CSE 468 Fall 2025
Course Intro

Jed Crandall

jedimaestro@asu.edu

A bit about me and the course

- Bias is towards Internet freedom rather than traditional network security
  - Math and technical details are all the same
- Emphasis on the underlying *math* of crypto and network protocol analysis
  - Necessary because…
- I learned to program on one of these...


disk II
drive 2
disk II
drive 1
apple II

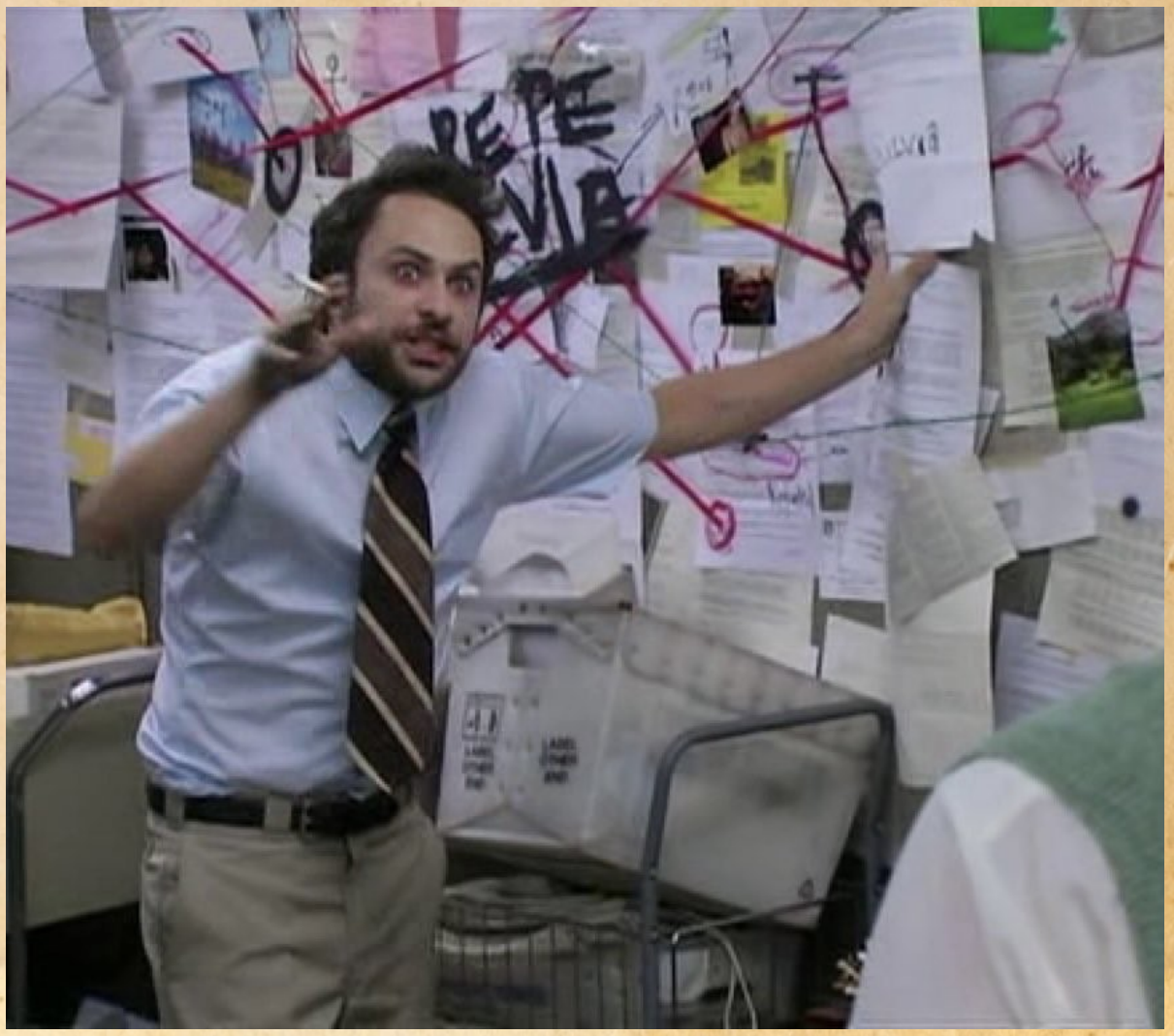
Susan O’Connor (1946-2025)


IBM
1130
IBM
GENERAL AUTOMATION
Not every minicomputer company was created by engineers
jumping ship. A marketing executive and a
Honeywell founded General

Take out your phone or laptop...

- Is it safe to use the network you're connected to? Is your Internet traffic encrypted to keep it safe? Will the crypto last 10 years?
- What are the apps you couldn't live without? How easily could your Internet Service Provider (ISP) take them away?
- Do you use good passwords? Are your accounts safe? Could there be malware on your phone?

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



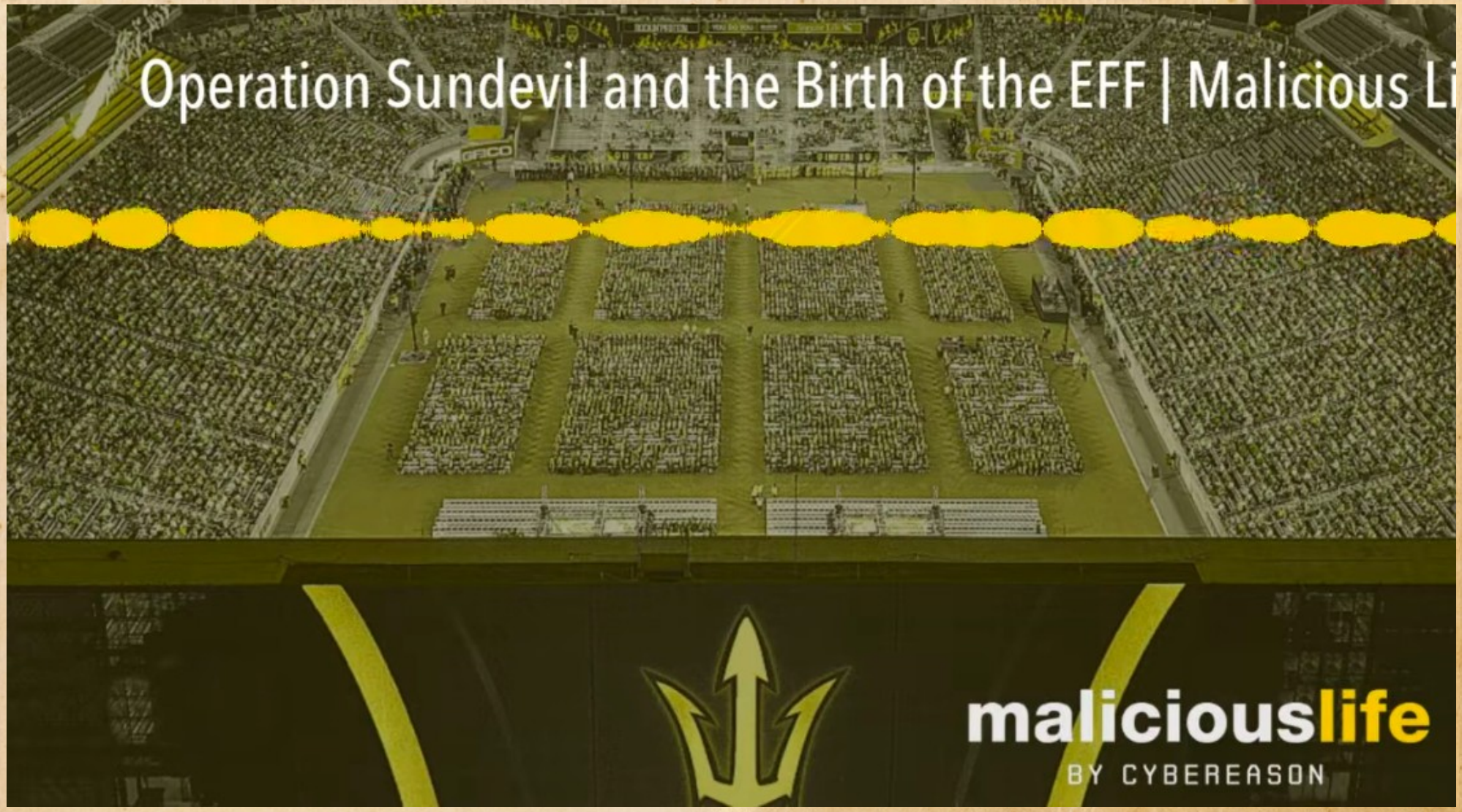
“How many of you have broken no laws this month? That's the kind of society I want to build. I want a guarantee - ***with physics and mathematics, not with laws*** - that we can give ourselves real privacy of personal communications.”

— John Gilmore

My goal: no cop outs in the way I teach this class…

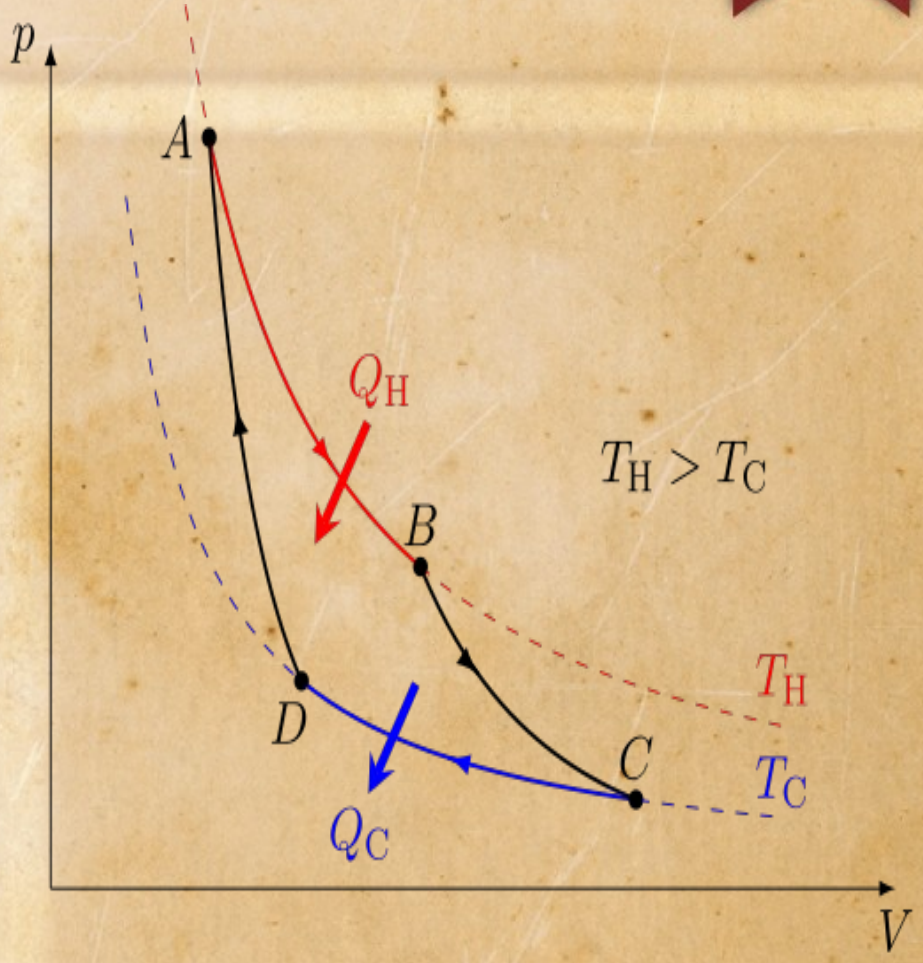
- If there are bits set in a particular way for cybersecurity reasons in a packet capture (PCAP), I hope to explain the math and physics behind why.
  - Especially if it's all about to change.
- If I say that a Deep Packet Inspection (DPI) machine can't handle a specific rate of traffic, I should be able to back that up with math and science.
- If I claim that you can't write a program to detect all possible malware, you should expect me to prove it.

Close your eyes and imagine that you’re still in your bed, sleeping, and haven’t woken up and come to class yet...



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

The kinds of things we’re going to learn about this semester have gotten people imprisoned, tortured, and killed.



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

Entropy

- Statistical foundation by Clausius, Gibbs, Boltzmann, Maxwell, Planck, *etc.*

$$S = k \log W$$

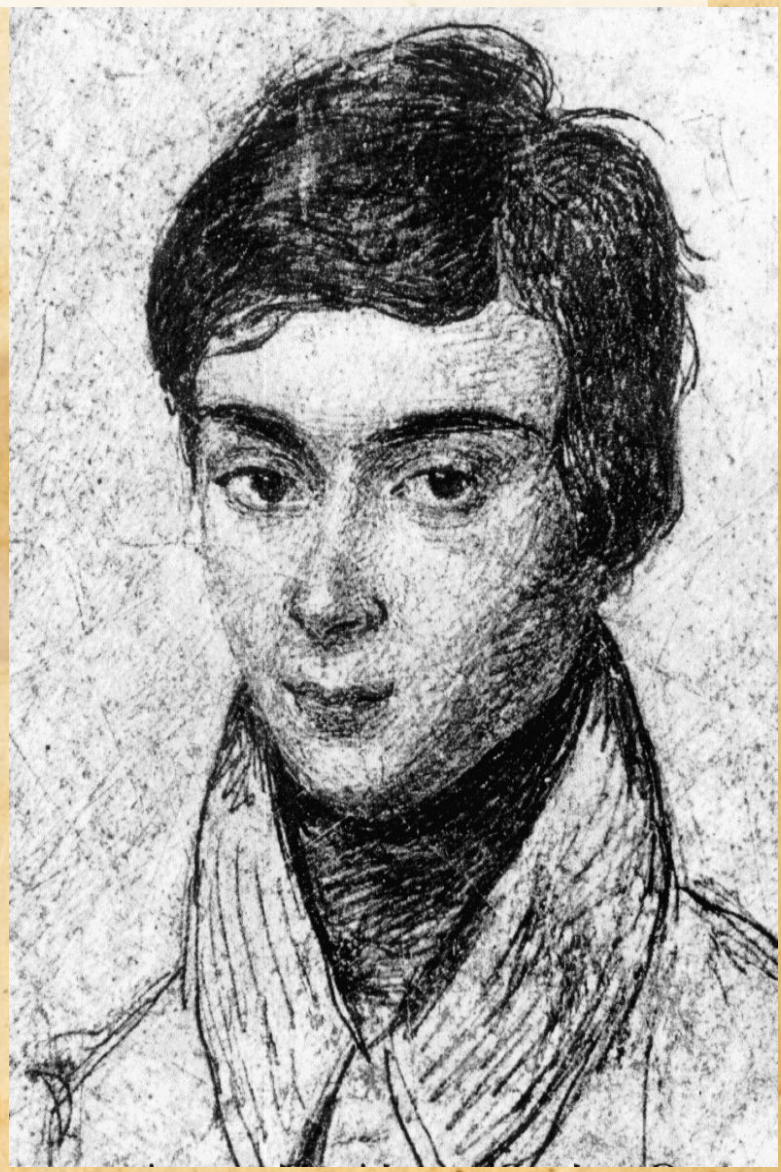
- Directly inspired the name of entropy in Shannon's **information theory:**

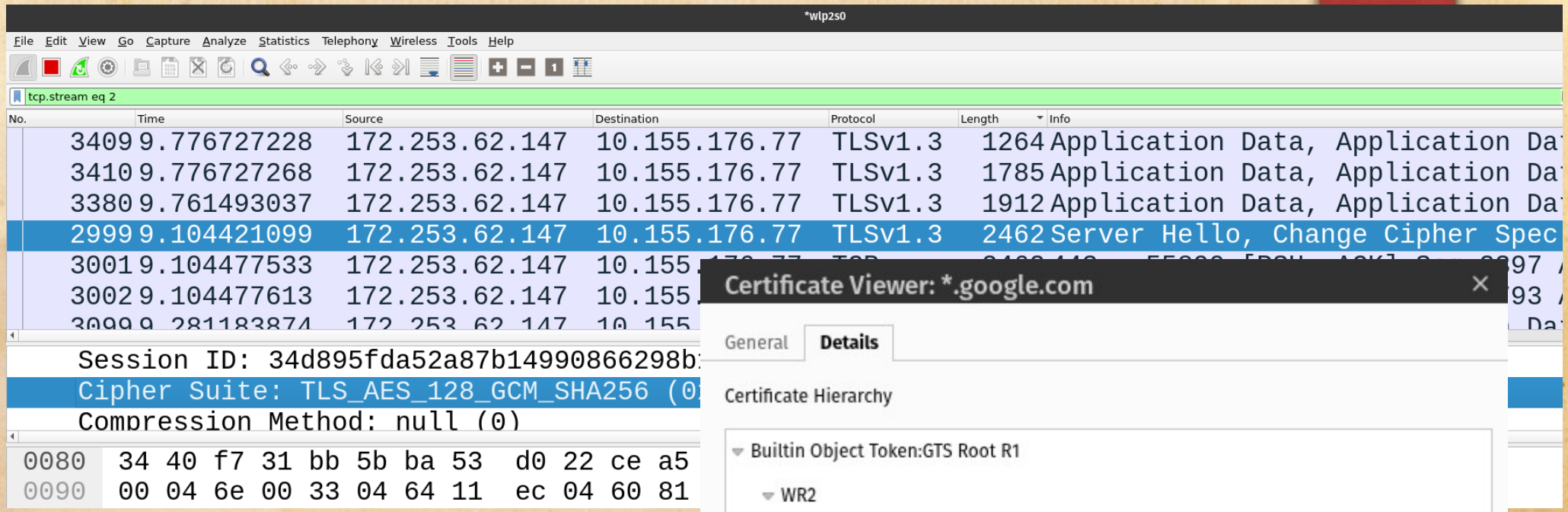
$$H = -\sum_i p_i \log_2(p_i)$$

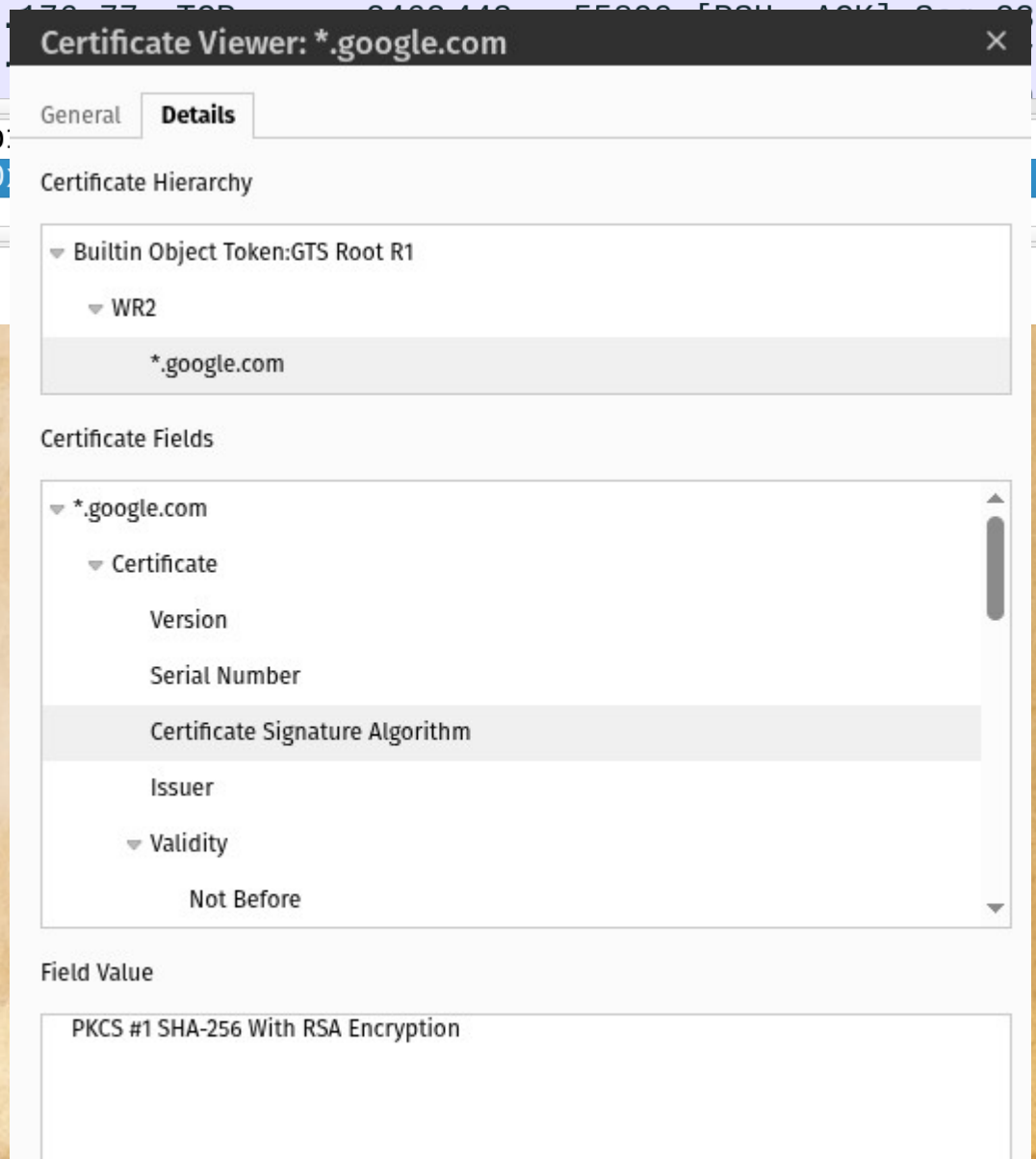
https://en.wikipedia.org/wiki/%C3%89variste_Galois

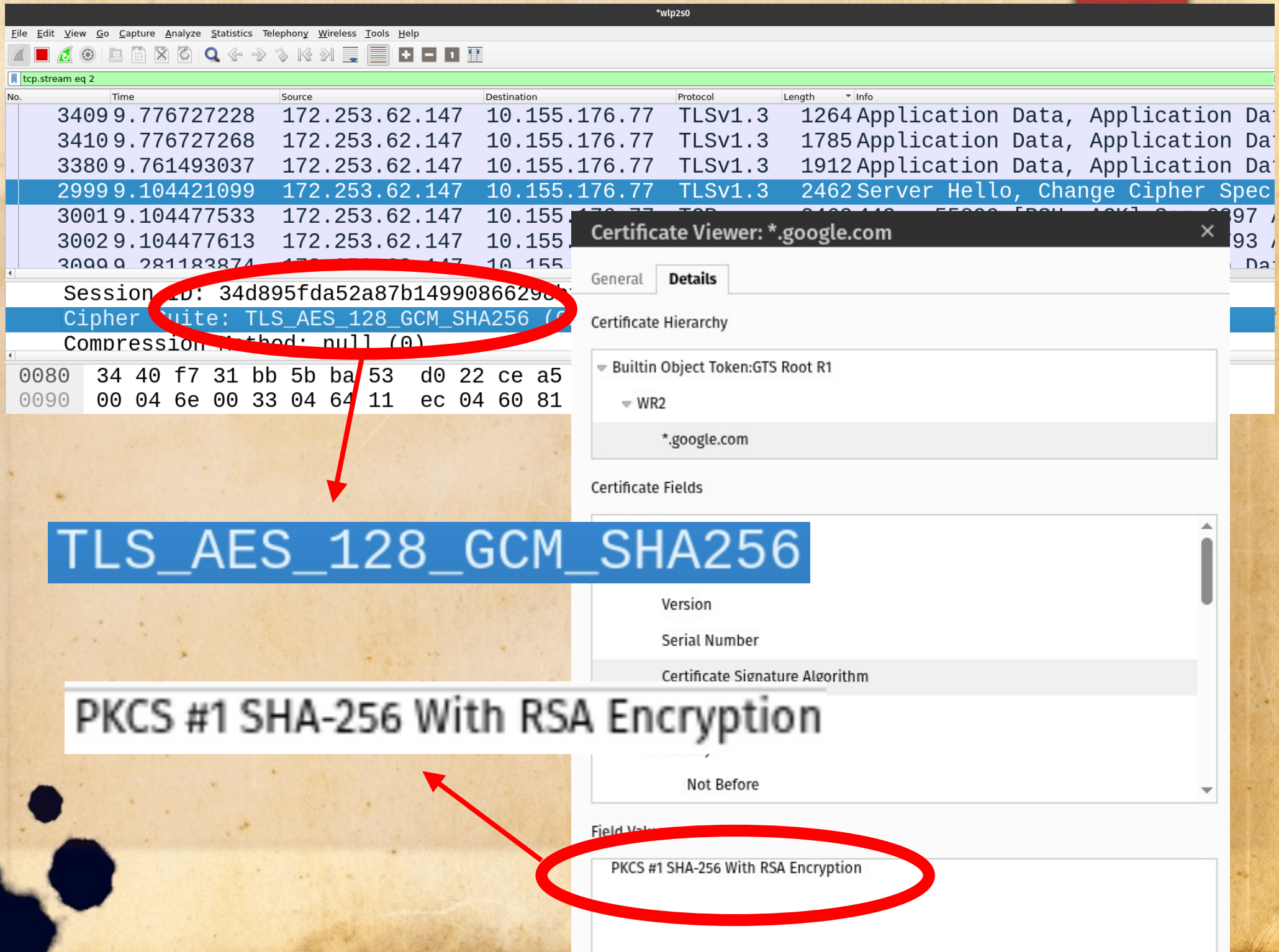
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

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

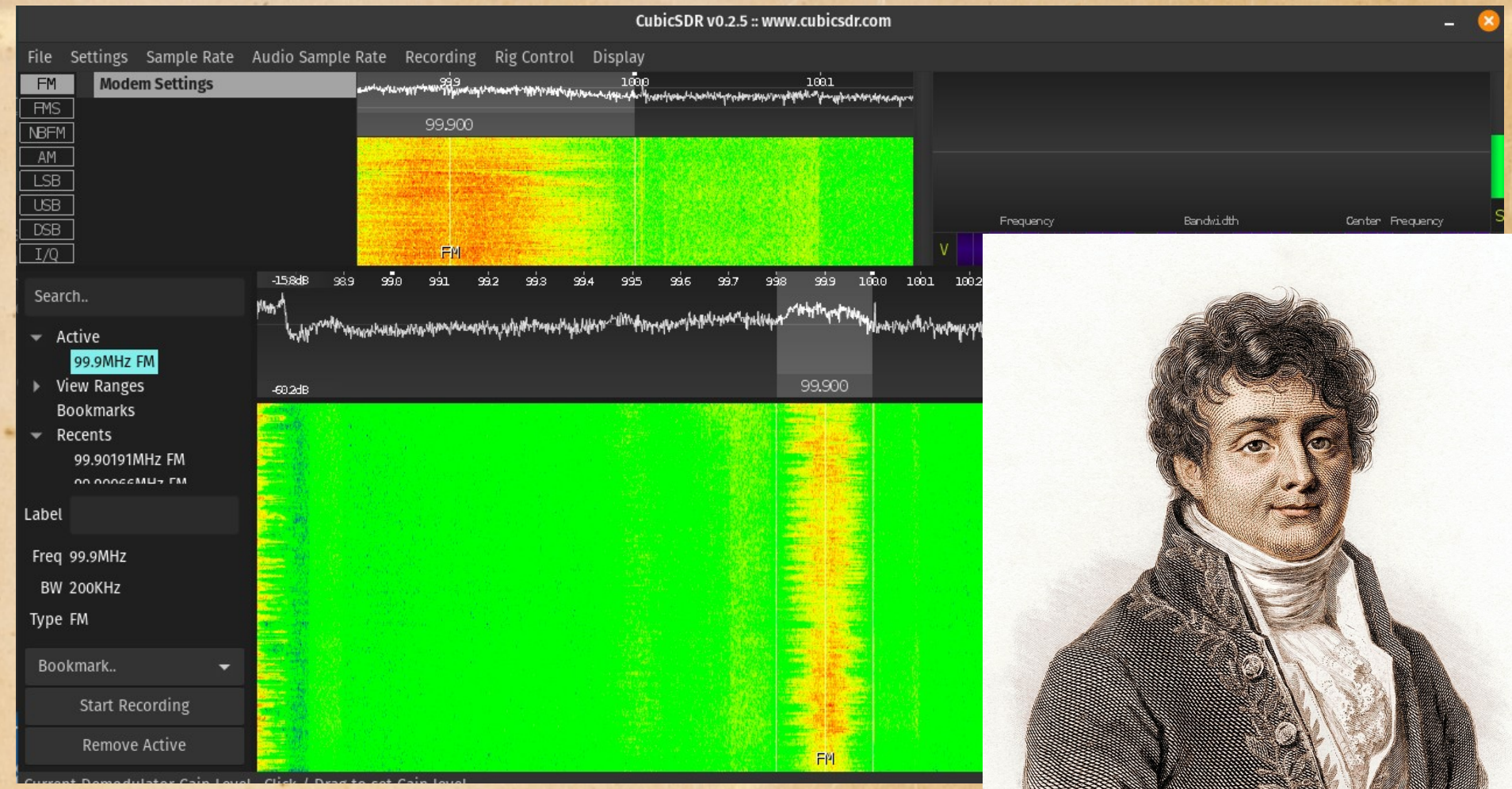



*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2
No. Time Source Destination Protocol Length Info
3409 9.776727228 172.253.62.147 10.155.176.77 TLSv1.3 1264 Application Data, Application Da
3410 9.776727268 172.253.62.147 10.155.176.77 TLSv1.3 1785 Application Data, Application Da
3380 9.761493037 172.253.62.147 10.155.176.77 TLSv1.3 1912 Application Data, Application Da
2999 9.104421099 172.253.62.147 10.155.176.77 TLSv1.3 2462 Server Hello, Change Cipher Spec
3001 9.104477533 172.253.62.147
3002 9.104477613 172.253.62.147
Session ID: 34d895fda52a87b14990866298b
Cipher Suite: TLS_AES_128_GCM_SHA256 (0
Compression Method: null (0)
0080 34 40 f7 31 bb 5b ba 53 d0 22 ce a5
0090 00 04 6e 00 33 04 64 11 ec 04 60 81


Certificate Viewer: *.google.com
General
Details
Certificate Hierarchy
Builtin Object Token:GTS Root R1
WR2
*.google.com
Certificate Fields
*.google.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
PKCS #1 SHA-256 With RSA Encryption


*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 2
No. Time Source Destination Protocol Length Info
3409 9.776727228 172.253.62.147 10.155.176.77 TLSv1.3 1264 Application Data, Application Da
3410 9.776727268 172.253.62.147 10.155.176.77 TLSv1.3 1785 Application Data, Application Da
3380 9.761493037 172.253.62.147 10.155.176.77 TLSv1.3 1912 Application Data, Application Da
2999 9.104421099 172.253.62.147 10.155.176.77 TLSv1.3 2462 Server Hello, Change Cipher Spec
3001 9.104477533 172.253.62.147
3002 9.104477613 172.253.62.147
Session ID: 34d895fda52a87b14990866
Cipher Suite: TLS_AES_128_GCM_SHA256
Compression Method: null (0)
0080 34 40 f7 31 bb 5b ba 53 d0 22 ce a5
0090 00 04 6e 00 33 04 64 11 ec 04 60 81
Certificate Viewer: *.google.com
General
Details
Certificate Hierarchy
Builtin Object Token:GTS Root R1
WR2
*.google.com
Certificate Fields
Version
Serial Number
Certificate Signature Algorithm
Not Before
PKCS #1 SHA-256 With RSA Encryption
TLS_AES_128_GCM_SHA256
PKCS #1 SHA-256 With RSA Encryption

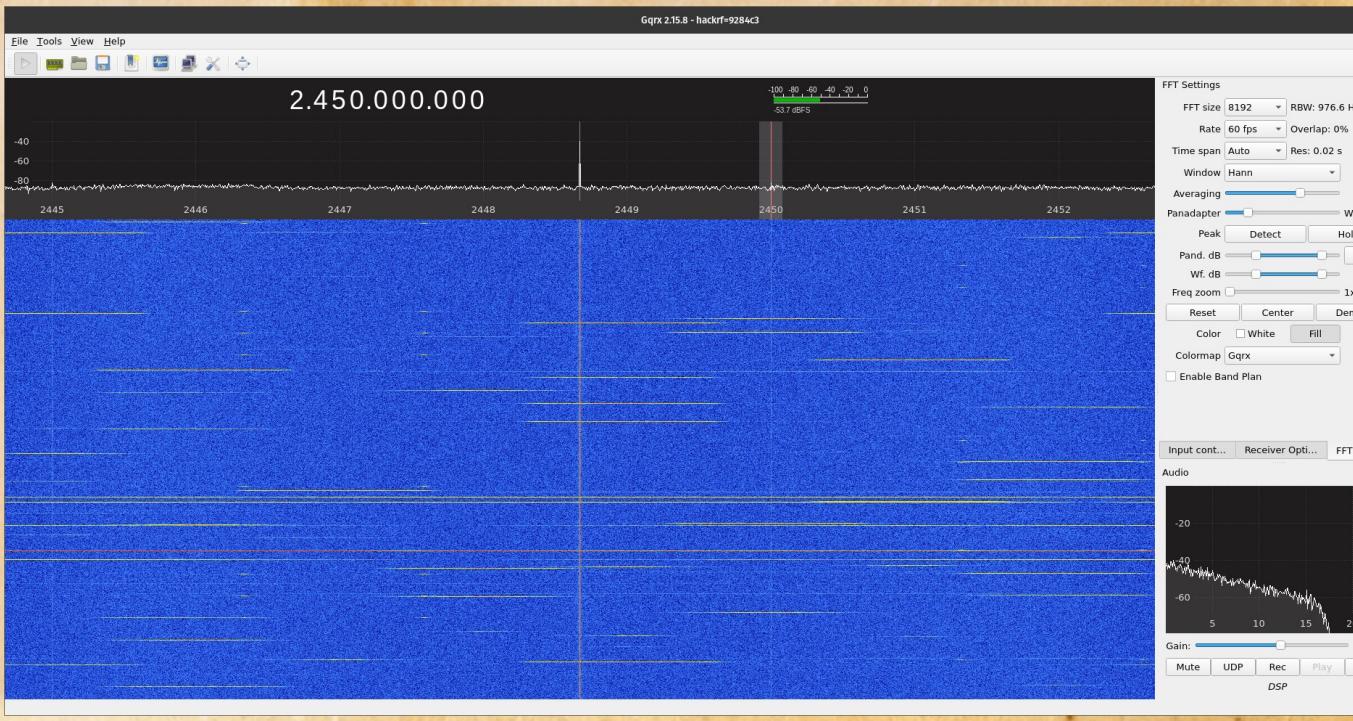
https://en.wikipedia.org/wiki/Joseph_Fourier



Coincidence?

- Carnot died in 1832, aged 36
- Gallois died in 1832, aged 20
- Fourier died in 1830, aged 62

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



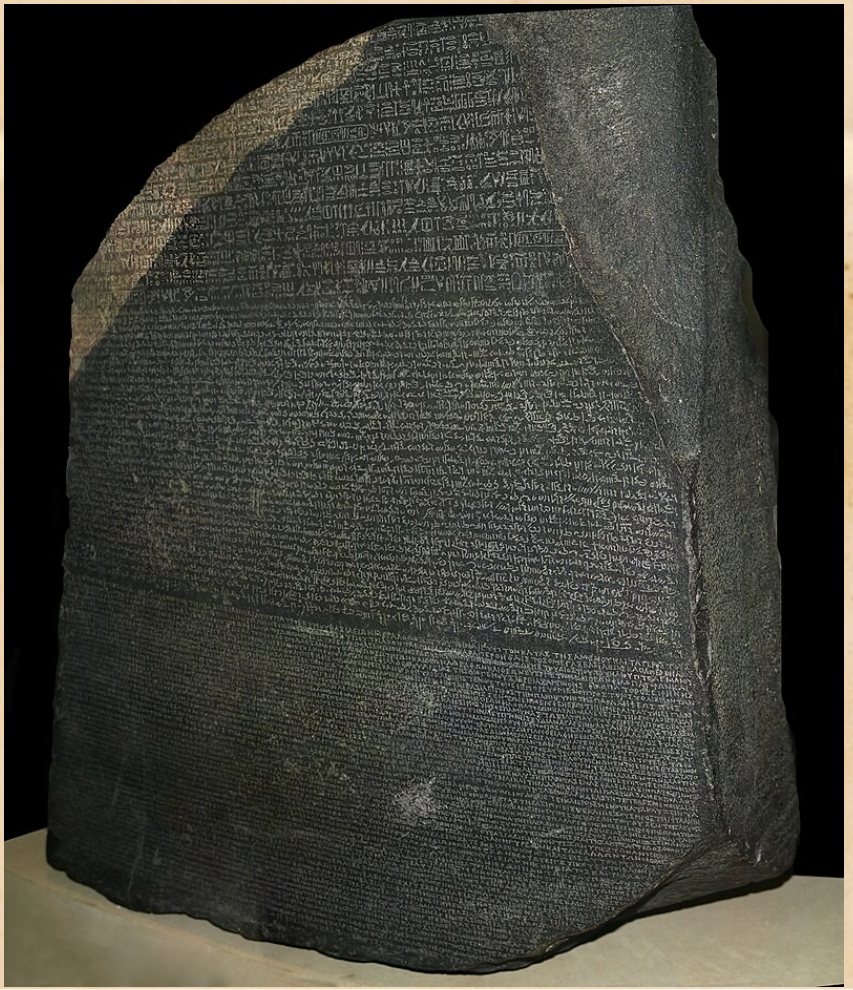
https://en.wikipedia.org/wiki/Hadamard_transform

$$H_0 = +(1)$$

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_3 = \frac{1}{2^{3/2}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

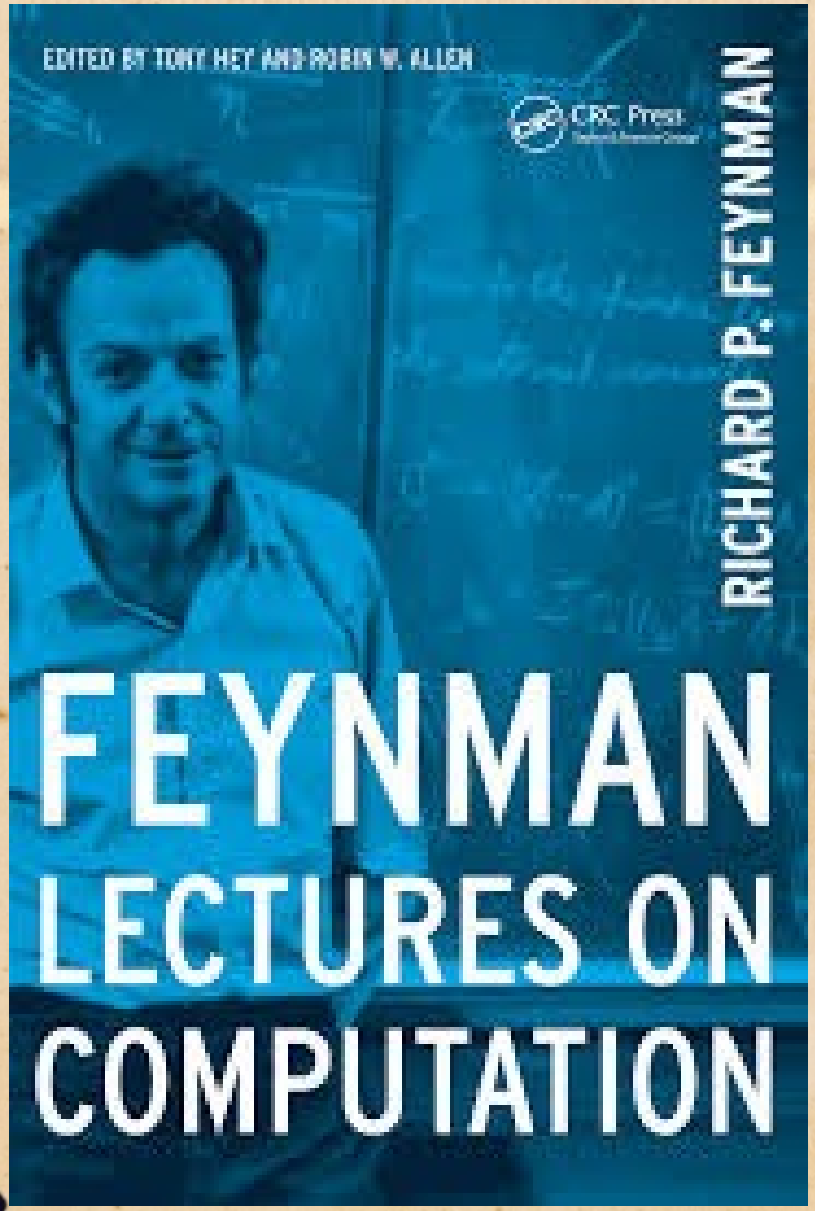


https://en.wikipedia.org/wiki/Rosetta_Stone

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

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

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

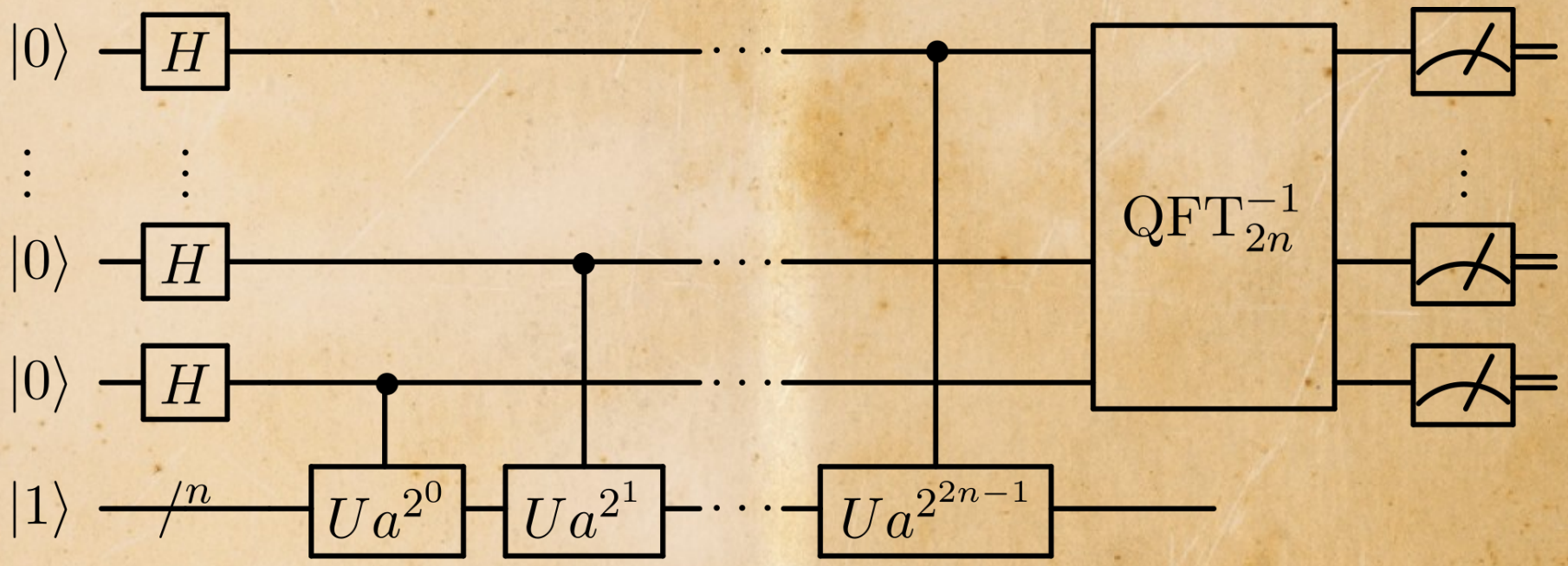


Lectures given 1983 through 1986...

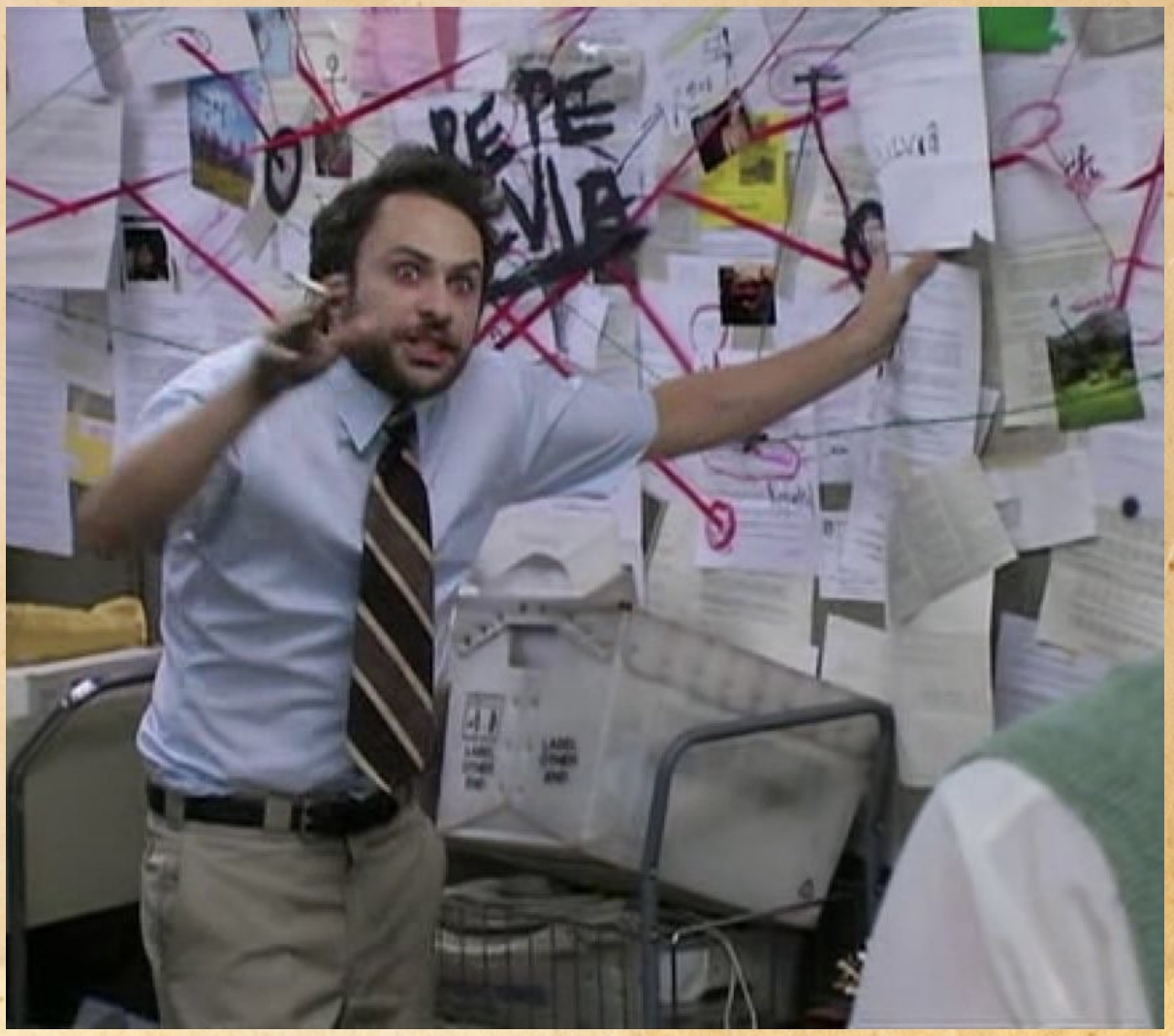
"Another similar problem deals with factorization: I give you a number *m*, and tell you that it is the product of two primes, *m=pq*. … It is possible to build our ignorance of the general solution of this mathematical problem into a ciphering message. … The moment some clever *guy* cracks it … we'd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

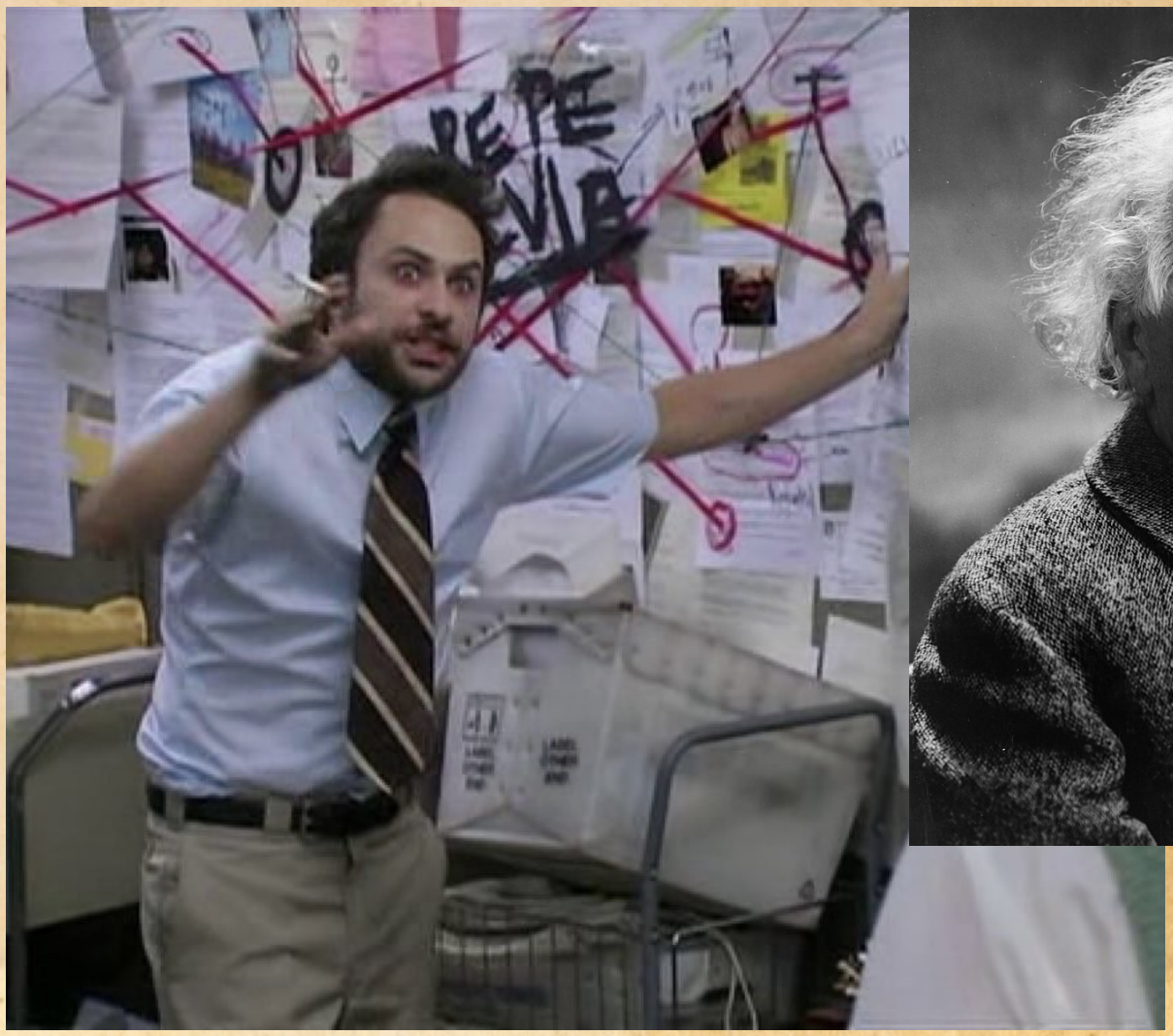
https://en.wikipedia.org/wiki/Shor%27s_algorithm

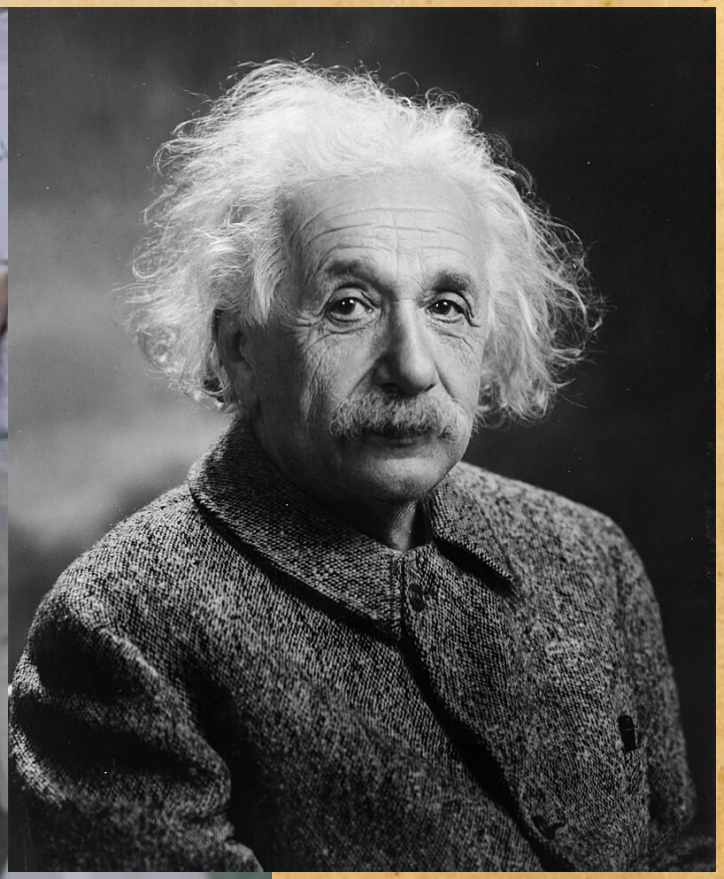


The semester is just getting started...

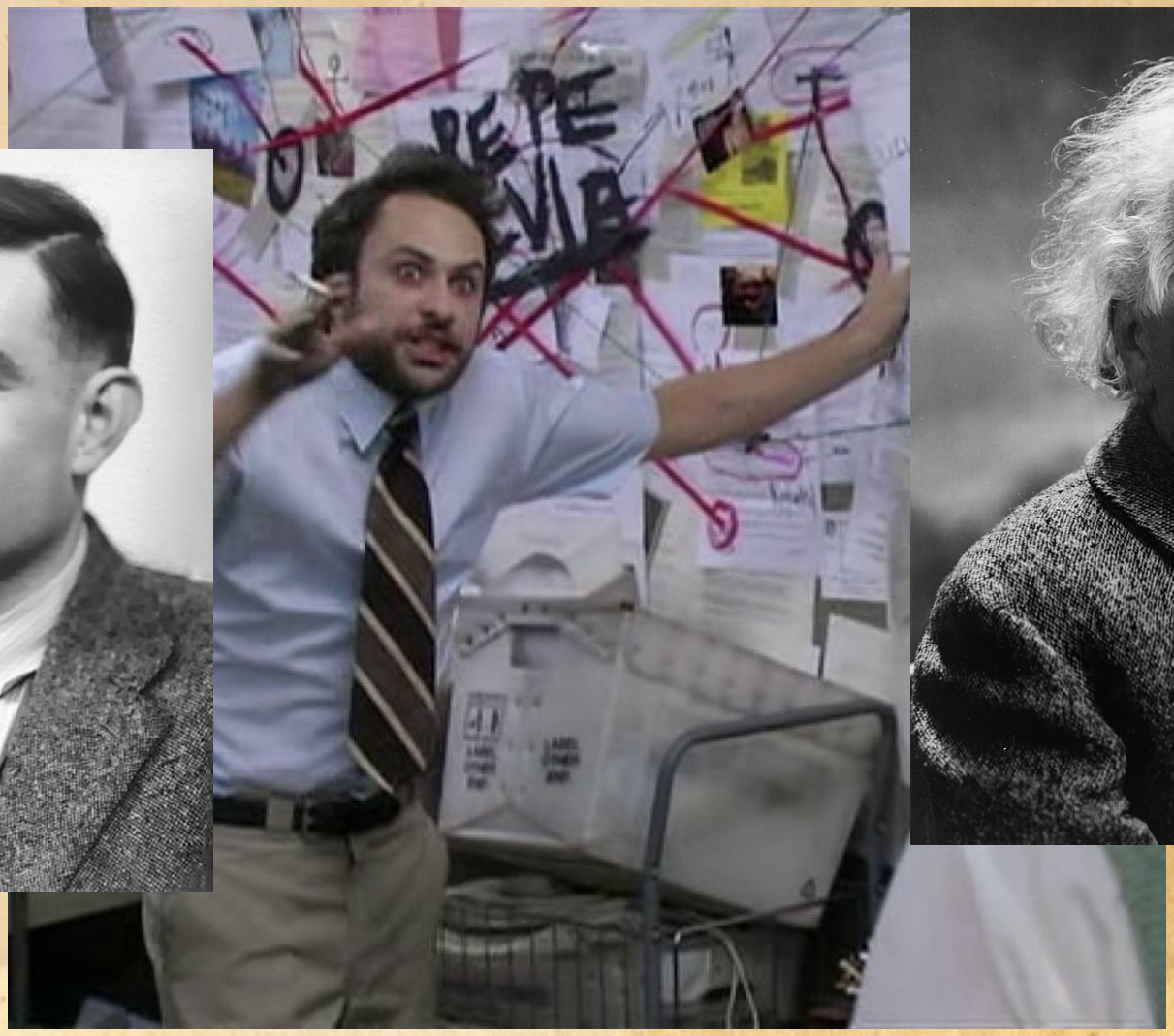


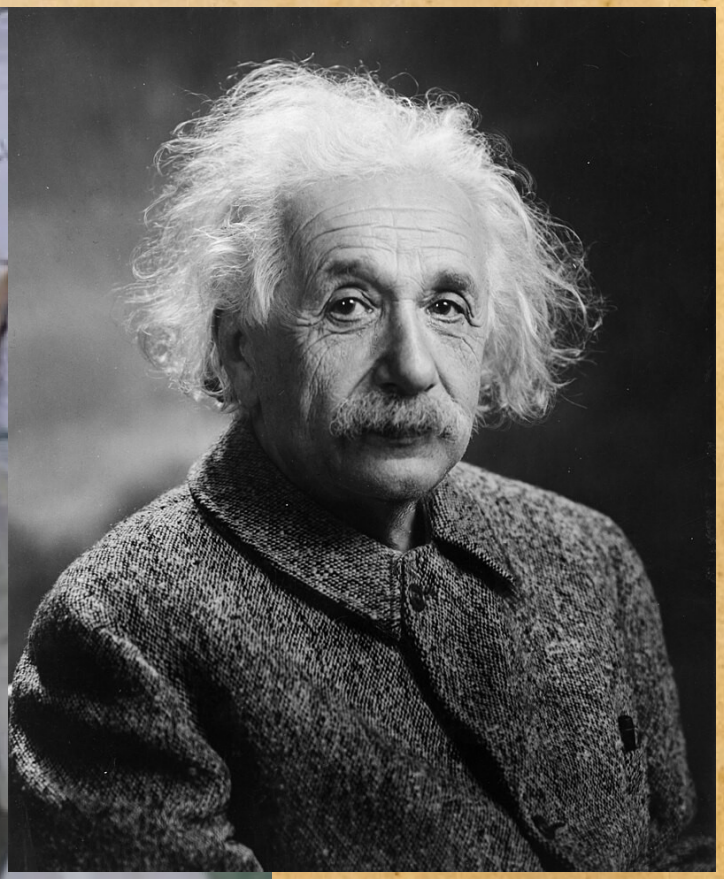
The semester is just getting started...





The semester is just getting started...





Take out your phone or laptop...

- Is it safe to use the network you're connected to? Is your Internet traffic encrypted to keep it safe? Will the crypto last 10 years?
- What are the apps you couldn't live without? How easily could your Internet Service Provider (ISP) take them away?
- Do you use good passwords? Are your accounts safe? Could there be malware on your phone?

Read the syllabus

- Three exams + final (check dates)
  - 4 * 20% = 80% of the grade
  - Simple (non-scientific) calculator and pen/pencil only
- Six digital artifacts, three homeworks, and an essay
  - 20% of the grade
- No curve or way to get out of the final

OXFORD

THE NATURE *of* COMPUTATION

Cristopher Moore & Stephan Mertens