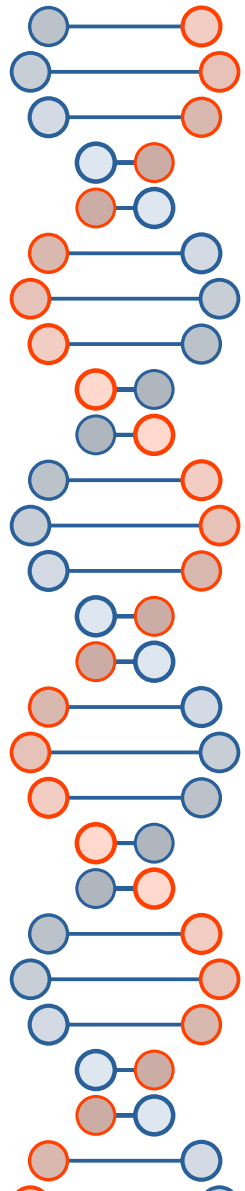


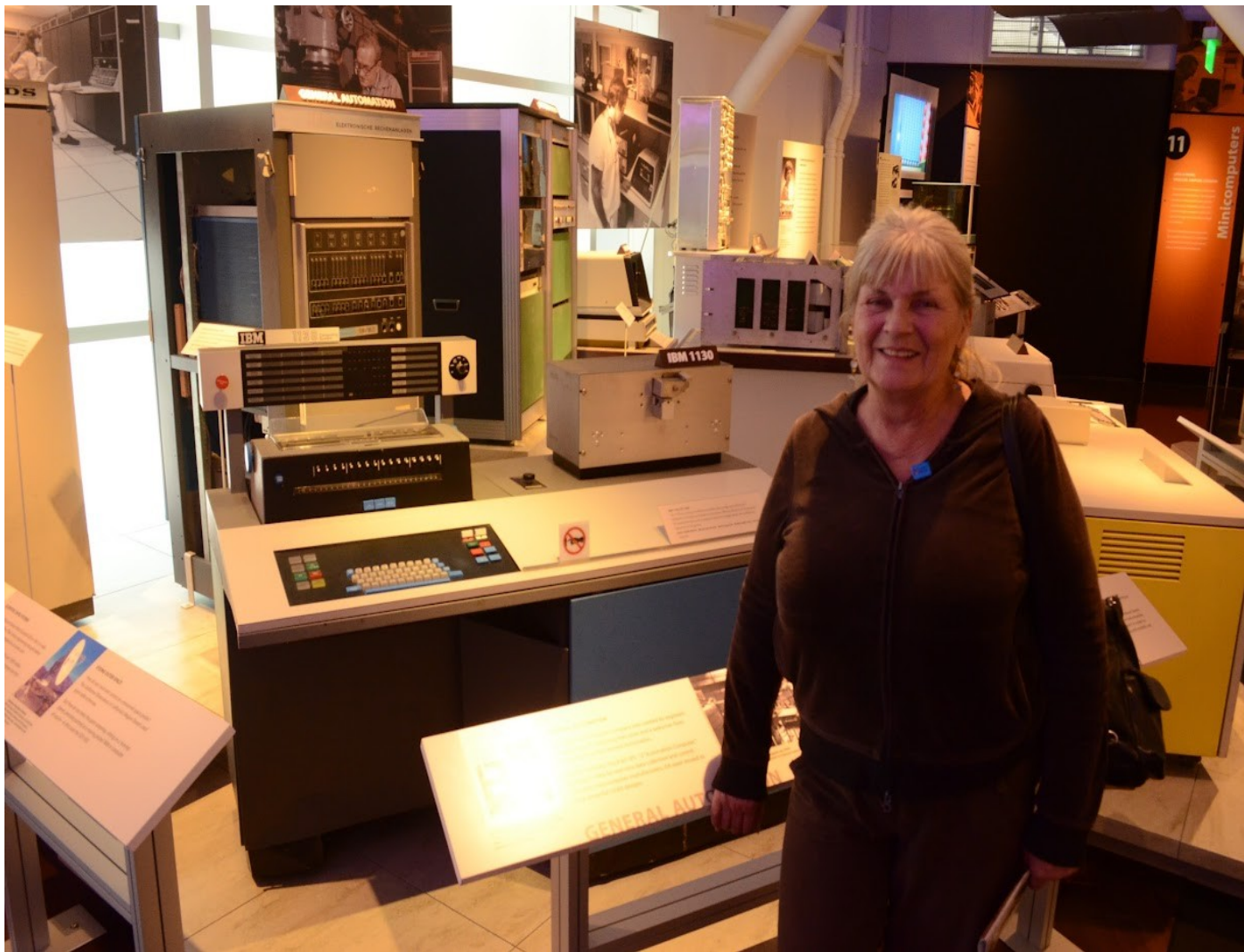
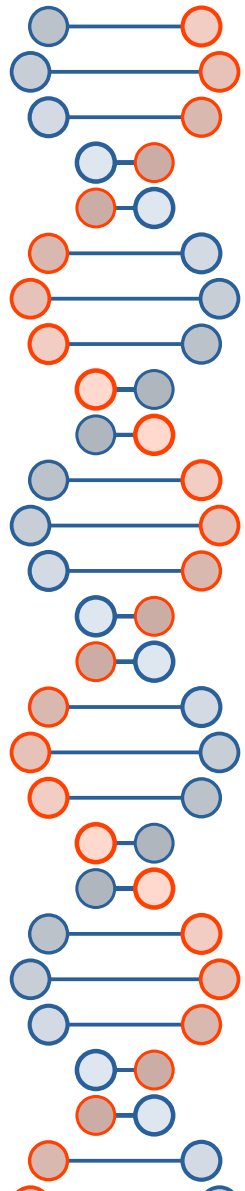
Computer Network Security

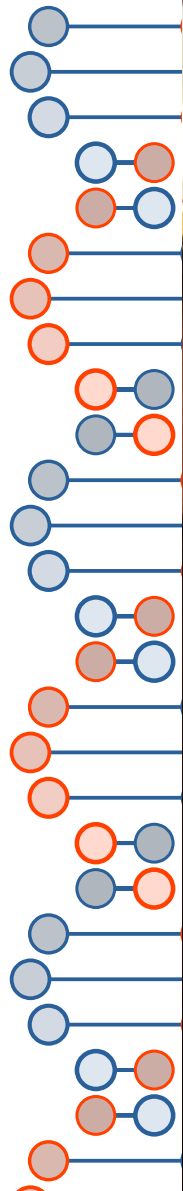
CSE 468

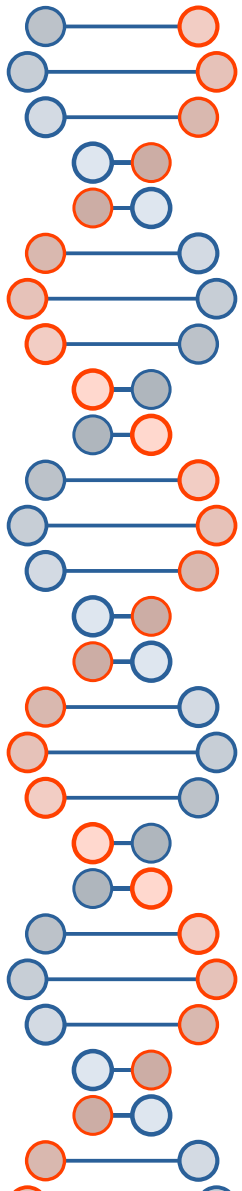
jedimaestro@asu.edu

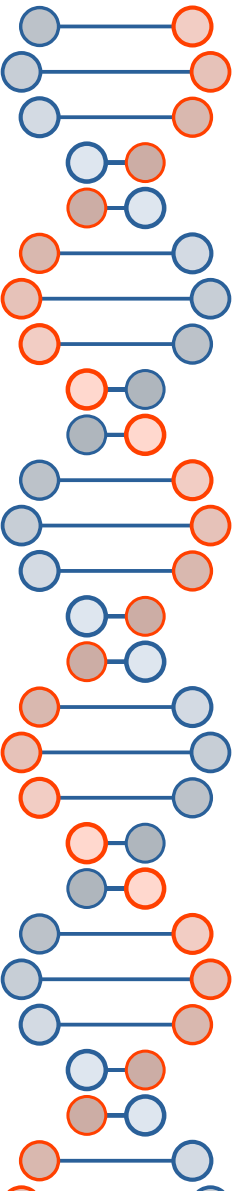


First, a bit about me...









```
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.
```

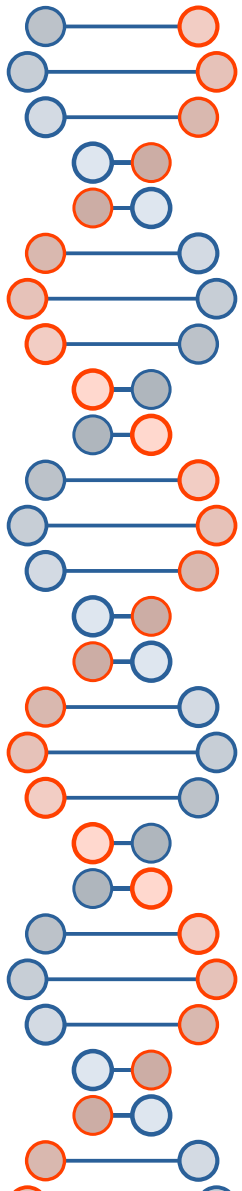
```
Debian Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law. For copyright information, press <F5>.
```

```
This boot floppy installs the Linux kernel version 2.0.0.
```

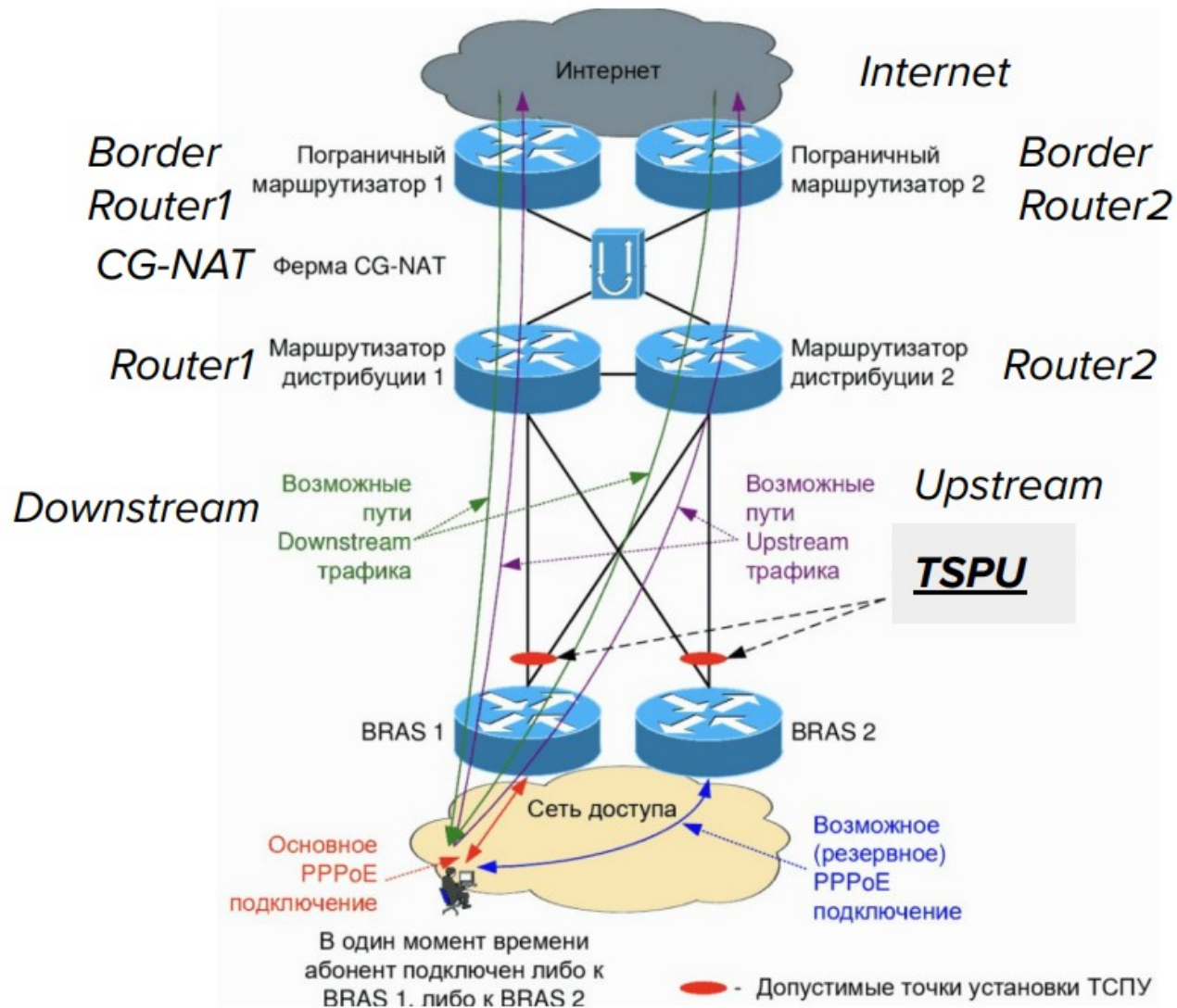
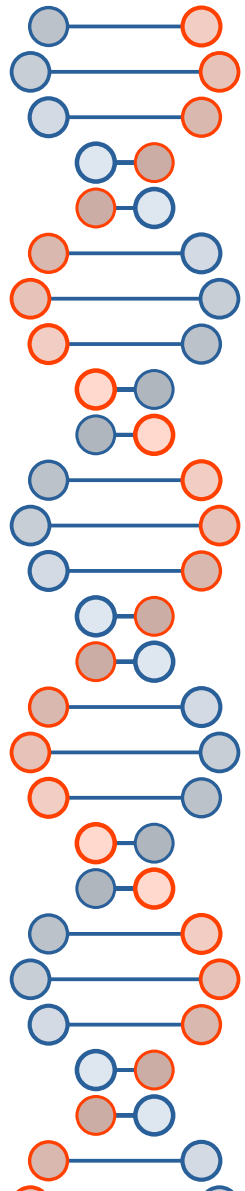
```
Press <F1> for help, or <ENTER> to boot!
```

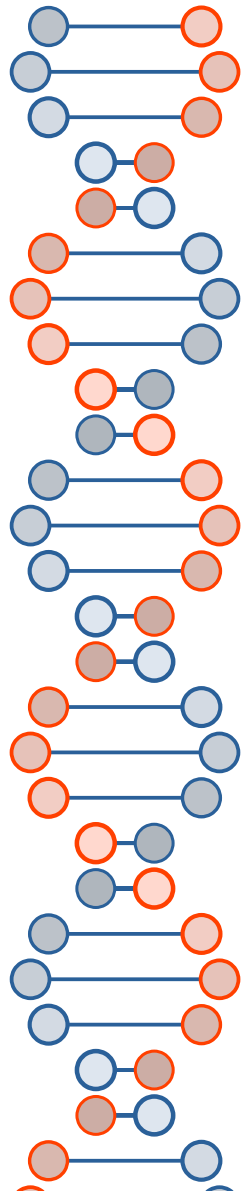
```
boot: _
```

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

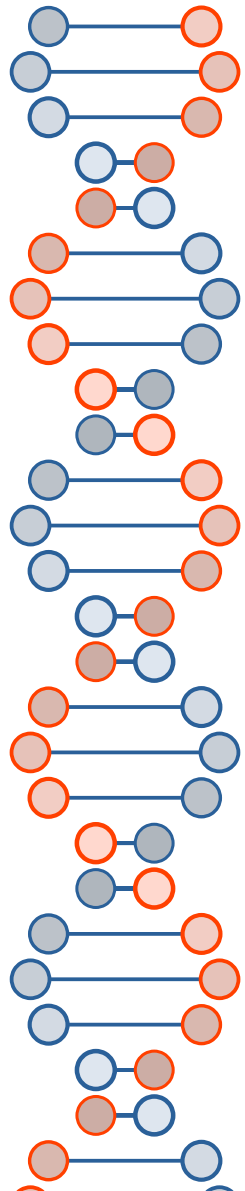


<https://en.wikipedia.org/wiki/PRIMOS>

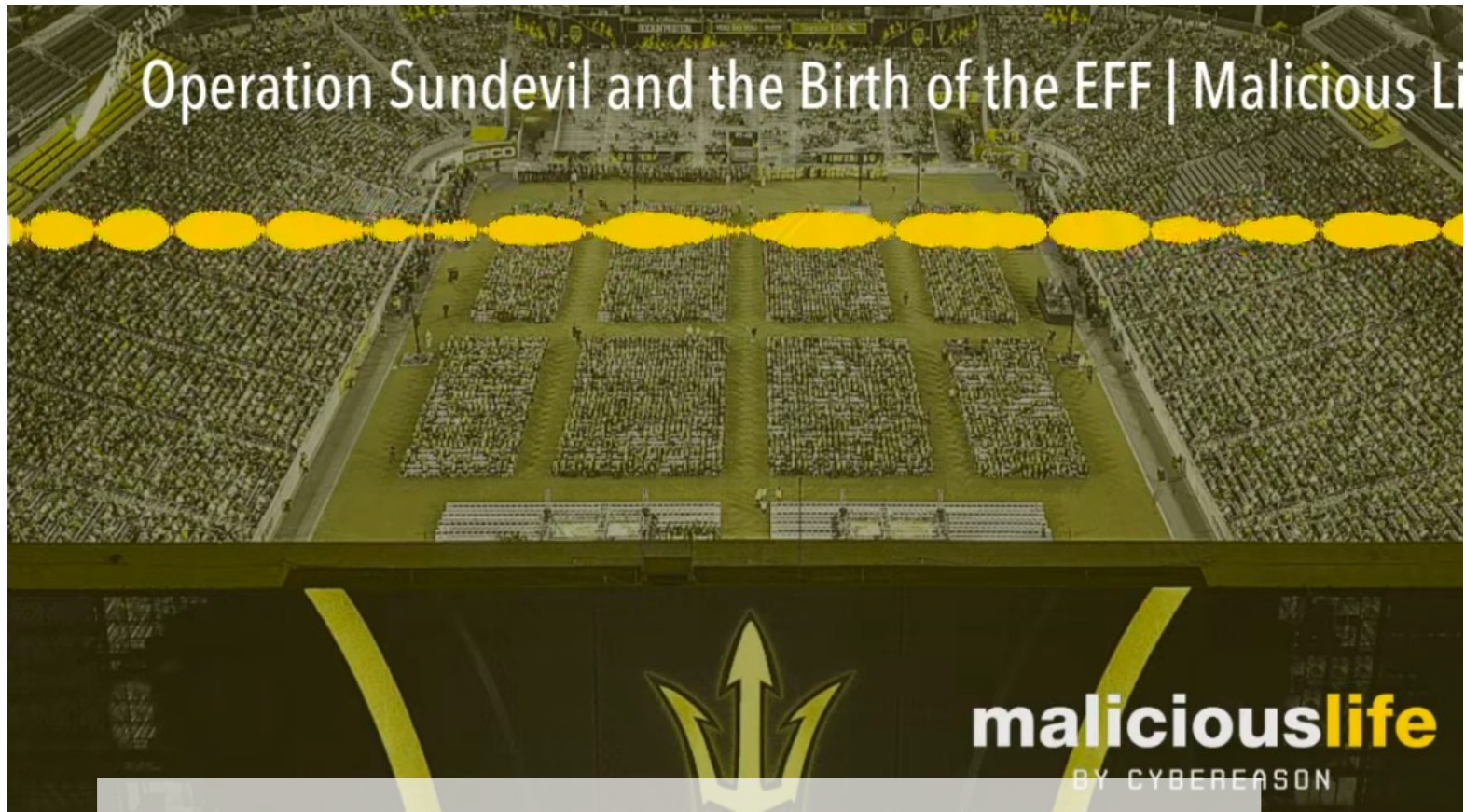
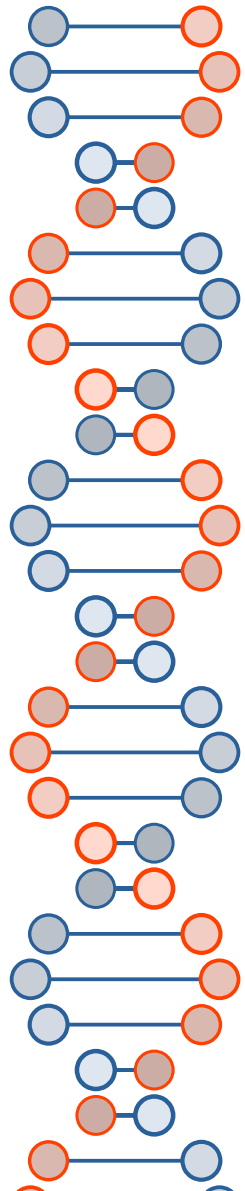




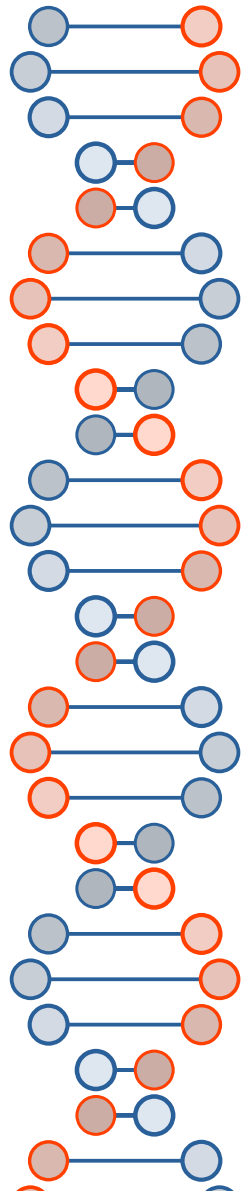
What are *you* hoping to learn this semester?

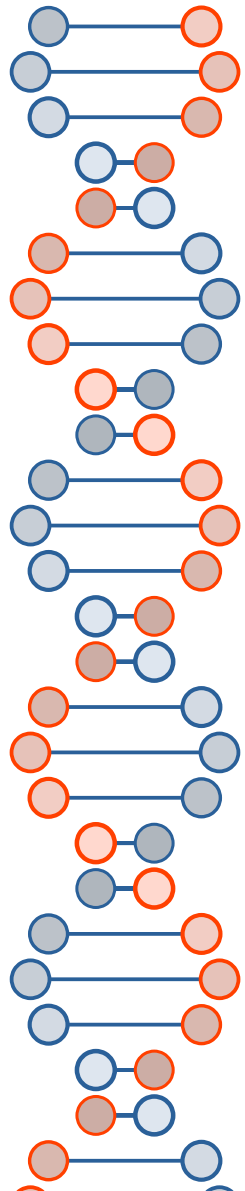


Close your eyes, rest your head. Imagine it's the middle of the night and you're not even thinking about CSE 468 or the beginning of the semester...

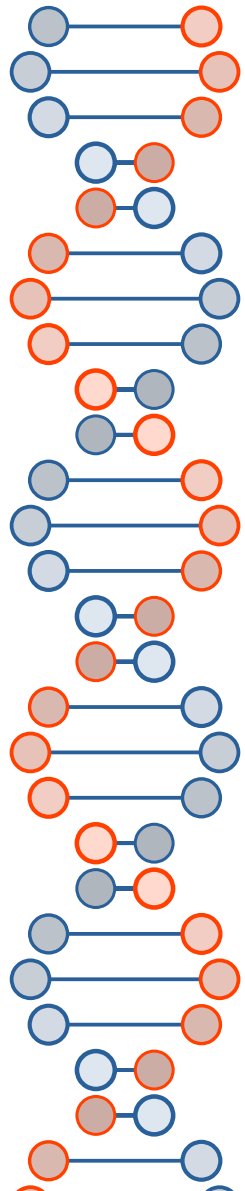


https://www.youtube.com/watch?v=Mookr_VrhyU





We're fortunate to be in a place and time where it's okay to explore the things we'll explore this semester.

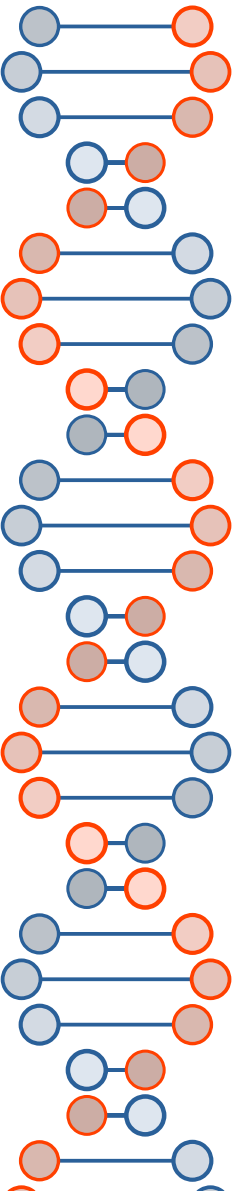


✦ AI Overview

The word "computer" was first used in **1613** by English writer Richard Braithwaite in his book *The Yong Mans Gleanings*. At the time, it referred to a person—a human who performed mathematical calculations or computations.  DEV Community +3

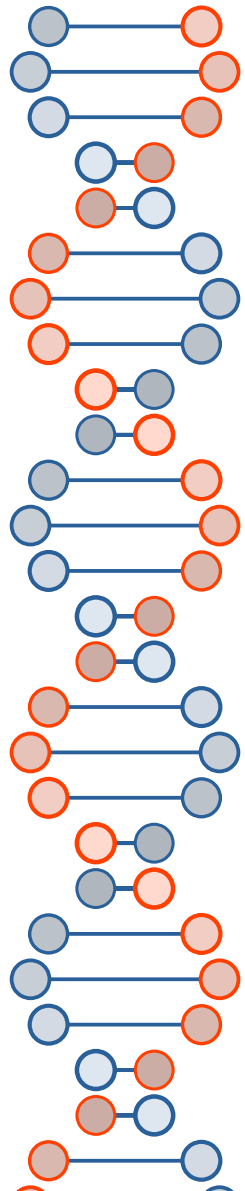
✦ AI Overview

The word "network" started being used in **the early 1500s**, initially describing physical textiles and openwork or meshed fabrics. Over time, its meaning expanded to physical systems, broadcasting, and computers.  Merriam-Webster +2



What we'll cover this semester

- Crypto
 - Hash functions, symmetric, asymmetric, quantum, *etc.*
- Network attacks and defenses
 - ARP poisoning, WiFi security, DNS security, *etc.*
- Network Intrusion Detection and related topics
 - NIDS evasion, information controls, malware, *etc.*



The foundations of what we'll learn this semester were mostly invented...



...in history; mostly by criminals, political dissidents, and other misfits.

The specifics of what we'll learn this semester are public knowledge and you shouldn't get in trouble for learning them in an academic *context*, but...



<https://www.bbc.com/news/world-latin-america-39930772>



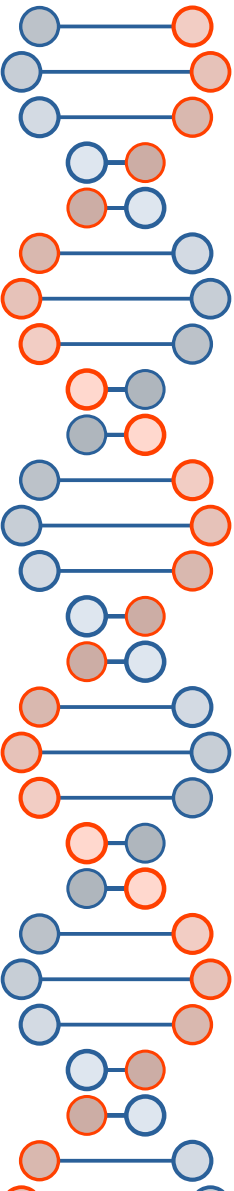
<https://www.frontlinedefenders.org/en/case/rona-wilson-arrested>



<https://walledculture.org/remembering-aaron-swartz-who-died-on-this-day-a-victim-of-the-copyright-system/>

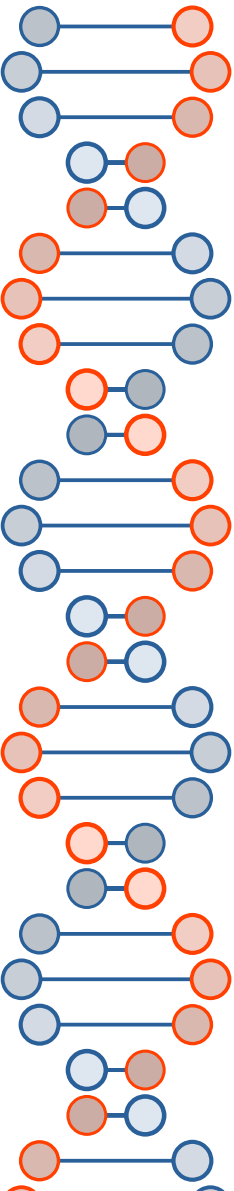


<https://www.whistleblowers.org/members/edward-snowden/>



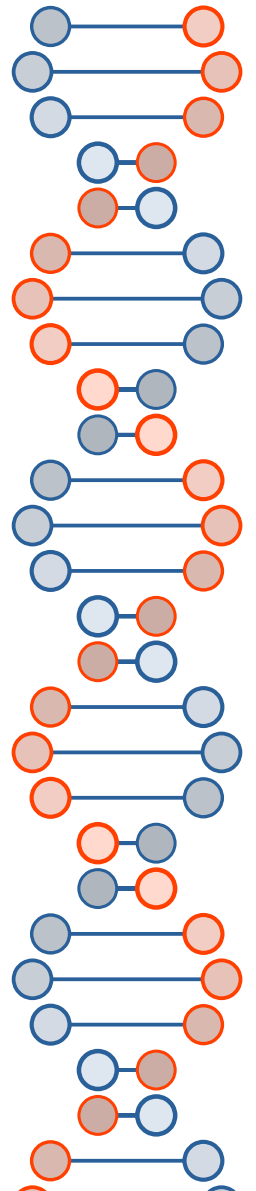
“Computation” in the ancient world

- Continued fractions, decimal approximation, irrational numbers, *etc.*
 - Babylonian Root Extraction (1800 BCE)
 - Hippasus of Metapontum (450 BCE)
 - Heron’s Method (1st Century CE)



“Computation” in the ancient world

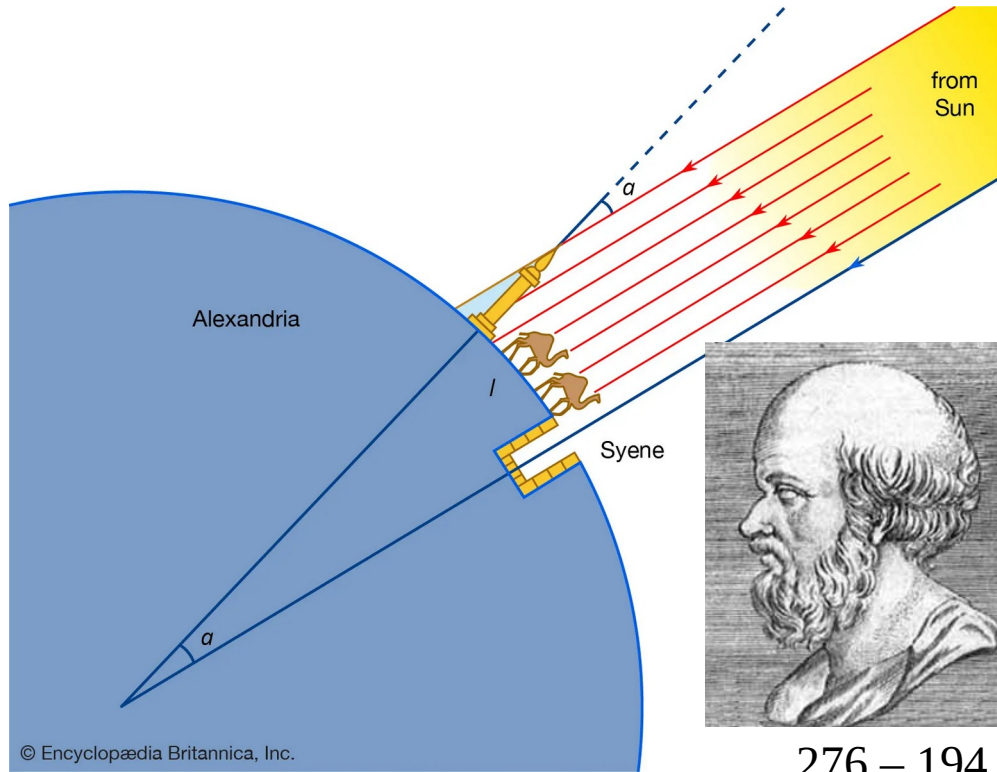
- Fun with integers
 - Rhind Mathematical Papyrus (1650 BCE)
 - Abacus (1200 BCE)
 - Euclid’s algorithm (~300 BCE)
 - Diophantus of Alexandria (~250 CE)
 - Polynomials with whole numbers
 - Post-quantum crypto
- Chinese Remainder Theorem (3rd—5th century CE)
 - Used in crypto implementations today



“Computation” in the ancient world

- Harmonics, bit reversal permutations (*i.e.*, butterfly pattern), *etc.*
 - Pythagoras and musical chords (530–500 BCE)
 - Shrimad Rajchandra and Jain Mathematicians (Tracing back to the 4th Century BCE)
 - Babylonian astronomers (300–50 BCE)

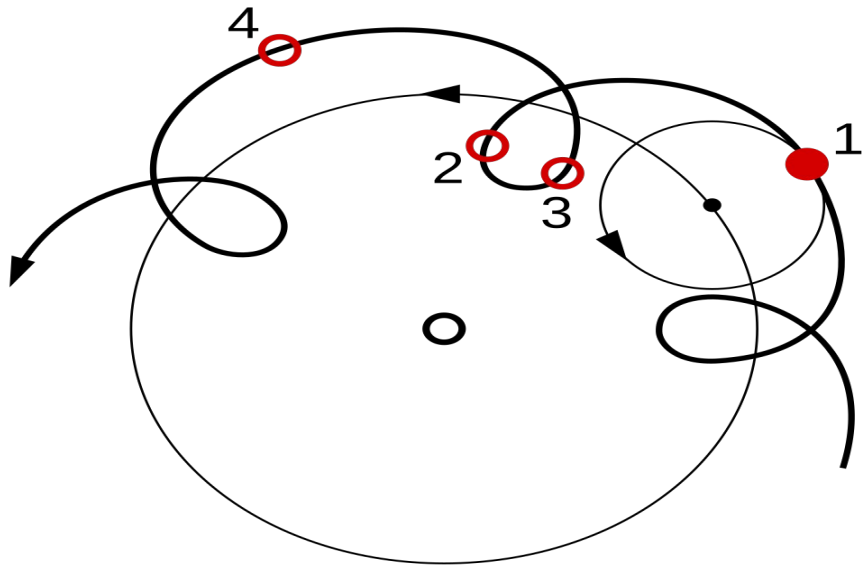
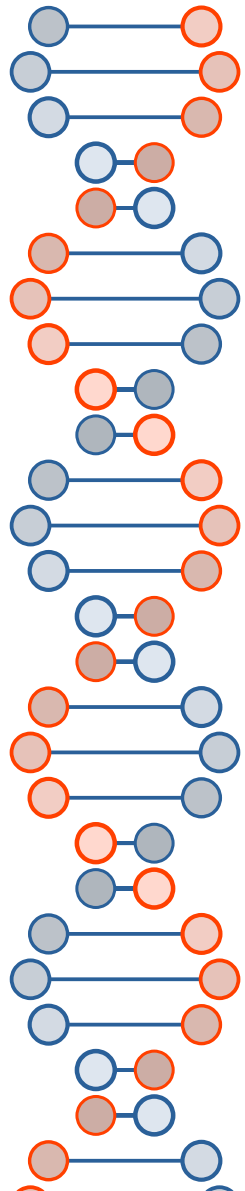
<https://en.wikipedia.org/wiki/Eratosthenes>



276 – 194 BCE

	2	3	4	5	6	7	8	9	10	Prime numbers			
11	12	13	14	15	16	17	18	19	20	2	3	5	7
21	22	23	24	25	26	27	28	29	30	11	13	17	19
31	32	33	34	35	36	37	38	39	40	23	29	31	37
41	42	43	44	45	46	47	48	49	50	41	43	47	53
51	52	53	54	55	56	57	58	59	60	59	61	67	71
61	62	63	64	65	66	67	68	69	70	73	79	83	89
71	72	73	74	75	76	77	78	79	80	97	101	103	107
81	82	83	84	85	86	87	88	89	90	109	113		
91	92	93	94	95	96	97	98	99	100				
101	102	103	104	105	106	107	108	109	110				
111	112	113	114	115	116	117	118	119	120				

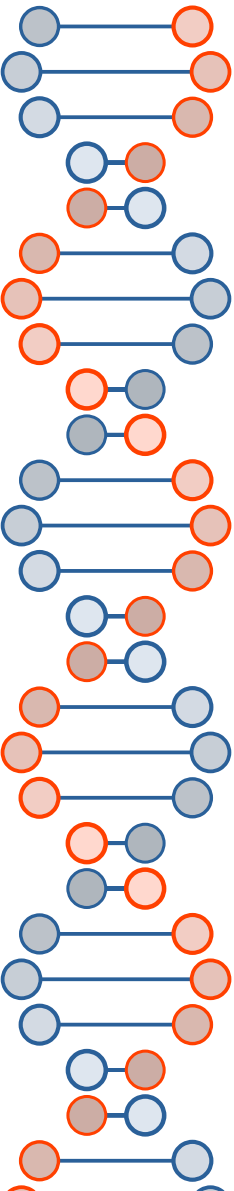
<https://www.britannica.com/biography/Eratosthenes>



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

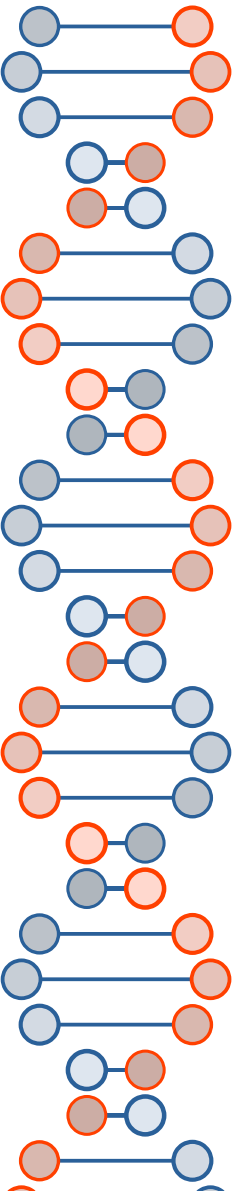


Giordano Bruno



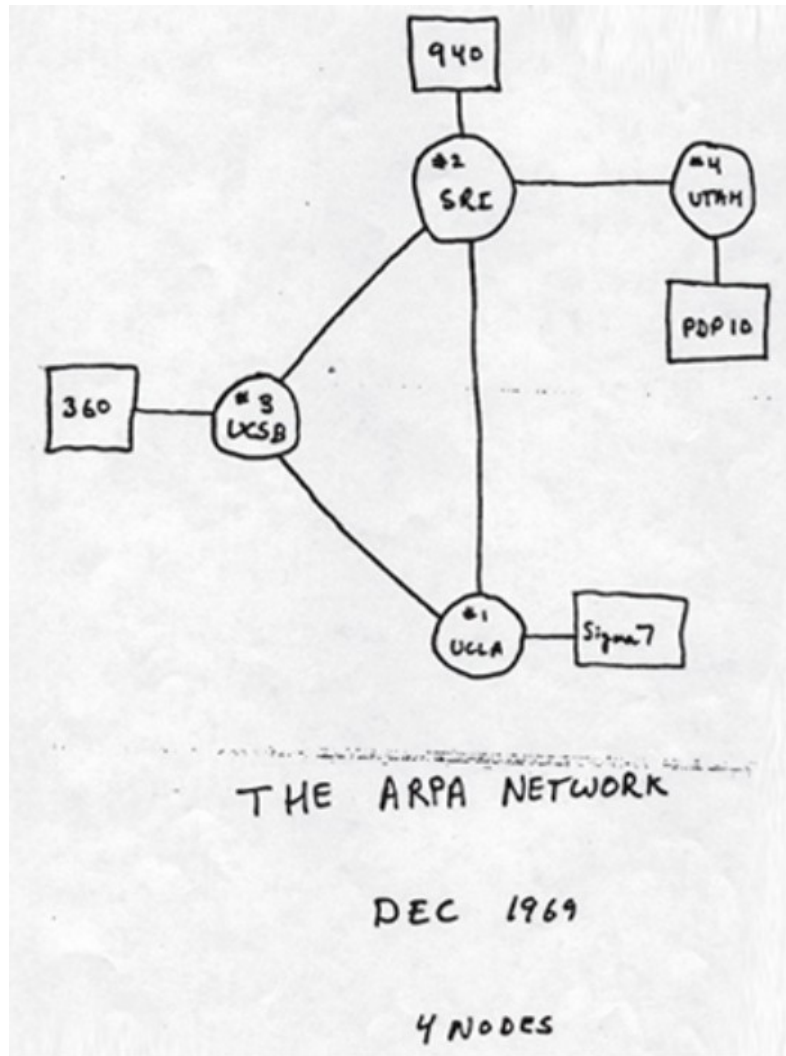
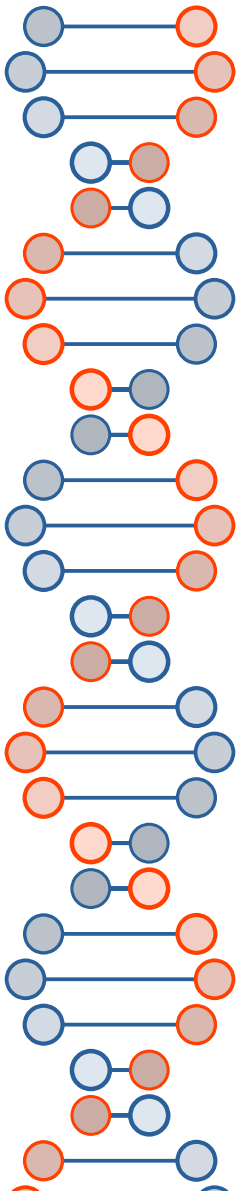
Computation continued

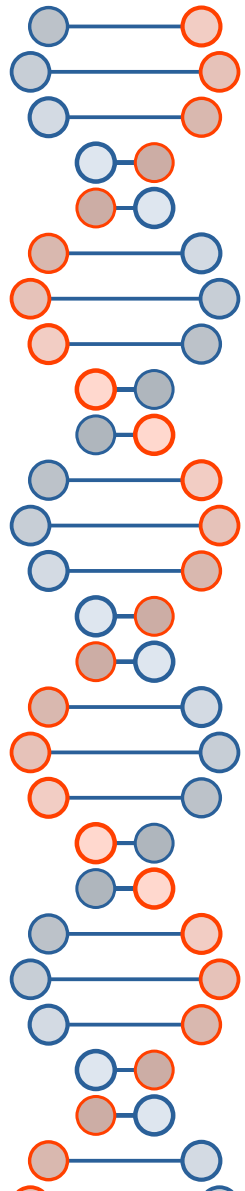
- Logarithm-based or analog: Antikythera Mechanism (150–100 BCE), Al-Biruni's Geared Calendar Computer (~1000), Al-Jazari's Castle Clock (1206), Napier's bones (1617)
- Jacquard Loom (1804) → Babbage's Difference Engine (1821) and Analytical Engine (1834)
- Hollerith cards (1890)
- ENIAC (1945), Colossus (1943), *etc.*



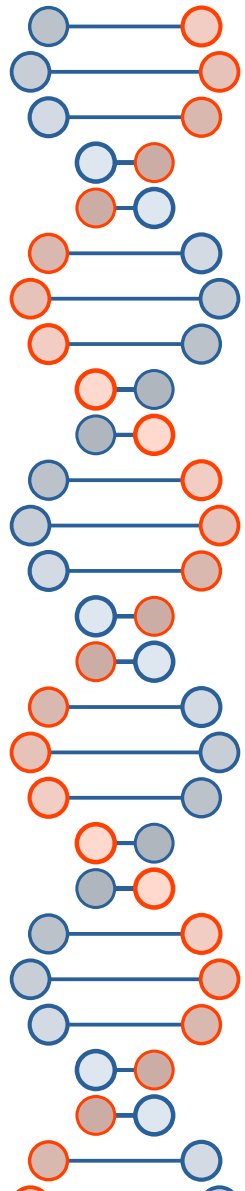
Communication Networks

- Mail systems and smoke signals (ancient Chinese and Romans, for example)
- Relays in the Mongolian Empire (13th and 14th century)
- Optical Telegraph, or Semaphore (invented in France in 1792)
- Electric telegraph, developed in the 1830s and 1840s
- Telephone networks, starting in the 1870s
- Packet switch data networks in the early 1960s

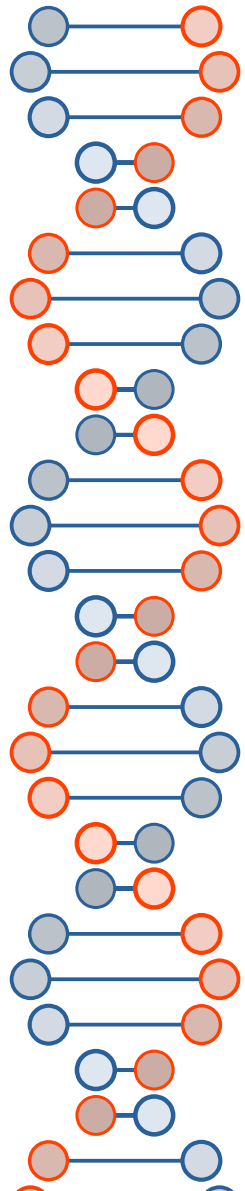




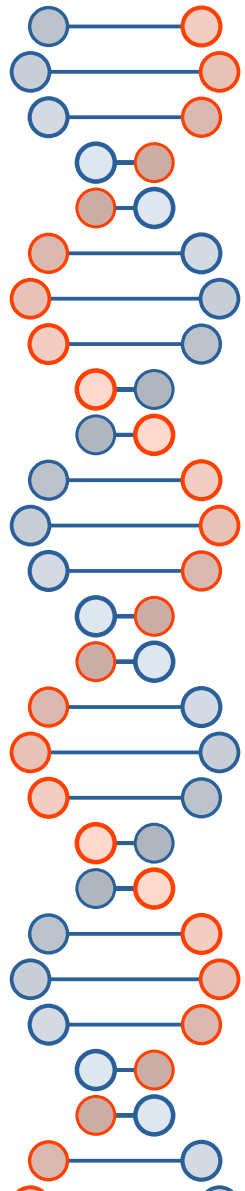
<https://www.rickcrandall.net/assets/media/uploads/pdf/3%20SDS%20940%20and%20Internet.pdf>



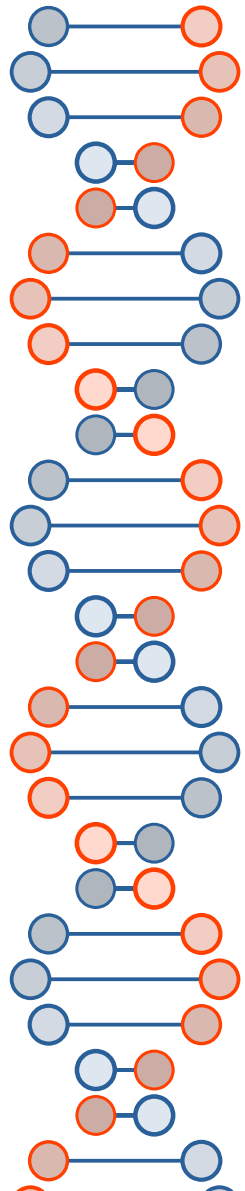
https://commons.wikimedia.org/wiki/File:DEC_PDP-10_%28DECsystem_10%29_mainframe_computer_system_at_Living_Computer_Museum_%28strongly_edited_image%29.jpg



By Joe Mabel, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=31996455>

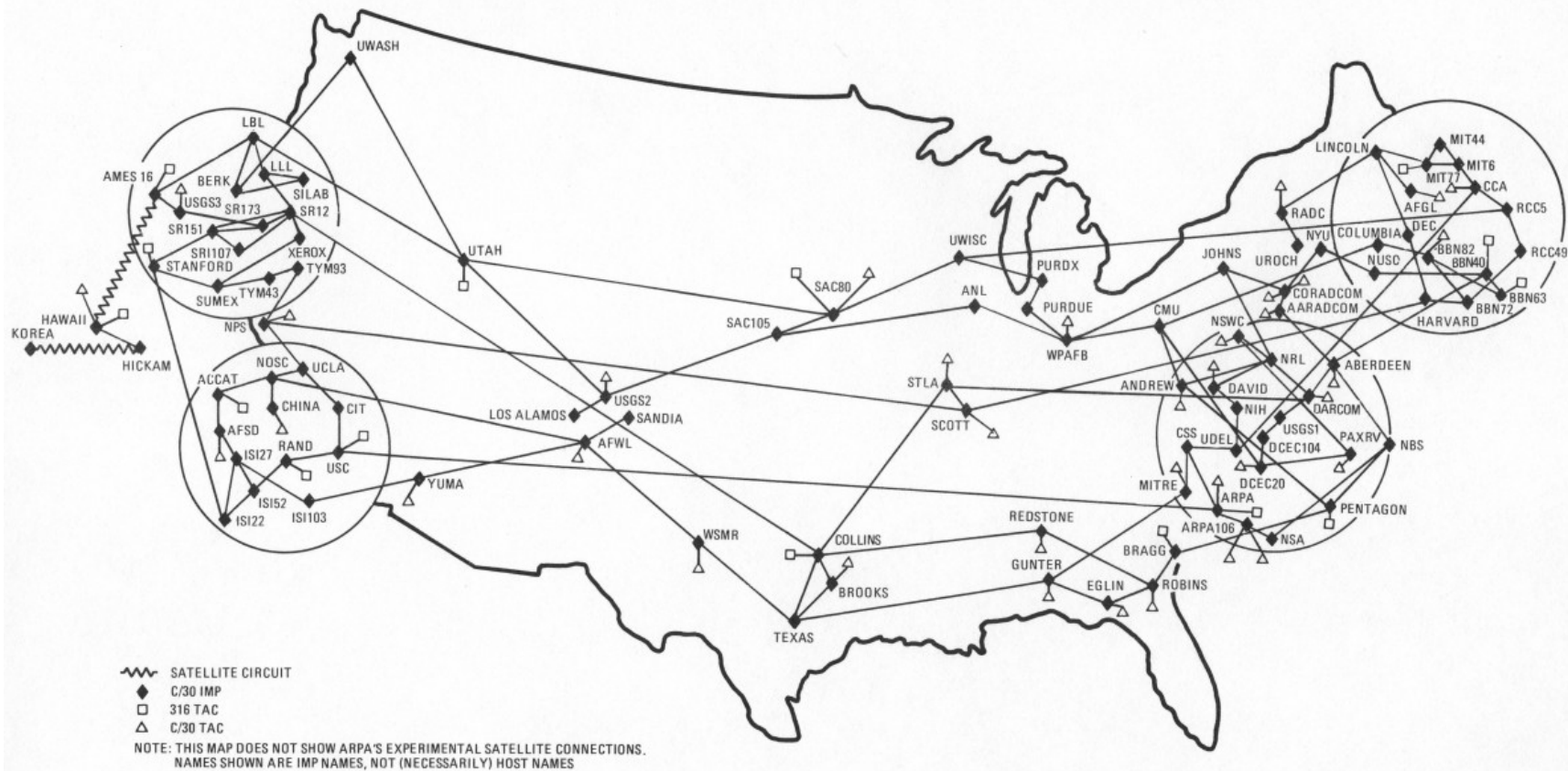


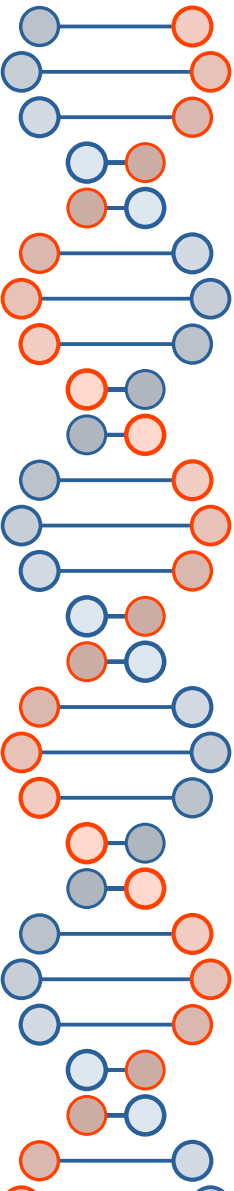
https://commons.wikimedia.org/wiki/File:IBM_System_360_model_30_profile.agr.jpg



<https://www.computerhistory.org/revolution/networking/19/407/2086>

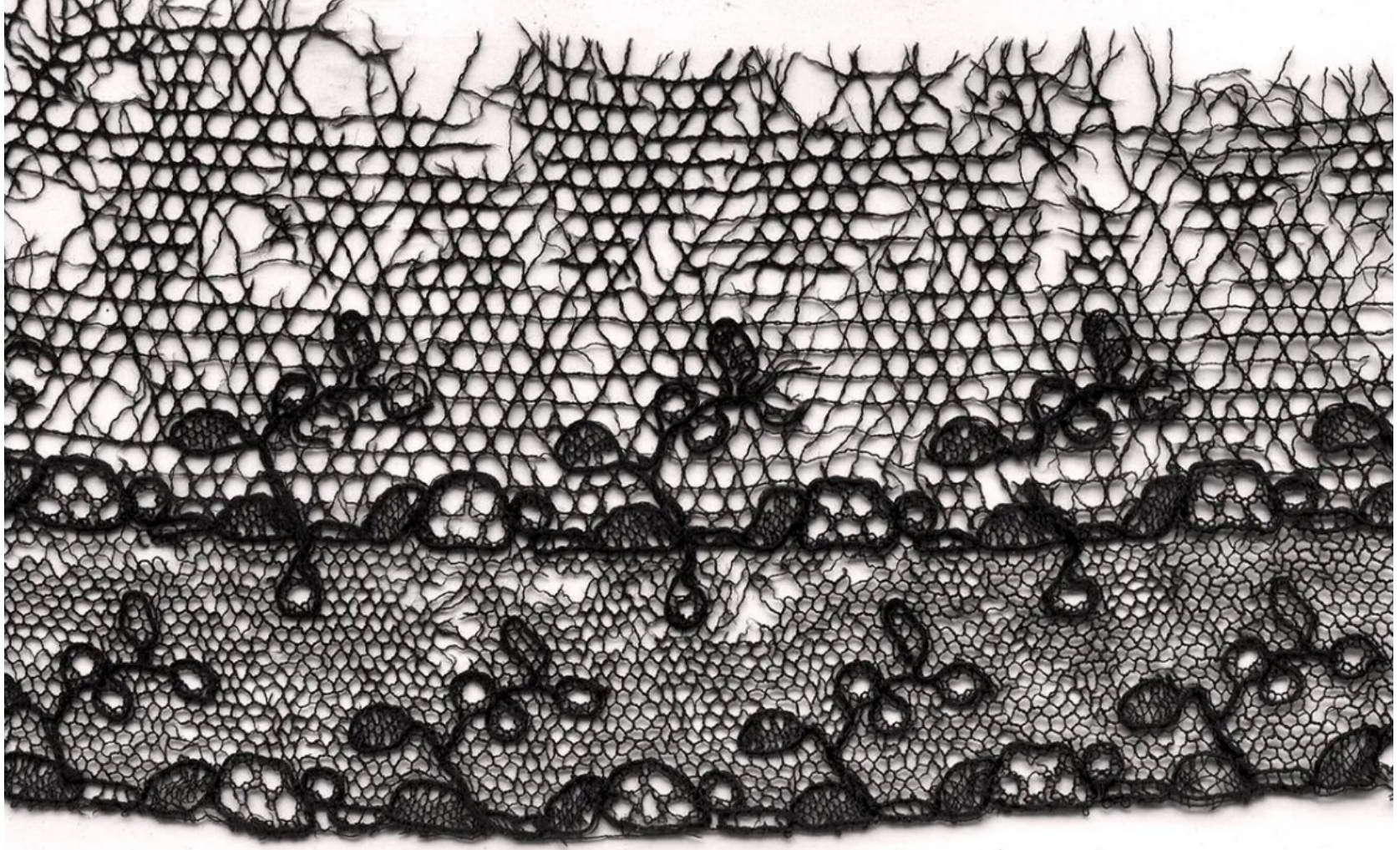
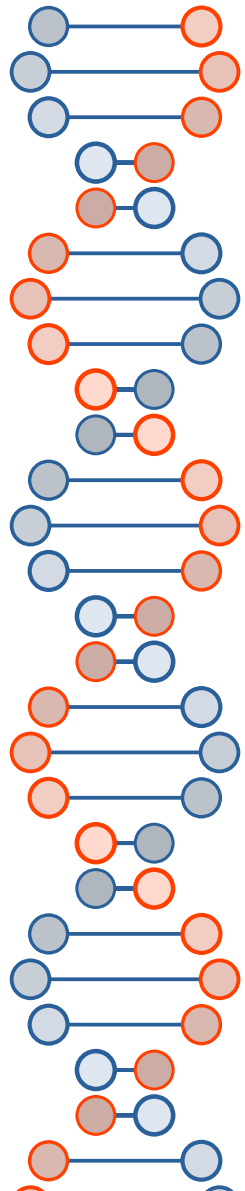
ARPANET/MILNET GEOGRAPHIC MAP, JANUARY 1984



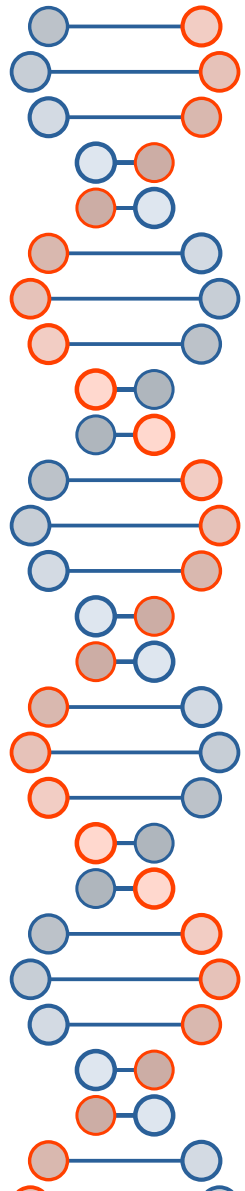


Birth of *the* Internet

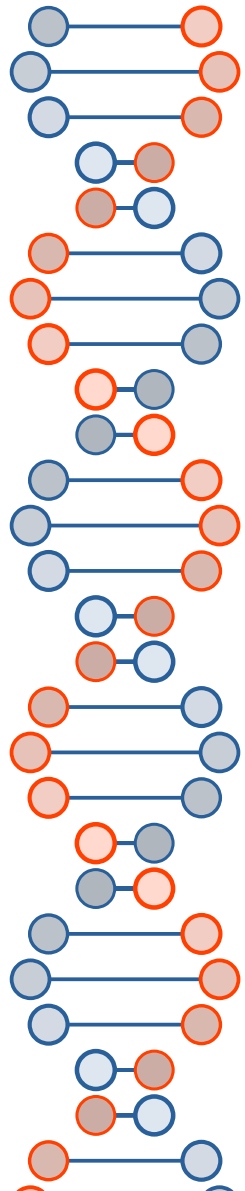
- December 9th, 1968 – “Mother of all demos”
 - Douglas Engelbart presented hypertext, windows, a mouse, teleconferencing, networked computers, GUIs, *etc.*
- October 29th, 1969 – ARPANET comes online
- January 1st, 1983 – ARPANET switches to TCP/IP
- May 9th, 1990 – Operation SunDevil raids
- August 6th, 1991 – Tim Berners-Lee posts a summary of the World Wide Web project on the `alt.hypertext` USENET newsgroup



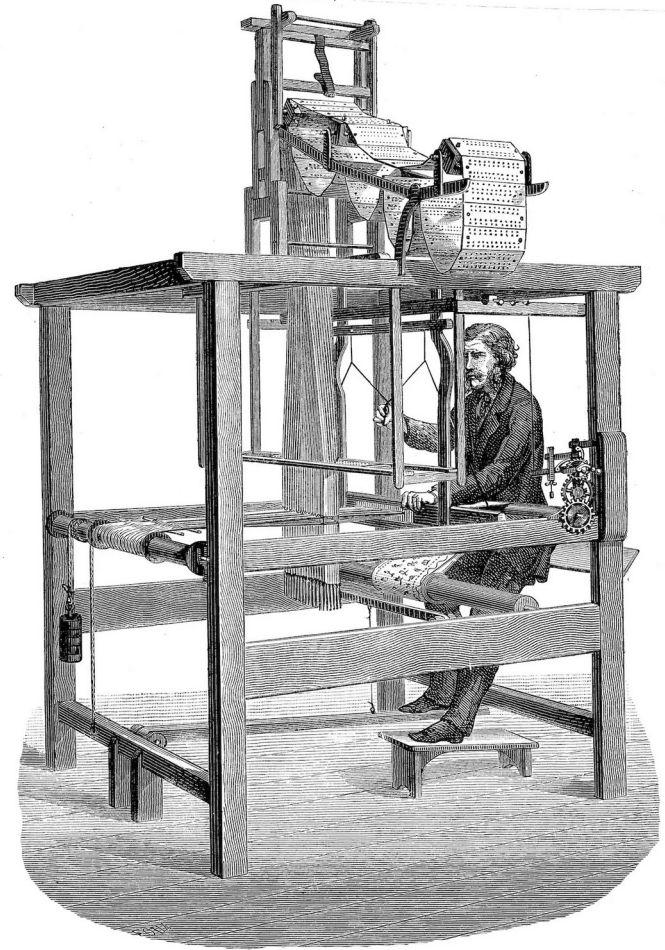
<https://www.britannica.com/technology/netting>



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



- Jacquard loom built in 1804
- Arrested in 1805, taken to Paris
 - Appeared before Napoleon and a mathematician named Lazare Carnot
 - Given a pension and royalties
- Thrown into a river by silk workers in Lyon
- Inspired Babbage's Analytical Engine (1837)
 - Improvement over Difference Engine
 - Ada Lovelace and the first computer program (1843)



<https://www.historytoday.com/archive/months-past/jacquard-patents-his-first-loom>

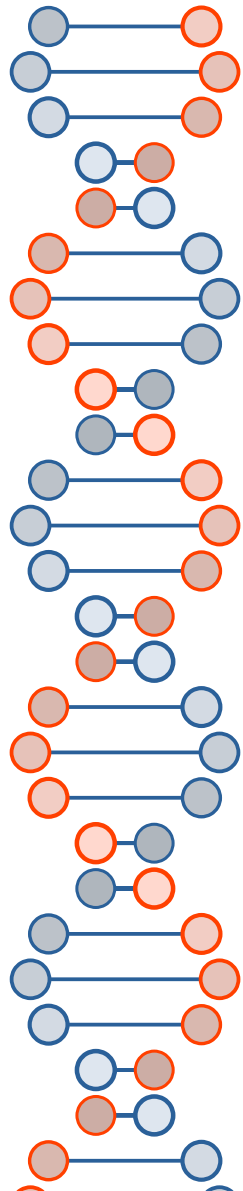


Diagram for the computation by the Engine of the Numbers of Bernoulli. See Note G. (page 722 *et seq.*)

Indication of change in the value on any Variable.	Statement of Results.	Data.			Working Variables.									
		$1V_1$	$1V_2$	$1V_3$	$0V_4$	$0V_5$	$0V_6$	$0V_7$	$0V_8$	$0V_9$	$0V_{10}$	$0V_{11}$	$0V_{12}$	$0V_{13}$
		0 0 0 1	0 0 0 2	0 0 0 4	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
		1	2	n										
$\{1V_2 = 1V_2\}$	$= 2n$	...	2	n	2n	2n	2n							
$\{1V_3 = 1V_3\}$	$= 2n - 1$	1	...	...	2n - 1									
$\{1V_4 = 2V_4\}$	$= 2n + 1$	1	...	...	...	2n + 1								
$\{1V_5 = 1V_5\}$	$= 2n + 1$	1	...	...	...	2n + 1								
$\{2V_5 = 0V_5\}$	$= \frac{2n - 1}{2n + 1}$	...	...	...	0	0	...	...	...	...	...			
$\{1V_{11} = 2V_{11}\}$	$= \frac{1}{2} \cdot \frac{2n - 1}{2n + 1}$	...	2	...	...	...	...	...	...	...	...			
$\{1V_2 = 1V_2\}$	$= \frac{1}{2} \cdot \frac{2n - 1}{2n + 1}$	...	2	...	...	...	...	...	...	...	...			
$\{2V_{11} = 0V_{11}\}$	$= -\frac{1}{2} \cdot \frac{2n - 1}{2n + 1} = A_0$	...	...	...	...	...	...	...	...	...	...			
$\{0V_{13} = 1V_{13}\}$	$= -\frac{1}{2} \cdot \frac{2n - 1}{2n + 1} = A_0$	...	...	...	...	...	...	...	...	...	...			
$\{1V_3 = 1V_3\}$	$= n - 1 (= 3)$	1	...	n	...	...	...	...	...	...	n - 1			$-\frac{1}{2} \cdot \frac{2n - 1}{2n + 1} = A_0$
$\{1V_1 = 1V_1\}$	$= n - 1 (= 3)$	1	...	n	...	...	...	...	...	...	n - 1			
$\{1V_2 = 1V_2\}$	$= 2 + 0 = 2$	...	2	...	...	...	...	2						
$\{0V_7 = 1V_7\}$	$= 2n$	...	...	...	...	...	...	2						
$\{1V_6 = 1V_6\}$	$= \frac{2n}{2} = A_1$	...	...	...	...	...	2n	2						
$\{0V_{11} = 3V_{11}\}$	$= \frac{2n}{2} = A_1$	...	...	...	...	...	2n	2						
$\{1V_{21} = 1V_{21}\}$	$= B_1 \cdot \frac{2n}{2} = B_1 A_1$	...	...	...	...	...	...	...						
$\{3V_{11} = 3V_{11}\}$	$= B_1 \cdot \frac{2n}{2} = B_1 A_1$	...	...	...	...	...	...	...						
$\{1V_{12} = 0V_{12}\}$	$= -\frac{1}{2} \cdot \frac{2n - 1}{2n + 1} + B_1 \cdot \frac{2n}{2}$	...	...	...	...	...	...	...						
$\{1V_{13} = 2V_{13}\}$	$= -\frac{1}{2} \cdot \frac{2n - 1}{2n + 1} + B_1 \cdot \frac{2n}{2}$	...	...	...	...	...	...	...						
$\{1V_{10} = 2V_{10}\}$	$= n - 2 (= 2)$	1	...	...	...	...	...	...						$\left\{ -\frac{1}{2} \cdot \frac{2n - 1}{2n + 1} + B_1 \cdot \frac{2n}{2} \right\}$

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

Lazare Carnot

- Military mobilization
 - Side note: René Carmille
- Father of Sadi Carnot
 - Carnot engine → “entropy”
→ information theory
- Tables du Cadastre (1792 to 1801)
 - In the elite "Section 1" alongside other legendary minds like Legendre



https://en.wikipedia.org/wiki/Carnot_engine_explanation#/media/File:Sadi_Carnot.jpeg



https://en.wikipedia.org/wiki/File:Lazare_Carnot_1948_Issue.jpg

Tables du Cadastre



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

Gaspard de Prony



https://en.wikipedia.org/wiki/Adrien-Marie_Legendre

Adrien-Marie Legendre



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

Others in the French Academy of Sciences



https://en.wikipedia.org/wiki/Andr%C3%A9-Marie_Amp%C3%A8re

André-Marie Ampère



https://en.wikipedia.org/wiki/Pierre-Simon_Laplace

Pierre-Simon Laplace



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

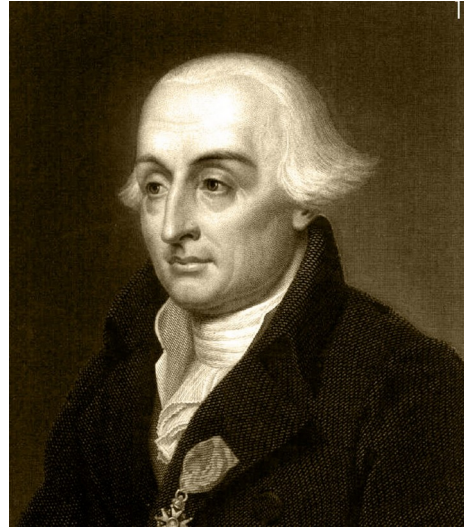
Leonhard Euler

Others in the French Academy of Sciences



https://en.wikipedia.org/wiki/Sim%C3%A9on_Denis_Poisson

Siméon Denis Poisson



https://en.wikipedia.org/wiki/Joseph-Louis_Lagrange

Joseph-Louis Lagrange



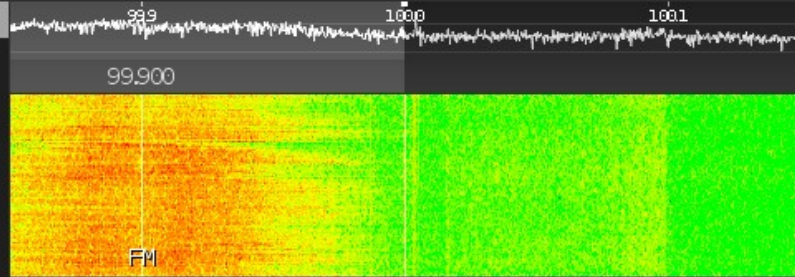
https://en.wikipedia.org/wiki/Joseph_Fourier

Joseph Fourier

File Settings Sample Rate Audio Sample Rate Recording Rig Control Display

FM
FMS
NBFM
AM
LSB
USB
DSB
I/Q

Modem Settings



Frequency

Bandwidth

Center Frequency

99900000

200000

100000000

Search..

Active

99.9MHz FM

View Ranges

Bookmarks

Recents

99.90191MHz FM

99.90066MHz FM

Label

Freq 99.9MHz

BW 200KHz

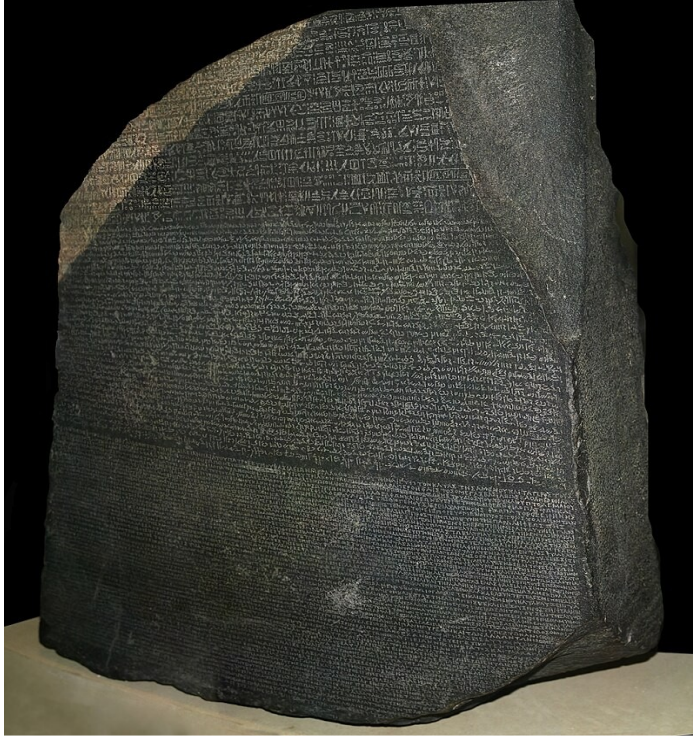
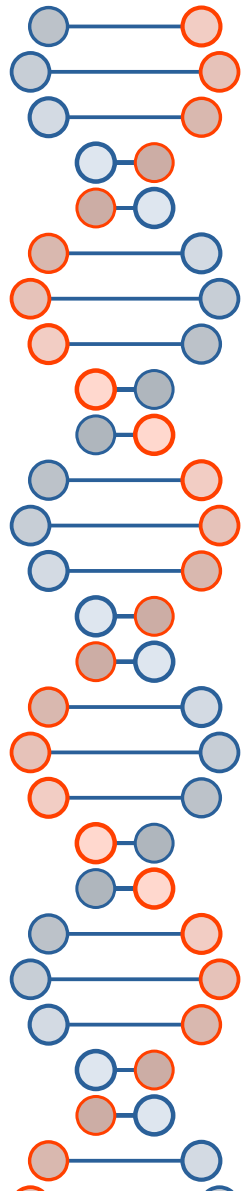
Type FM

Bookmark..

Start Recording

Remove Active

Current Demodulator Gain Level: Click / Drag to set Gain Level



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

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



People NOT in the French Academy of Sciences



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

Sophie Germain



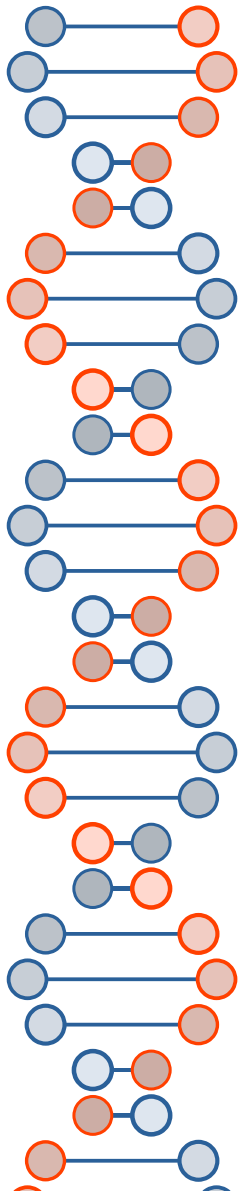
https://en.wikipedia.org/wiki/%C3%89variste_Galois

Évariste Galois



https://en.wikipedia.org/wiki/%C3%89milie_du_Ch%C3%A2telet

Émilie du Châtelet



Certificate Viewer: asu.edu

General Details

Certificate Hierarchy

- WE1
 - asu.edu

Certificate Fields

- Certificate Policies
- CRL Distribution Points
- Signed Certificate Timestamp List
- Certificate Signature Algorithm
- Certificate Signature Value
- SHA-256 Fingerprints
 - Certificate
 - Public Key

Field Value

X9.62 ECDSA Signature with SHA-256
X9.62 ECDSA Signature with SHA-256

Export...

In the French Academy of Sciences?



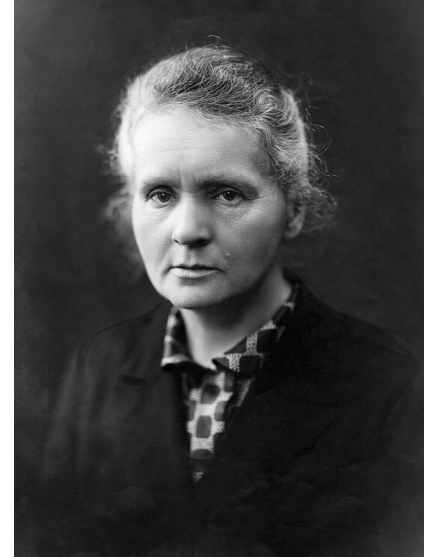
https://en.wikipedia.org/wiki/Niels_Bohr

Niels Bohr



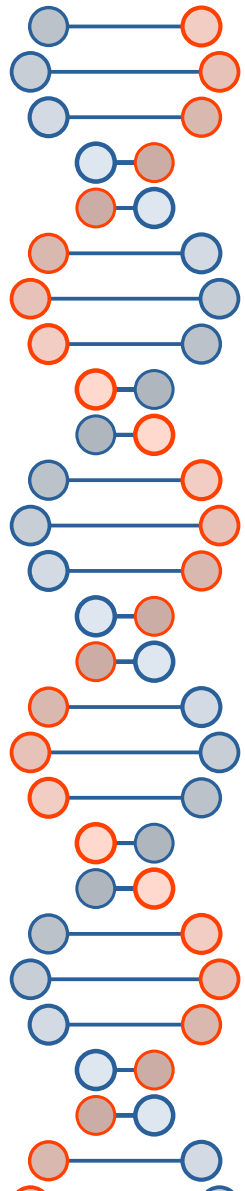
https://en.wikipedia.org/wiki/Emmy_Noether

Emmy Noether



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

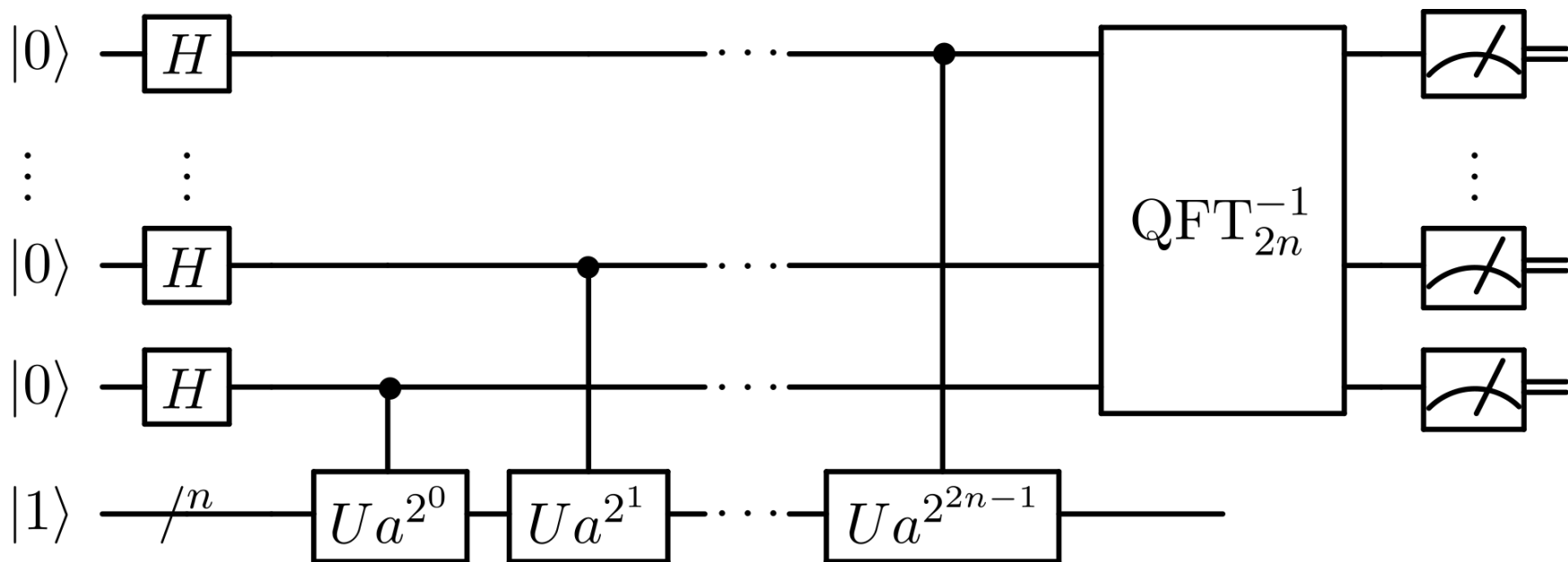
Marie Curie

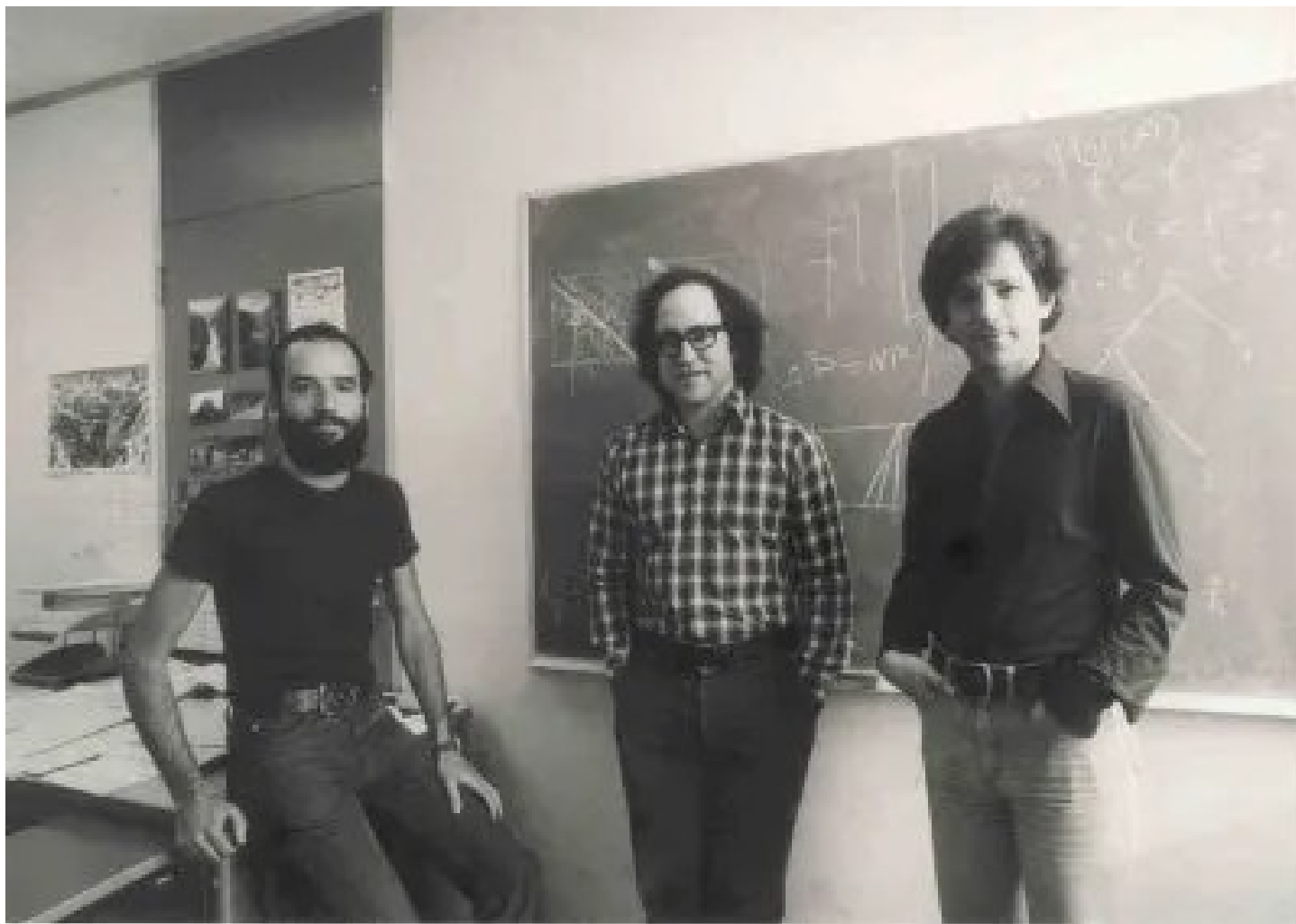
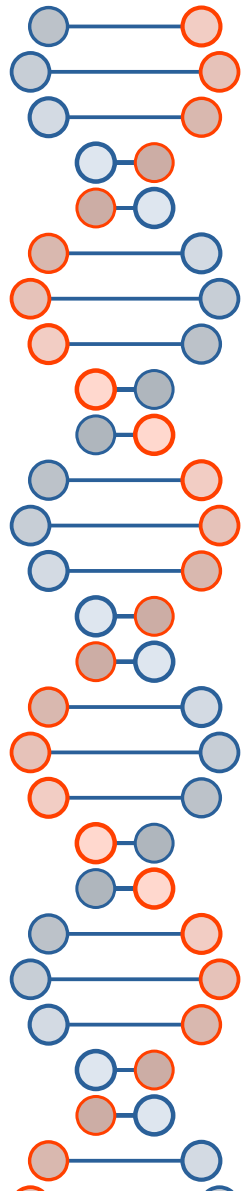


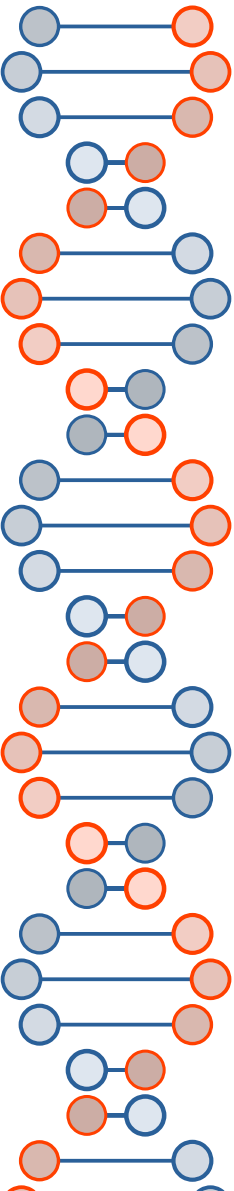
<https://www.flickr.com/photos/feuilllu/46700983592>



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







Diffie-Hellman – 1976

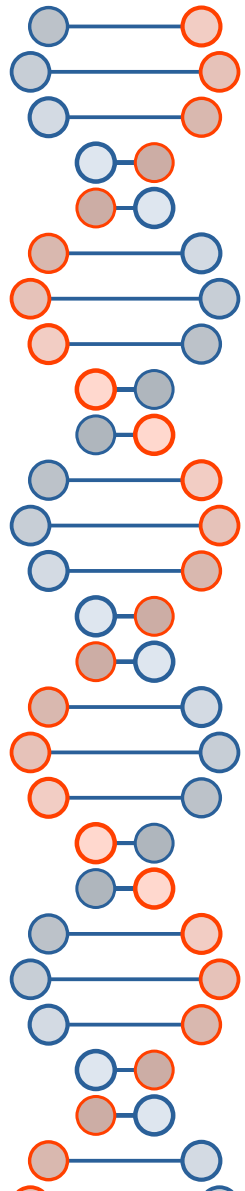
RSA – 1977

OAEF (Bellare and Rogaway) – 1994

*The Internet, telephone system, and packet switch networks
were largely unencrypted until the early 1990s*.*

What was that like?

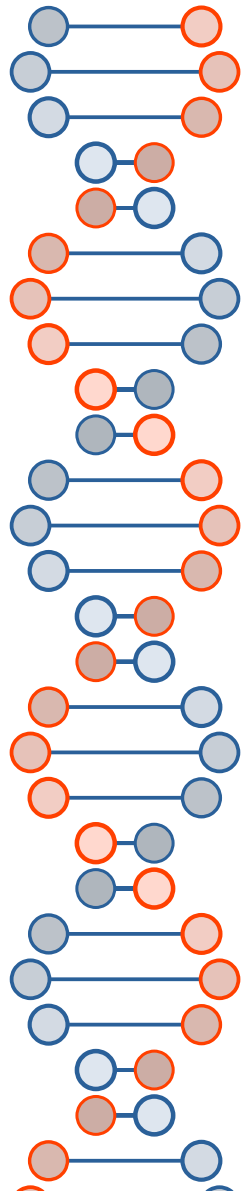
**also early 1990s: www and Operation Sundevil*



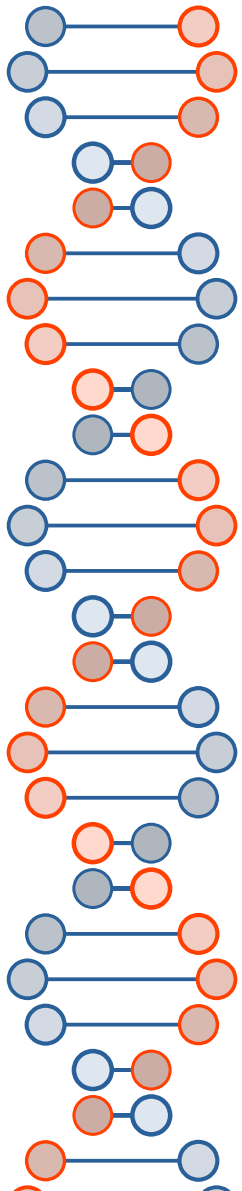
parmaster



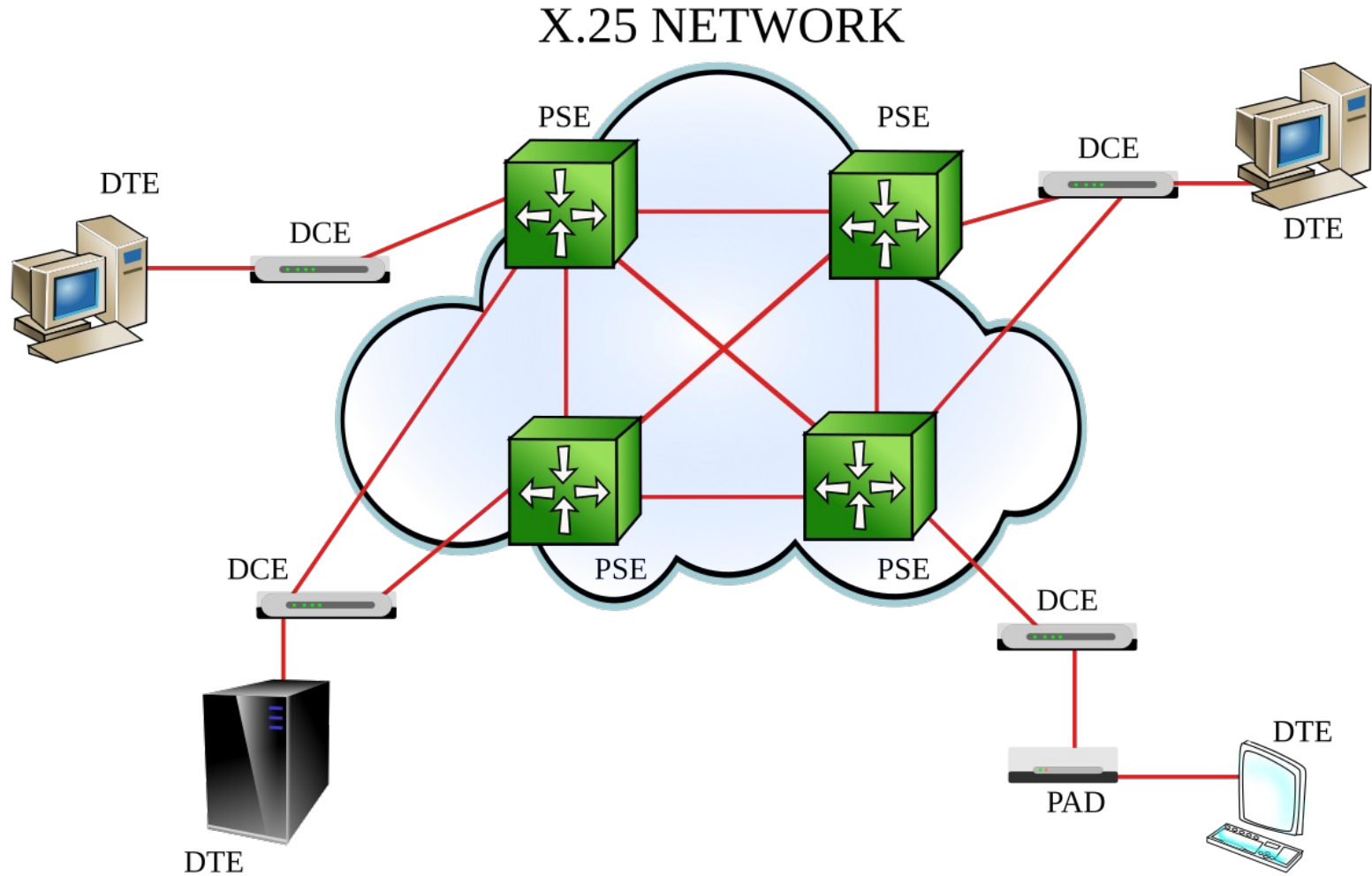
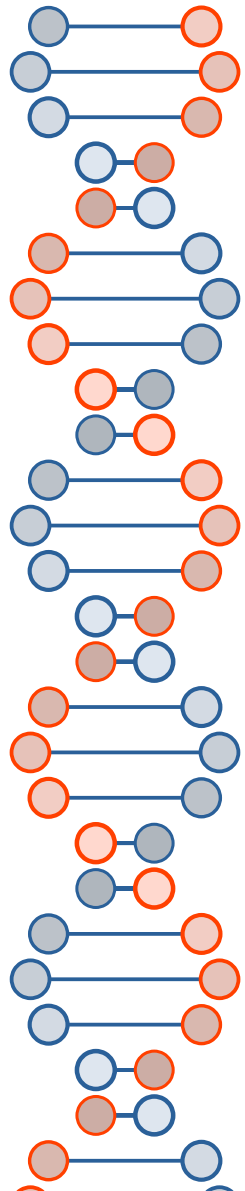
<https://www.youtube.com/watch?v=BkeXk9rBBrs>

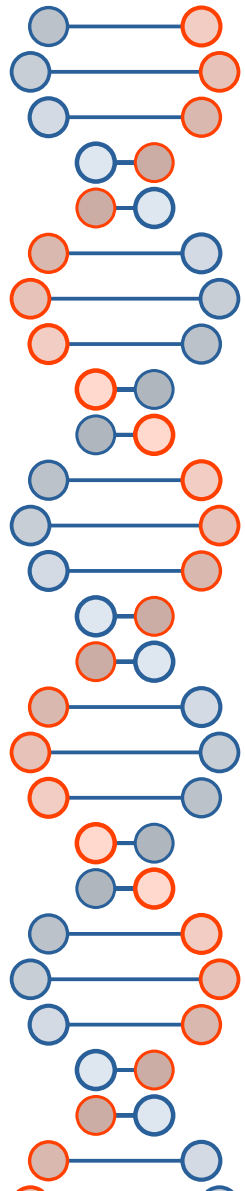


<https://www.paulgraham.com/bluebox.html>



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

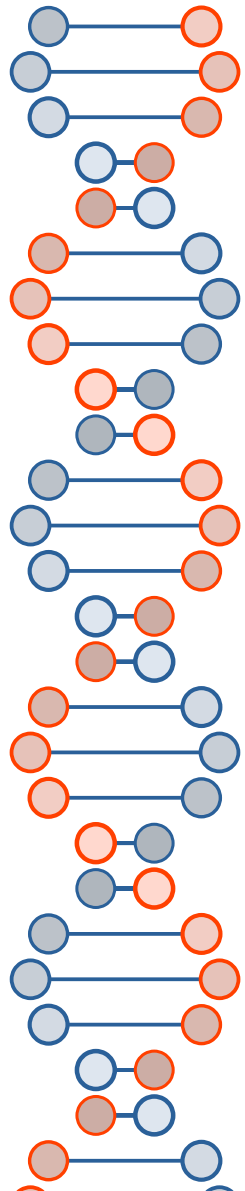




John “Corrupt” Lee



<https://www.listennotes.com/podcasts/the-gray-wolf/john-corrupt-lee-aka-john-j1qyldK5V4o/>



https://en.wikipedia.org/wiki/VAX_8000

```
$ JCP SHOW LINKS
Link JOB      Connect  -- JOB      Line virtual  NOH NOD NOT
Link PRT      Connect  -- QUE      Line virtual  NOH NOD NOT
Link CLOUDY   Connect  -- DNANJE   Line CLOUDY   NOH NOD NOT
Link FEDACH   Connect  -- TCPNJE   Line UCX      NOH NOD NOT
Link IMPVAX   Connect  -- DNANJE   Line IMPVAX   NOH NOD NOT
Link NJEVX1   Connect  -- TCPNJE   Line UCX      NOH NOD NOT
Link NJEVX2   Connect  -- TCPNJE   Line UCX      NOH NOD NOT
Link TSTVAX   Connect  -- DNANJE   Line TSTVAX   NOH NOD NOT
Link VAXSTN   Connect  -- DNANJE   Line VAXSTN   NOH NOD NOT
Link XLVII    Connect  -- DNANJE   Line XLVII    NOH NOD NOT
Link TSVMSA   Connect  -- DNANJE   Line TSVMSA   NOH NOD NOT
Link TSMST    Connect  -- DNANJE   Line TSMST    NOH NOD NOT
Link TSVMSZ   Active   -- DNANJE   Line TSVMSZ   NOH NOD NOT
$
$ SEND/COMMAND XLVII "CPQ IND"
$
(XLVII) - VAX 8650 running VAX/VMS V4.7
$
(XLVII) - Up since 14-APR-2020 01:10
$
$ █
```

<https://supratim-sanyal.blogspot.com/2020/04/vaxvms-47-with-decnet-link-to-hecnet.html>

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

WANTED BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME:MITNICK, KEVIN DAVID

AKS (S):MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex:MALE
Race:WHITE
Place of Birth:VAN NUYS, CALIFORNIA
Date(s) of Birth:08/06/63; 10/18/70
Height:5'11"
Weight:190
Eyes:BLUE
Hair:BROWN
Skin tone:LIGHT
Scars, Marks, Tattoos:NONE KNOWN
Social Security Number (s):550-39-5695
NCIC Fingerprint Classification: ...DOPM2OPM13DIPM19FM09



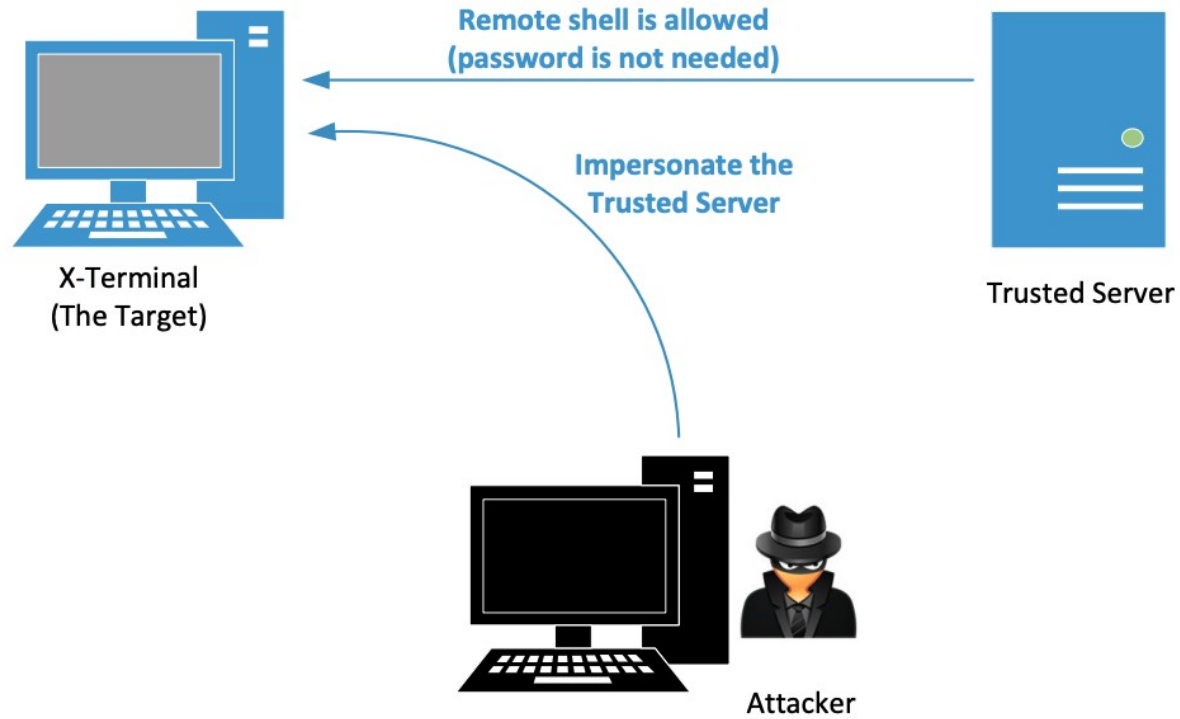


Figure 1: The illustration of the Mitnick Attack

<https://www.cs.swarthmore.edu/~chaganti/cs88/f22/labs/projects/mitnick/mitnick-attack.html>

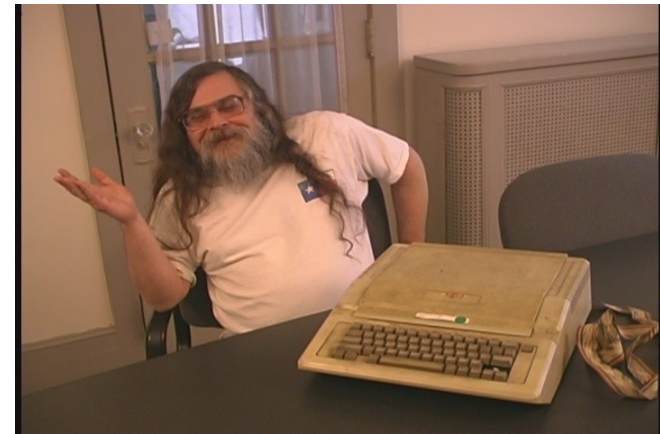
- Leslie Lynne Doucette, Electra, Tony the Trashman, Dr. Ripco, *etc.*



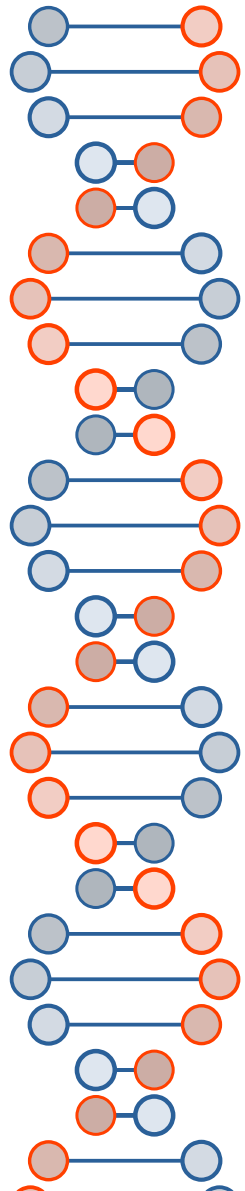
<https://www.lvswitches.com/product/ip-pbx-8000-IPPBX-systems.html>



<https://www.soundofdata.com/pbx-ip-pbx-and-virtual-pbx-what-is-what/>



<https://restincode.com/memorial.html?name=bruceesquibel>

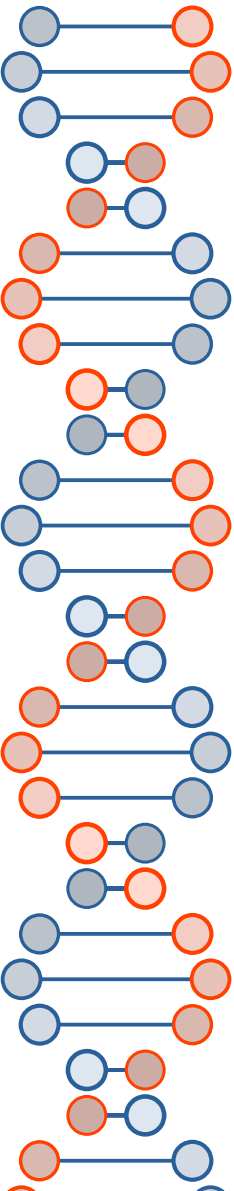


Learn a secret PIN one
digit at a time...

562_...

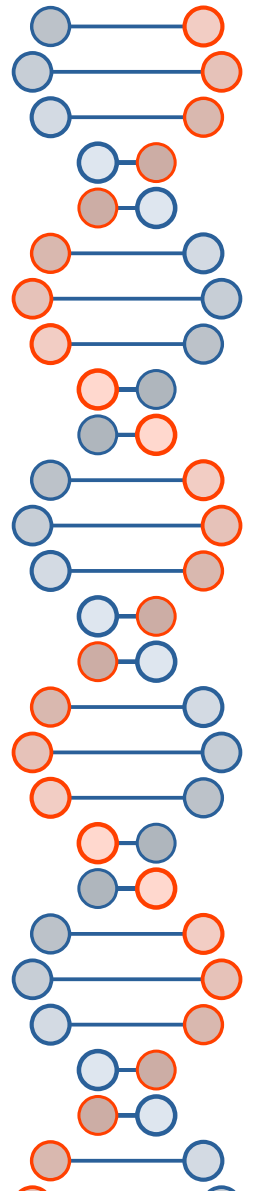


<https://en.wikipedia.org/wiki/Dumpster>



What we'll cover this semester

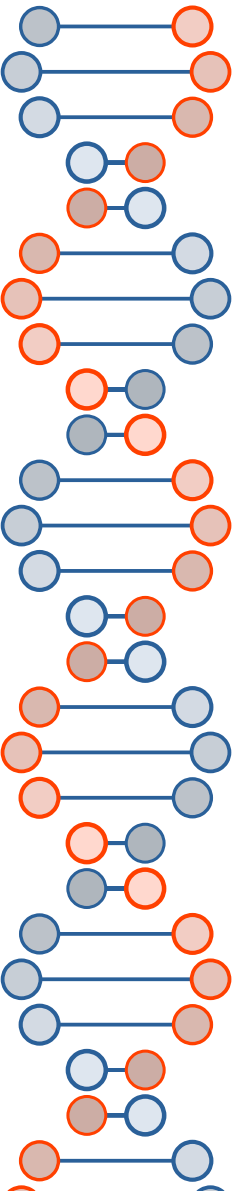
- Crypto
 - Hash functions, symmetric, asymmetric, quantum, *etc.*
- Network attacks and defenses
 - ARP poisoning, WiFi security, DNS security, *etc.*
- Network Intrusion Detection and related topics
 - NIDS evasion, information controls, malware, *etc.*



What we'll cover this semester

- Crypto
 - Hash functions, symmetric, asymmetric, quantum, *etc.*
- Network attacks and defenses
 - ARP poisoning, WiFi security, DNS security, *etc.*
- Network Intrusion Detection and related topics
 - NIDS evasion, information controls, malware, *etc.*

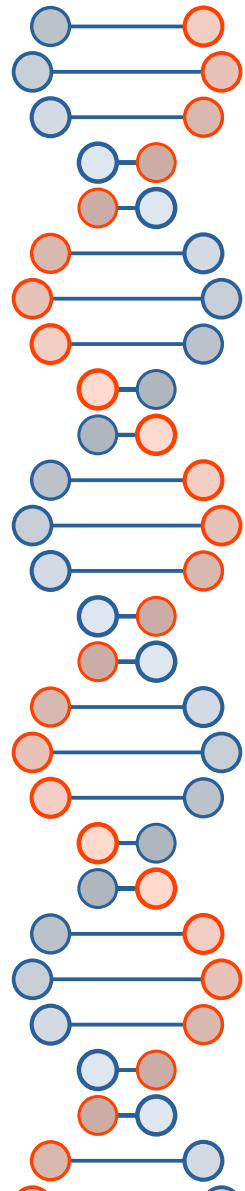
Foundations come from Galois, Fourier, Germain, Carnot (the son), Châtelet, and others who lived through the French revolutionary period.



What we'll cover this semester

- Crypto
 - Hash functions, symmetric, asymmetric, quantum, *etc.*
- Network attacks and defenses
 - ARP poisoning, WiFi security, DNS security, *etc.*
- Network Intrusion Detection and related topics
 - NIDS evasion, information controls, malware, *etc.*

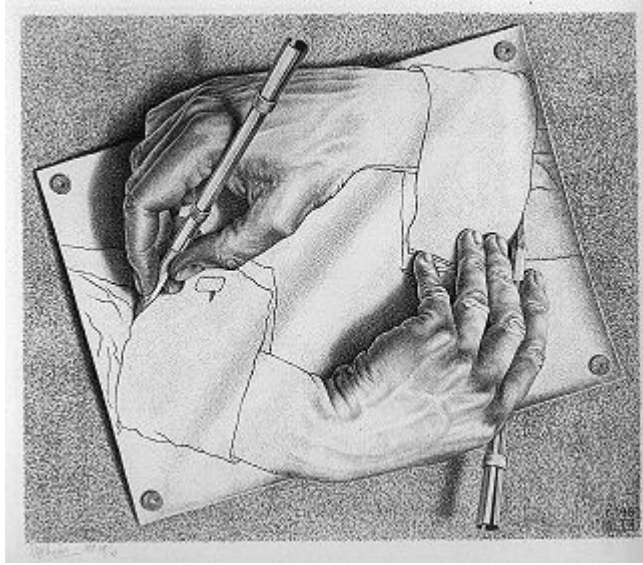
Dr. Who, the Master, the Legion of Doom, Masters of Deception, *etc.* used similar tricks in the wild long before network security research was a thing in academia.



What we'll cover this semester

- Crypto
 - Hash functions, symmetric, asymmetric, quantum, *etc.*
- Network attacks and defenses
 - ARP poisoning, WiFi security, DNS security, *etc.*
- Network Intrusion Detection and related topics
 - NIDS evasion, information controls, malware, *etc.*

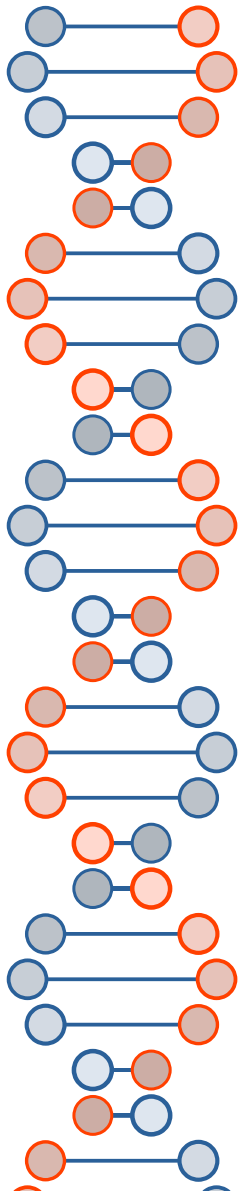
Kevin Mitnick, Corrupt, and others (*e.g.*, Legion of Doom and Masters of Deception) were doing things like connection hijacking and “getting root through the CPU” long before there was any academic research on these topics.



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

“Four hostile newspapers are more to be feared than a thousand bayonets.”

– Napoleon Bonaparte



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

“Where there’s a shell there’s a way.”

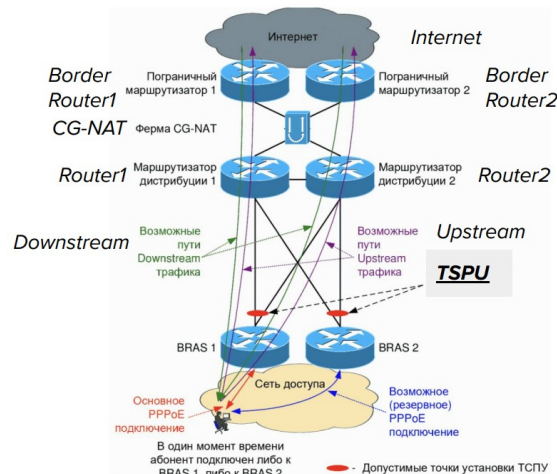
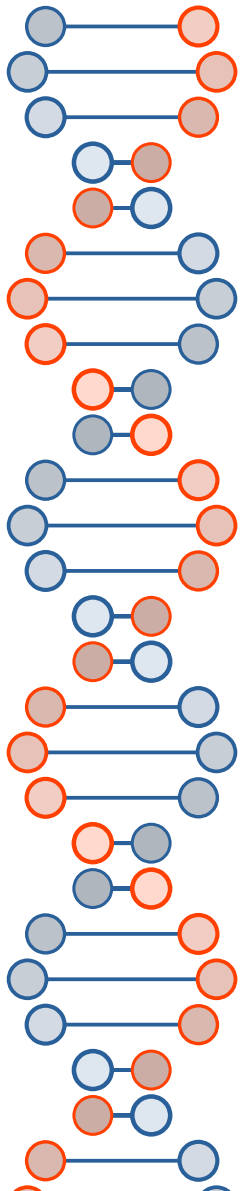
– 20th Century proverb
(based on a 17th Century English proverb)

LETHAL WEAPON



“It doesn't matter how beautiful your guess is. It doesn't matter how smart you are, who made the guess, or what his name is—if it disagrees with experiment, it is wrong.”

— Richard Feynman



==Phrack Magazine==

Volume Four, Issue Forty-Three, File 6 of 27

-:[Phrack Prophile]:-

This issue our prophile features a hacker who has been around forever, who's been there and done that, literally. His handle is Dr. Who.

Hacking is the art of esoteric quests, of priceless and worthless secrets. Odd bits of raw data from smashed machinery of intelligence and slavery reassembled in a mosaic both hilarious in its absurdity and frightening in its power.

<https://phrack.org/issues/43/6>

