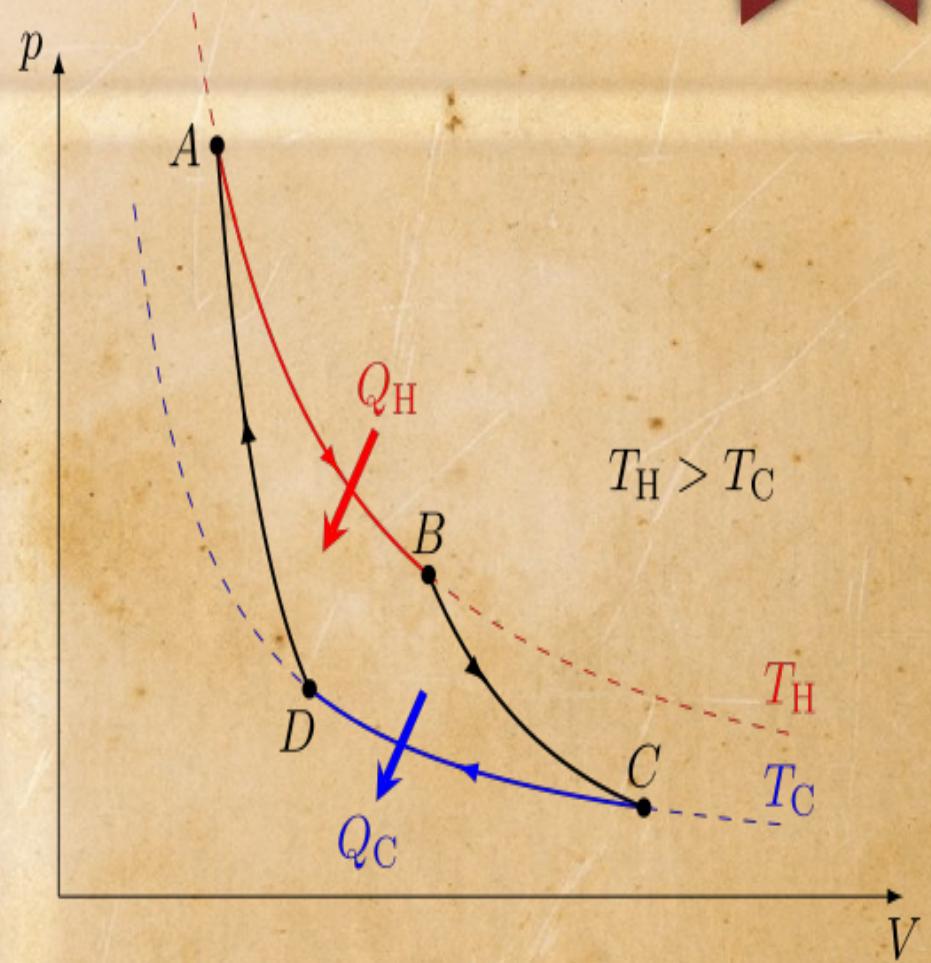
Giordano Bruno

https://en.wikipedia.org/wiki/Joseph_Fourier



Network security and French dudes who died in the early 1830s...



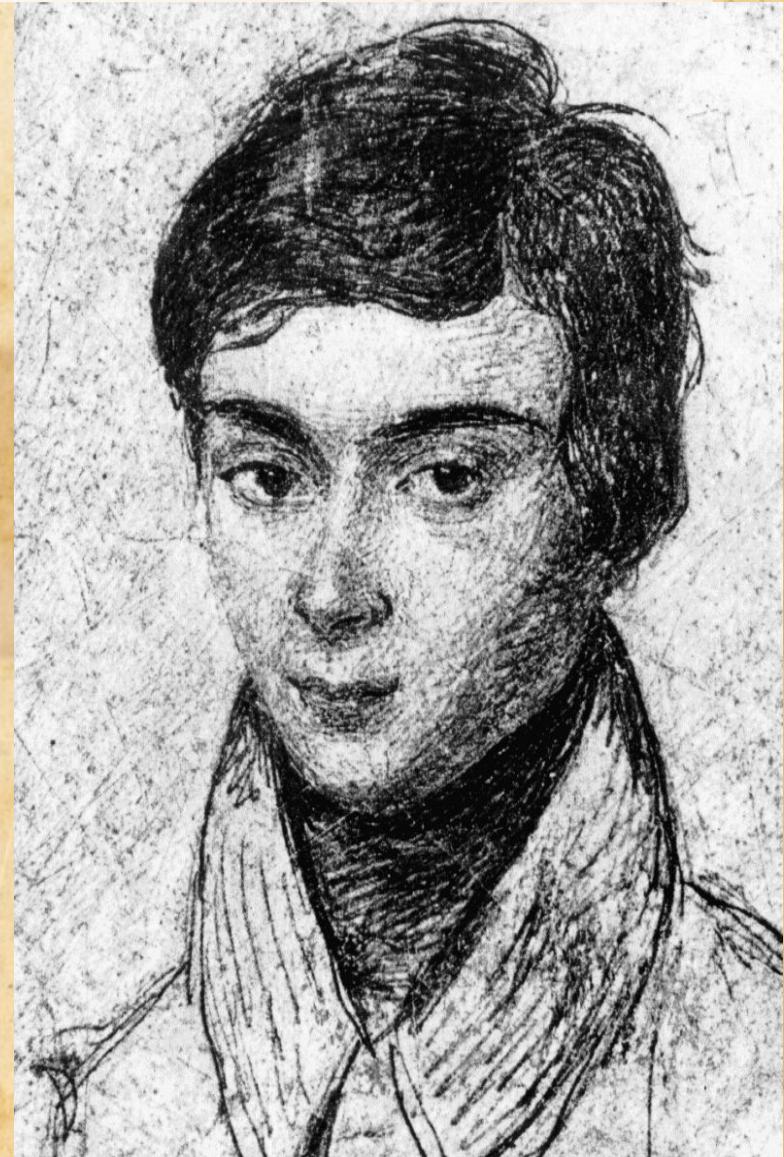


https://en.wikipedia.org/wiki/Nicolas_L%C3%A9onard_Sadi_Carnot
https://en.wikipedia.org/wiki/Carnot_heat_engine

https://en.wikipedia.org/wiki/%C3%89variste_Galois

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$\frac{a}{q}x^2 + \frac{bq+ap}{q^2}x + \frac{cq^2+bpq+ap^2}{q^3}$$

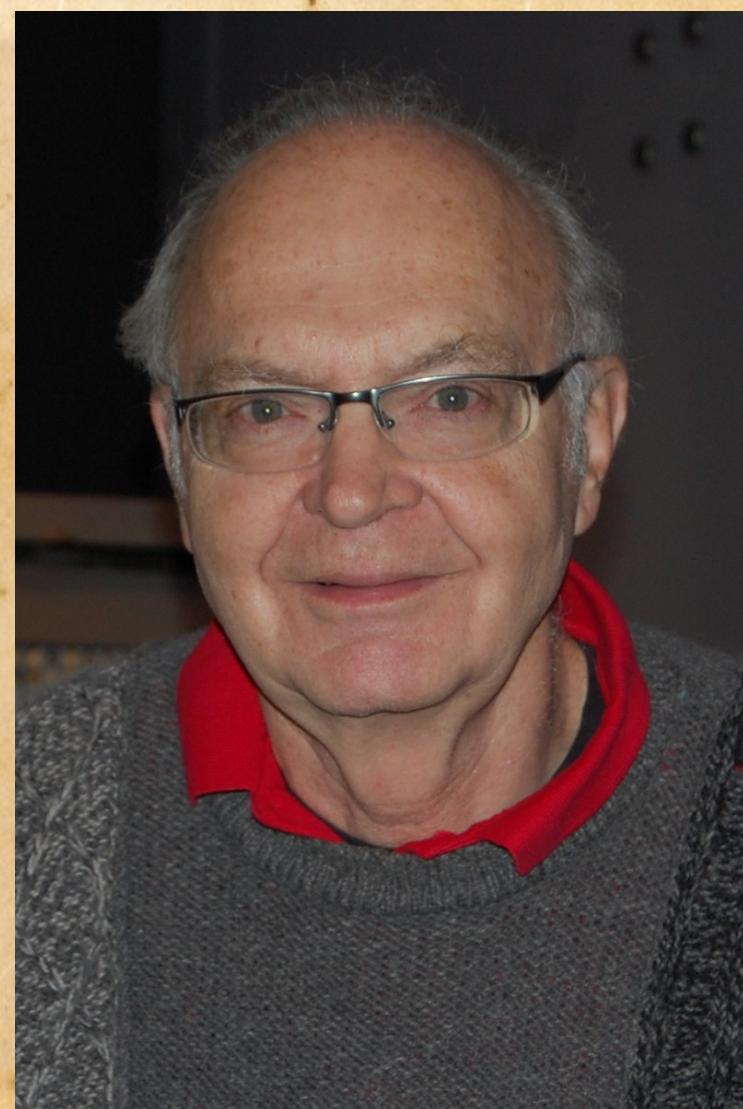
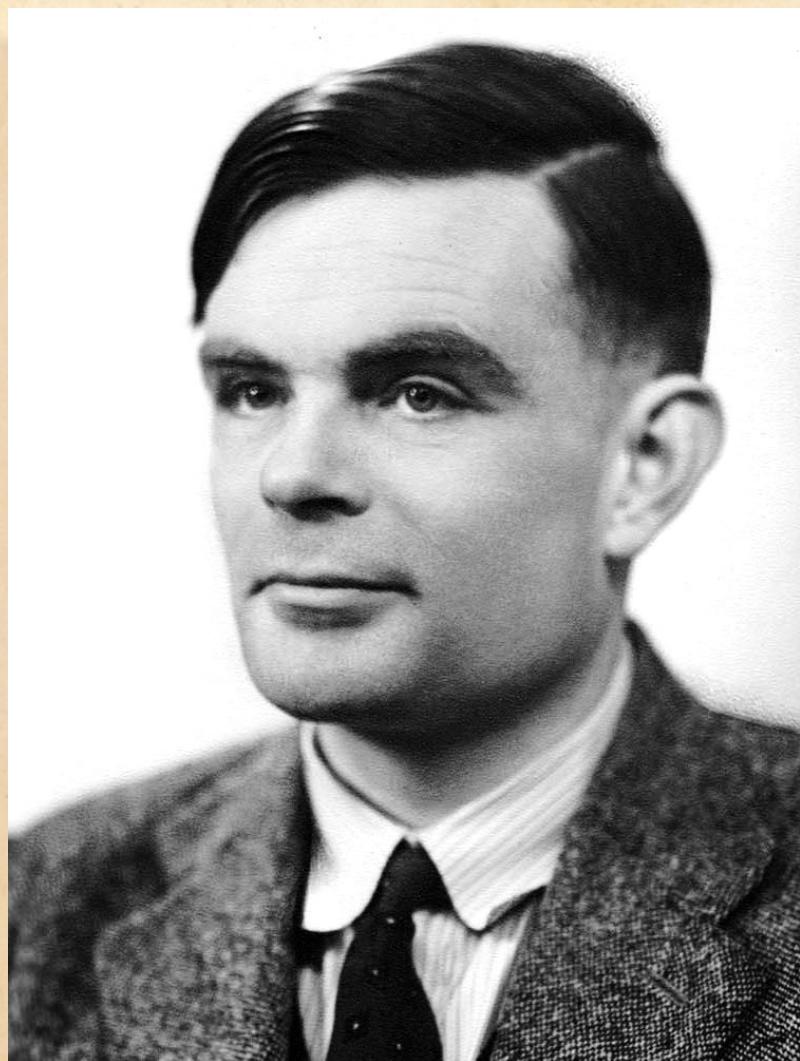


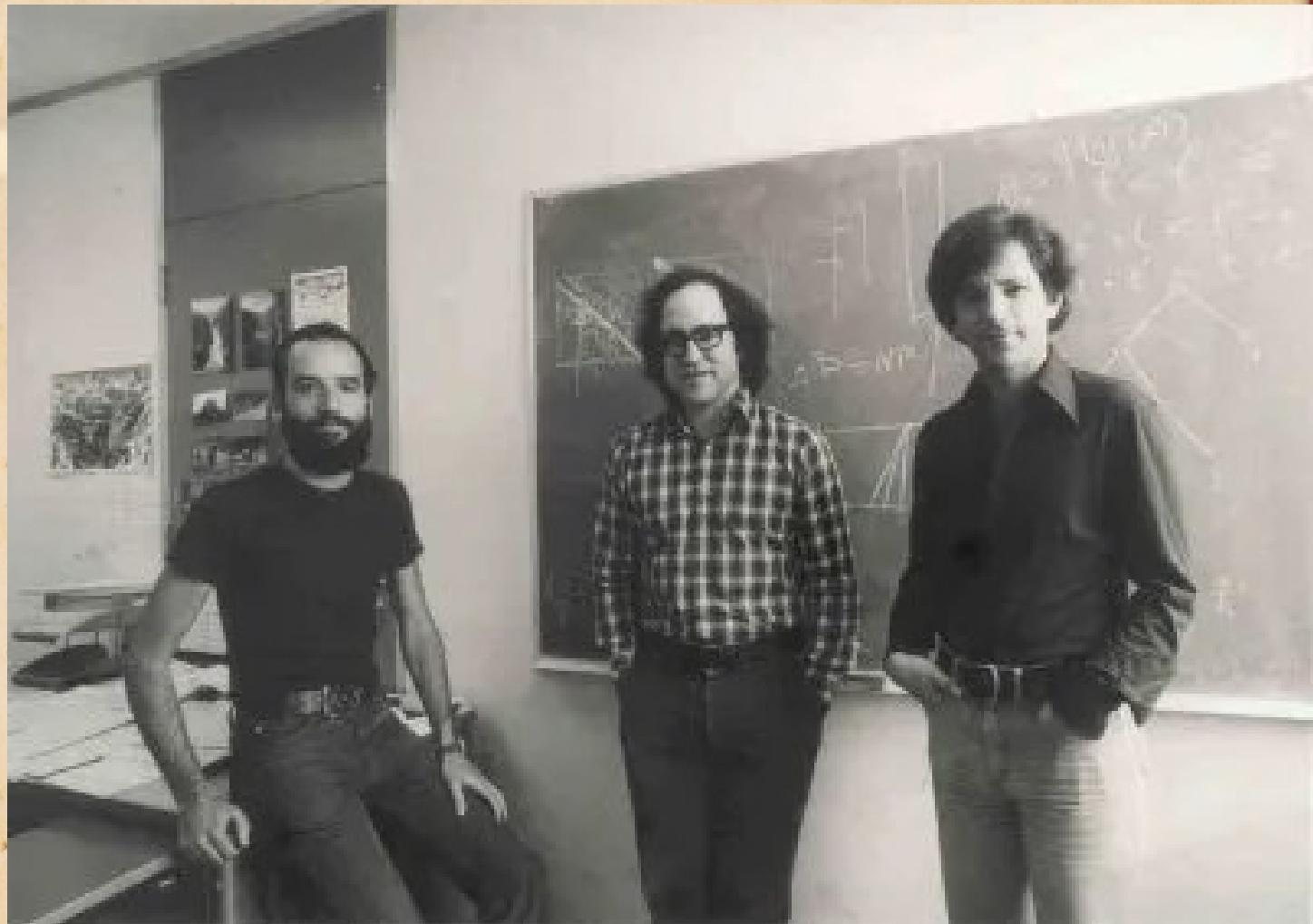


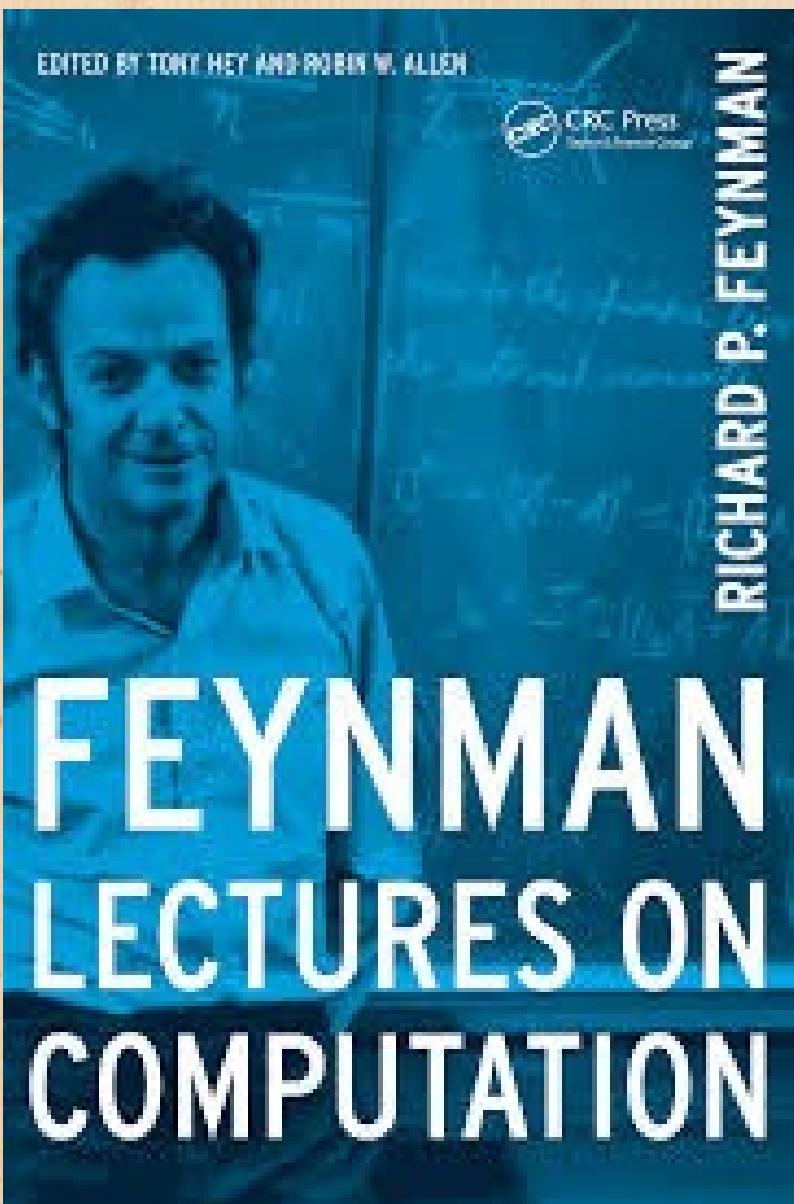
https://en.wikipedia.org/wiki/Emmy_Noether



https://en.wikipedia.org/wiki/Marie_Curie





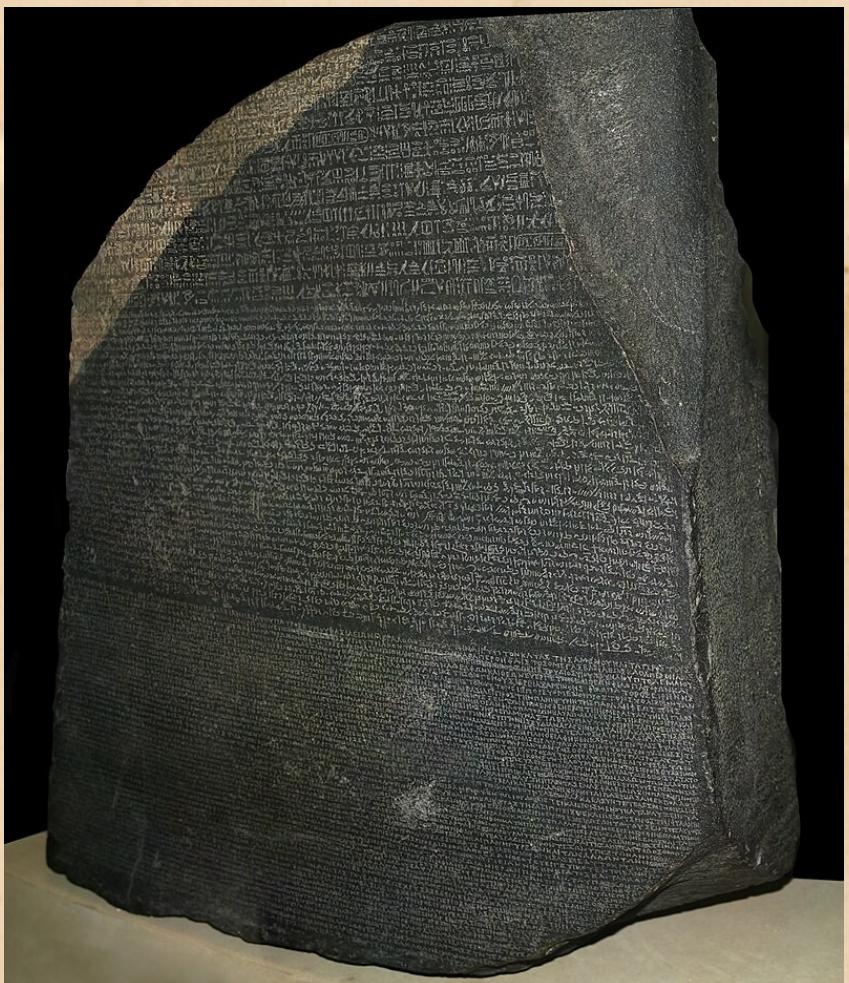


Lectures given 1983 through 1986...

"Another similar problem deals with factorization: I give you a number m , and tell you that it is the product of two primes, $m=pq$ It is possible to build our ignorance of the general solution of this mathematical problem into a ciphering message. ... The moment some clever guy cracks it ... we'd better find another one."

(page 91)

"What can be done, in these reversible quantum systems, to gain the speed available by concurrent operation has not been studied here." (page 210)

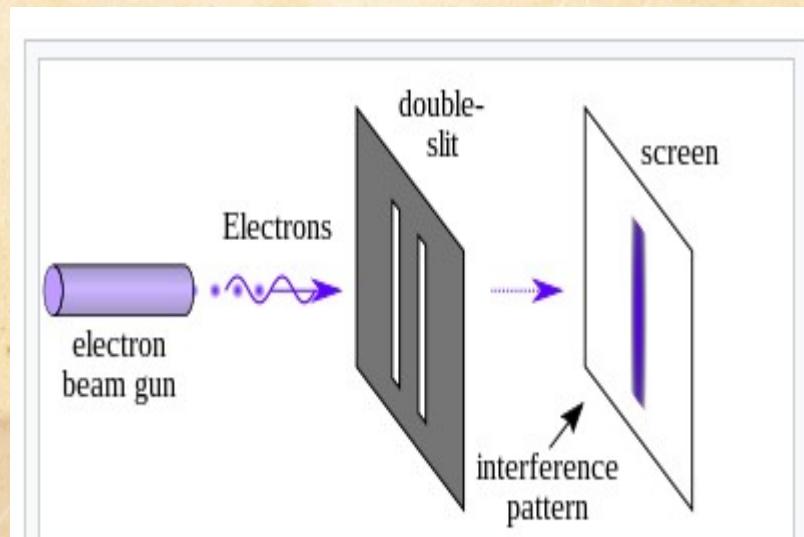


https://en.wikipedia.org/wiki/Rosetta_Stone

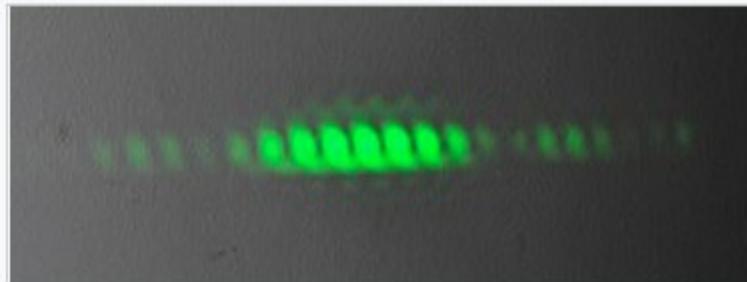
[https://en.wikipedia.org/wiki/Thomas_Young_\(scientist\)](https://en.wikipedia.org/wiki/Thomas_Young_(scientist))



https://en.wikipedia.org/wiki/Double-slit_experiment

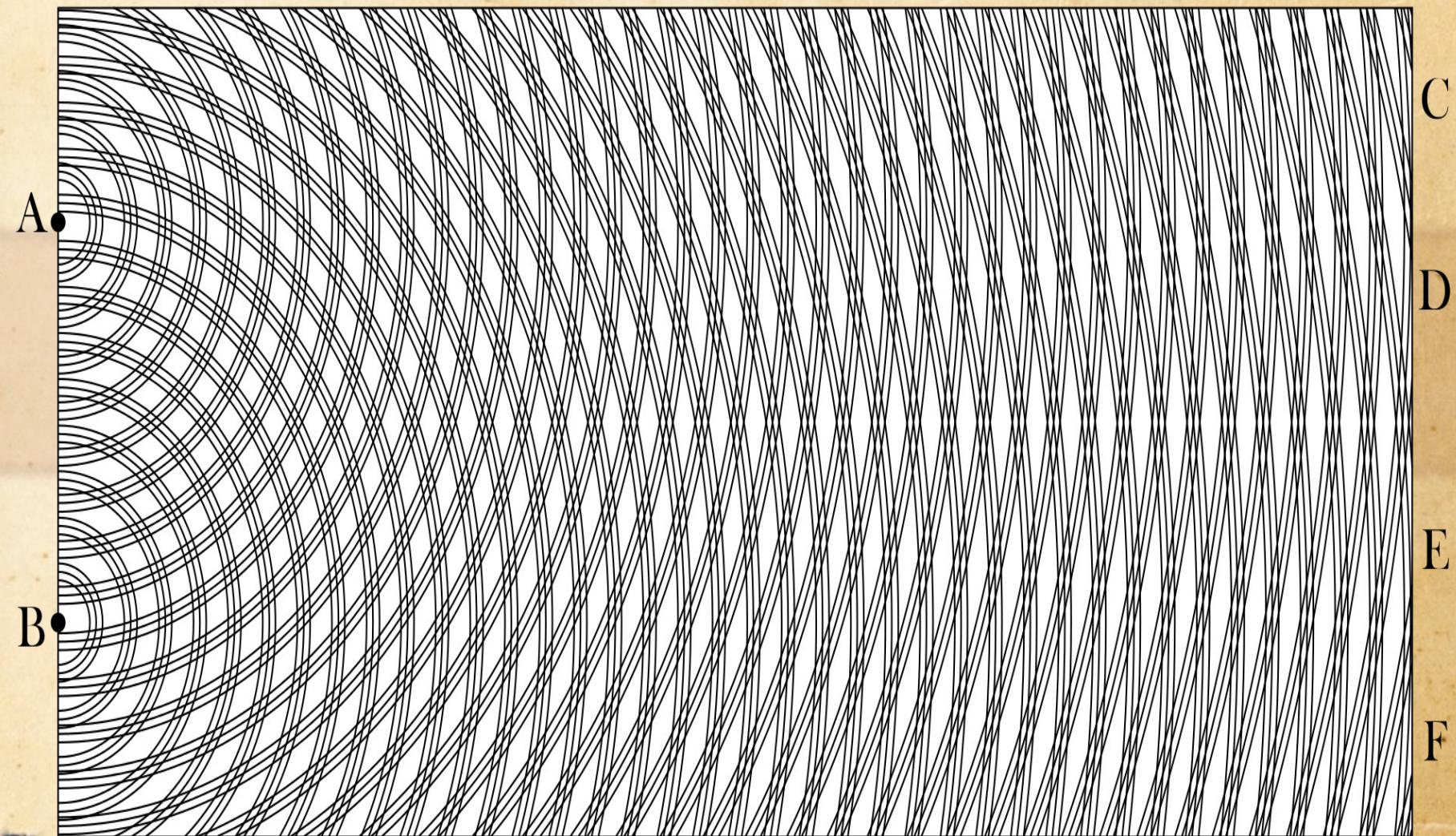


Photons or matter (like electrons) produce an interference pattern when two slits are used

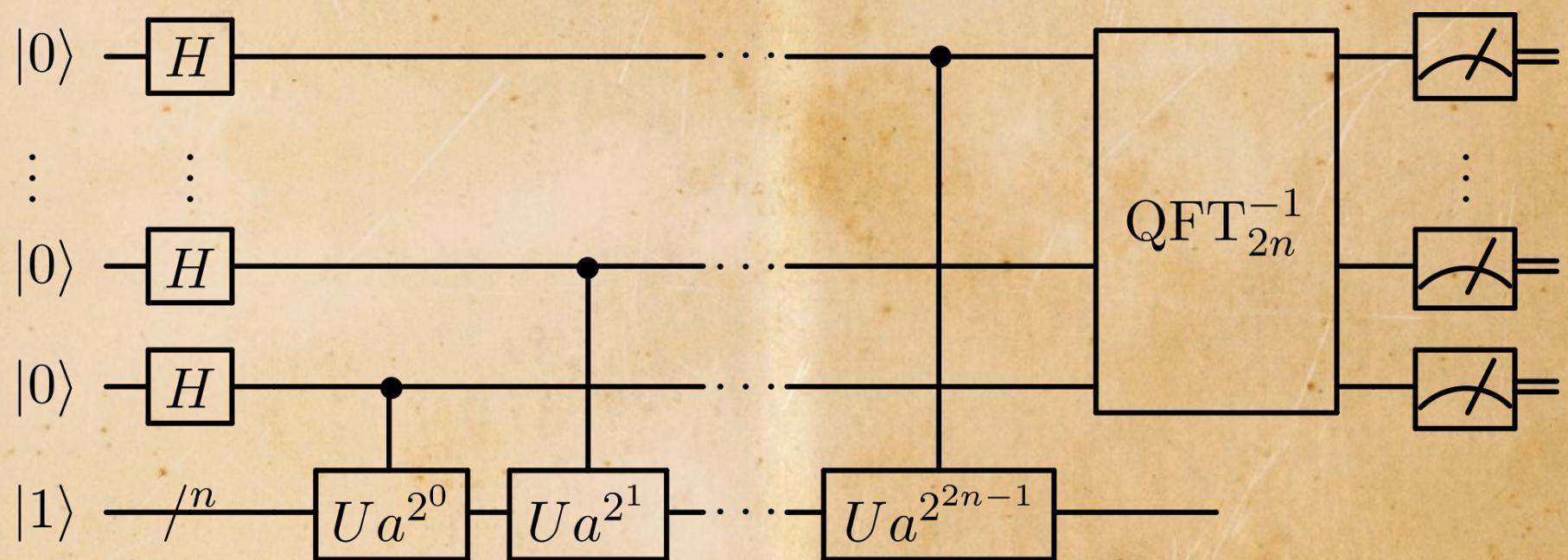


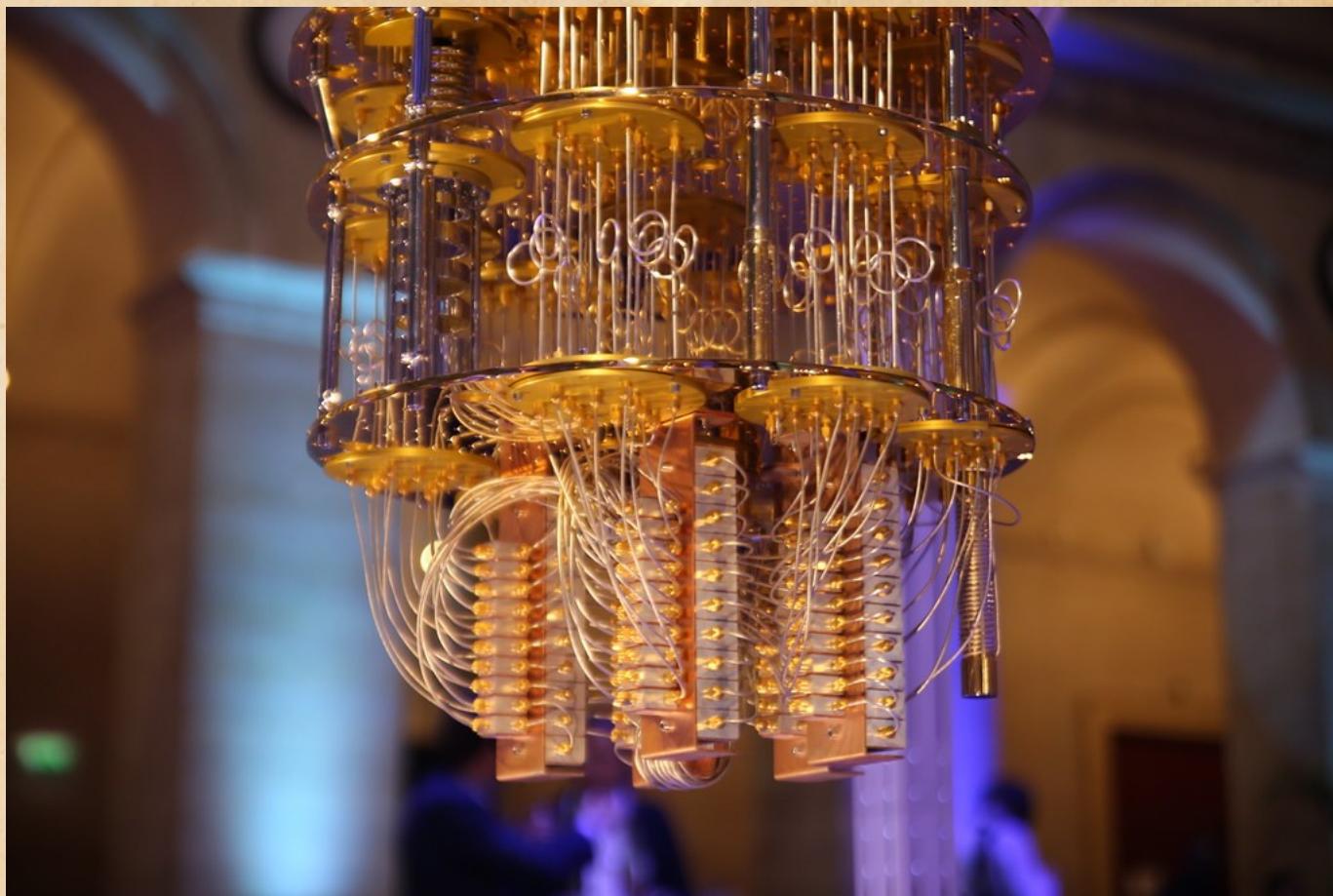
Light from a green laser passing through two slits 0.4mm wide and 0.1mm apart

https://en.wikipedia.org/wiki/Double-slit_experiment



https://en.wikipedia.org/wiki/Shor%27s_algorithm





<https://www.flickr.com/photos/feuilllu/46700983592>

Ways crypto/privacy and/or apps can be taken away

- Quantum computers
- The crypto was bad in the first place
- Security vulnerabilities render the crypto moot
- Targeted malware
- Enforced in the network
 - *E.g.*, TSPU or Great Firewall

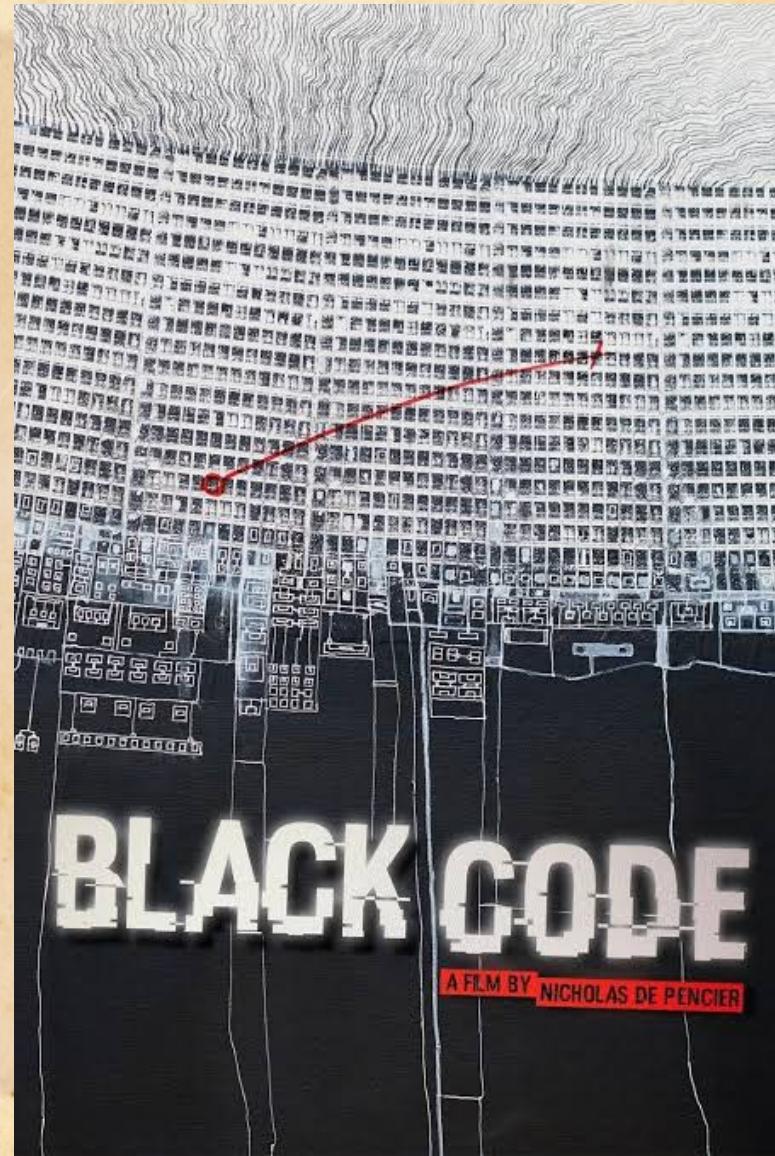
How you can help

- Hacker mentality
 - Whether or not you agree with the hacker manifesto
- Give up preconceived notions
 - “FFTs? Information theory? Ring theory? Quantum physics? I thought network security class would be practical, useful stuff.”
 - “I don’t need to know this stuff, I just want to graduate so I can fulfill my destiny of doing X.”
- Come to class, do the reading, ...

For Thursday (January 15th)...

- Read the hacker manifesto
- Listen to the Malicious Life podcast episode about Operation Sundevil







This work is licensed under
a Creative Commons Attribution-ShareAlike 3.0 Unported License.
It makes use of the works of
Kelly Loves Whales and Nick Merritt.