SAINTCON

By James Reynolds

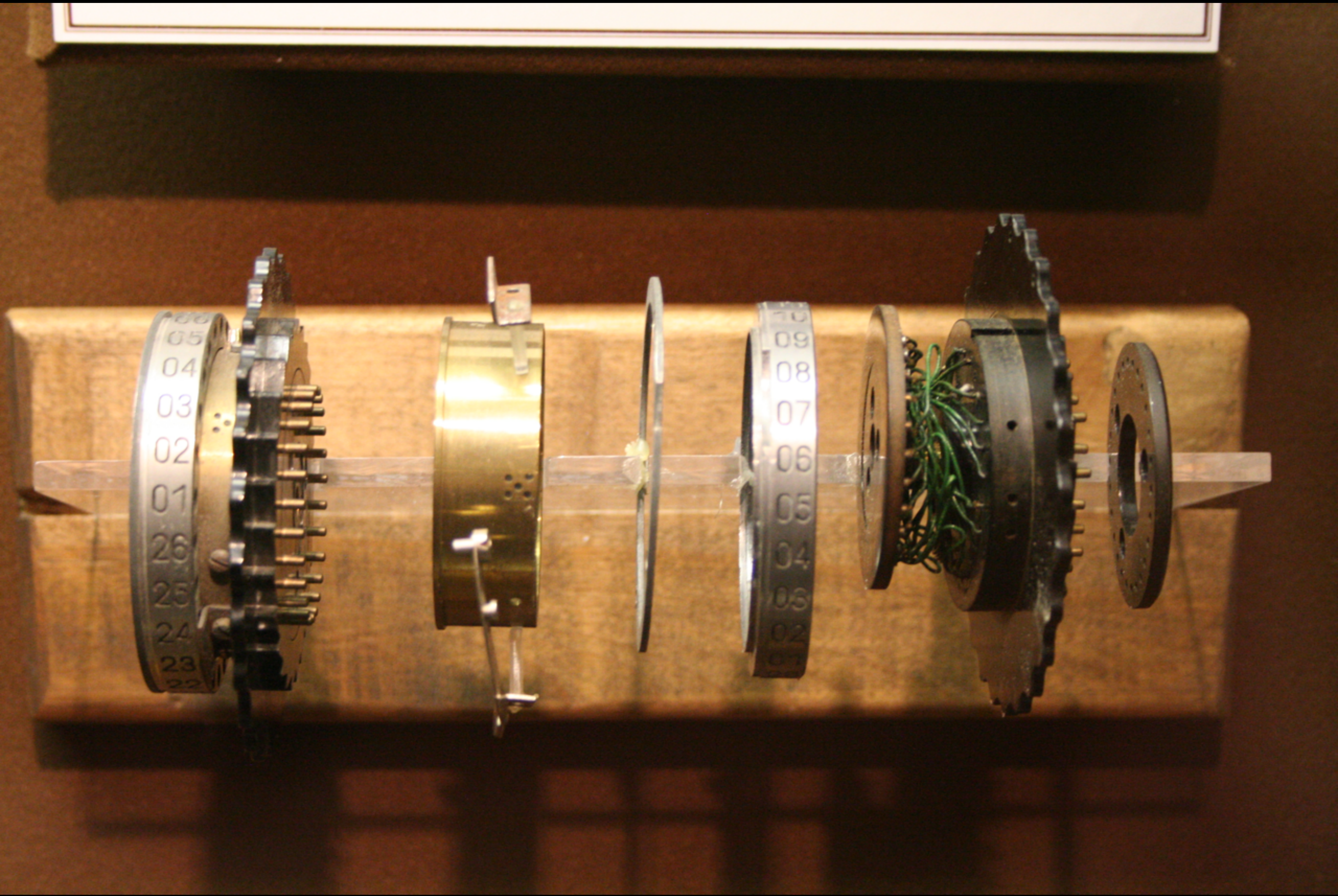
Other Local Conferences

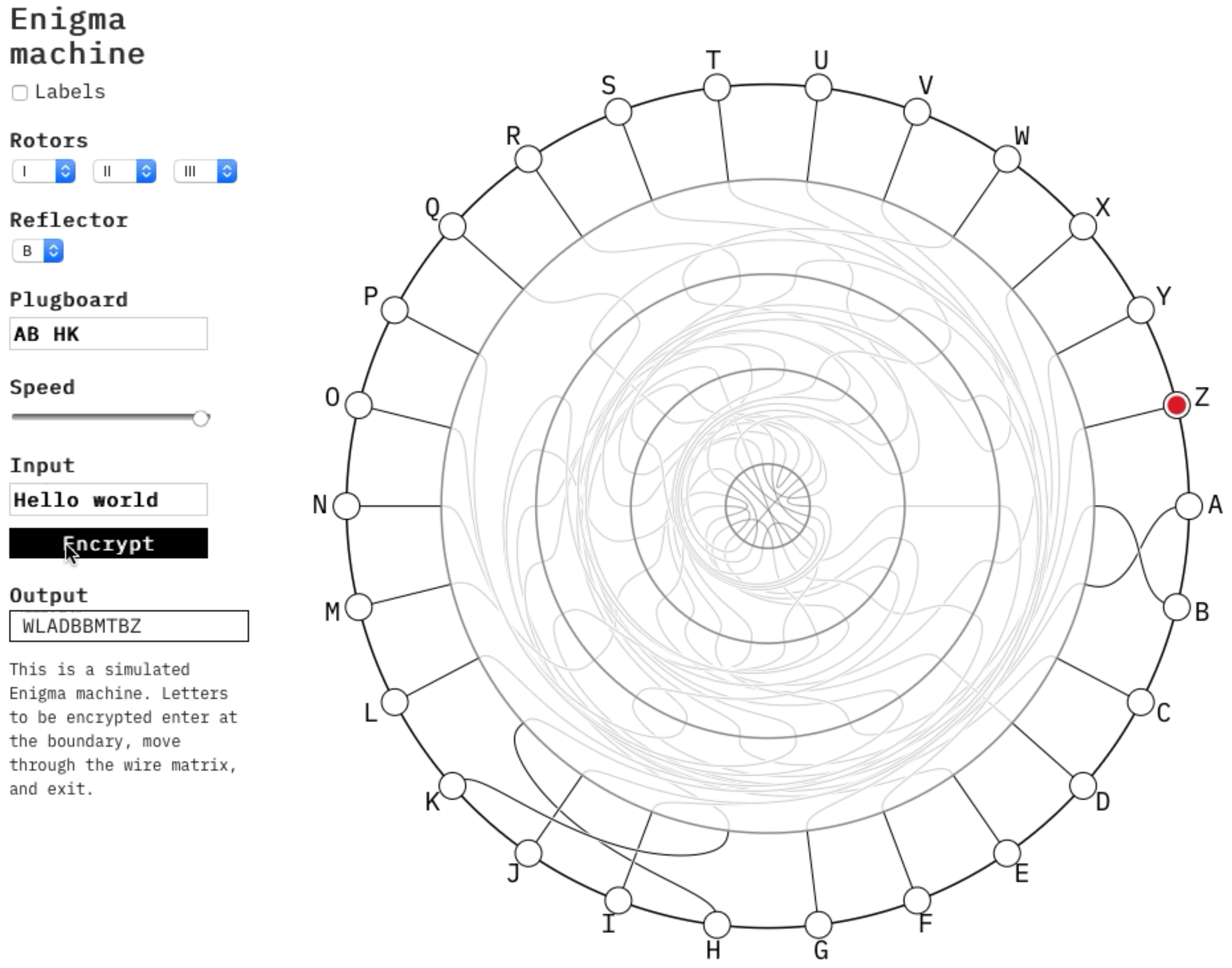
- SLC CyberSecurity (DataConnectors), Jan 30, free?
- Silicon Slopes, Jan 30-31, Salt Palace, $149 (early bird)
- Microsoft 365 Friday, Feb 7, Sandy, Free
- BSidesSLC, Mar 20-21, Sandy, ~$150-$200?
- UETN Tech Summit, Jun TBA (2 days), $150 (2019 sold out?)
- SLC Summit, Aug 25, University Marriott, free but limited
- SAINTCON, Oct 20-23, UVCC, $275 (2019 sold out)

ENIGMA

The Enigma

- Invented at the end of World War I
- Used by the Axis to encrypt Morse Code radio transmissions
- Something like 1.6x10^20 different settings (depending on the model)


06
05
04
03
02
01
26
25
24
23
22
10
09
08
07
06
05
04
03
02
01



Enigma machine

☐ Labels

Rotors: I II III

Reflector: B

Plugboard: AB HK

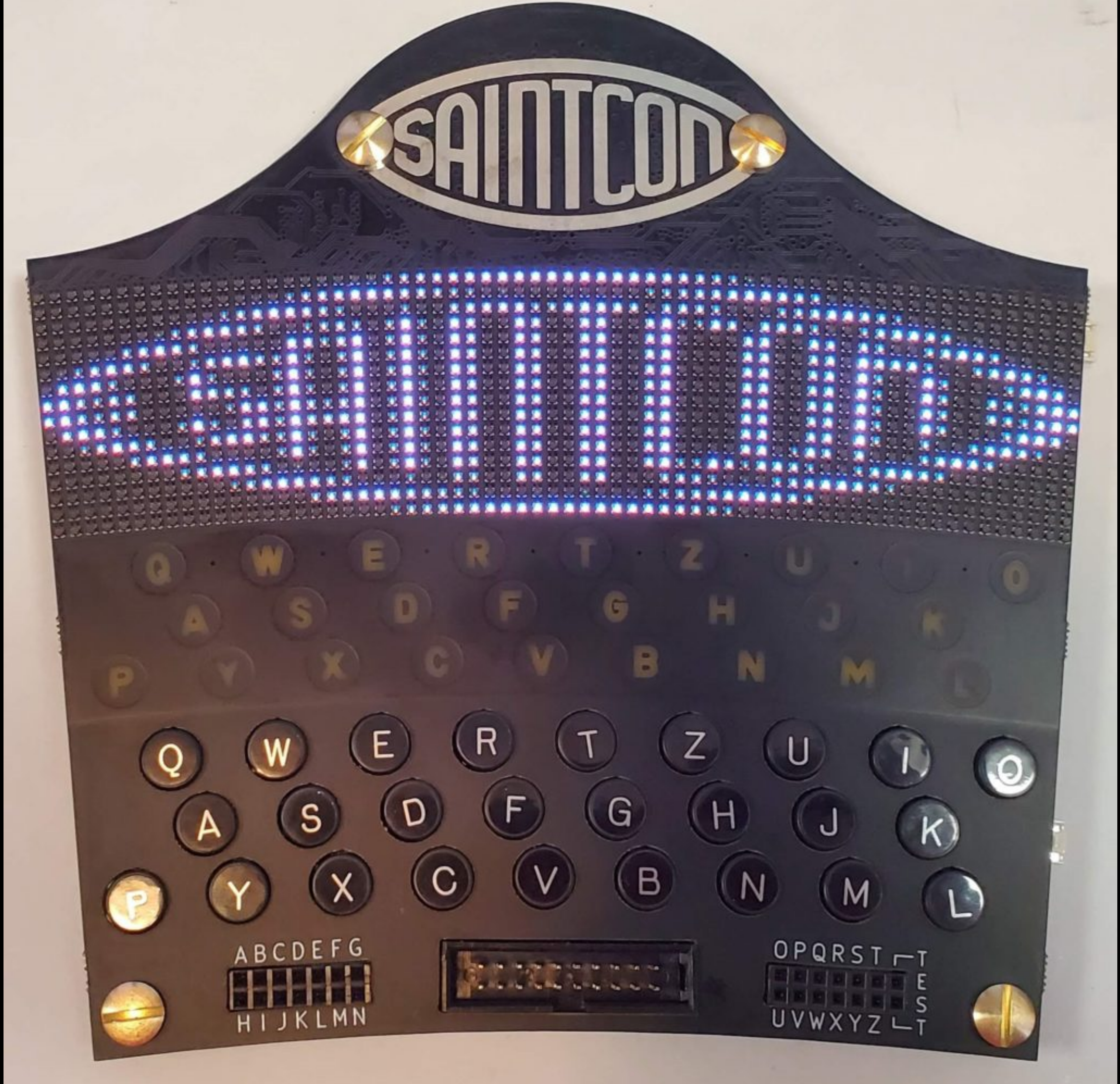
Speed

Input: Hello world

Output: WLADBBMTBZ

This is a simulated Enigma machine. Letters to be encrypted enter at the boundary, move through the wire matrix, and exit.

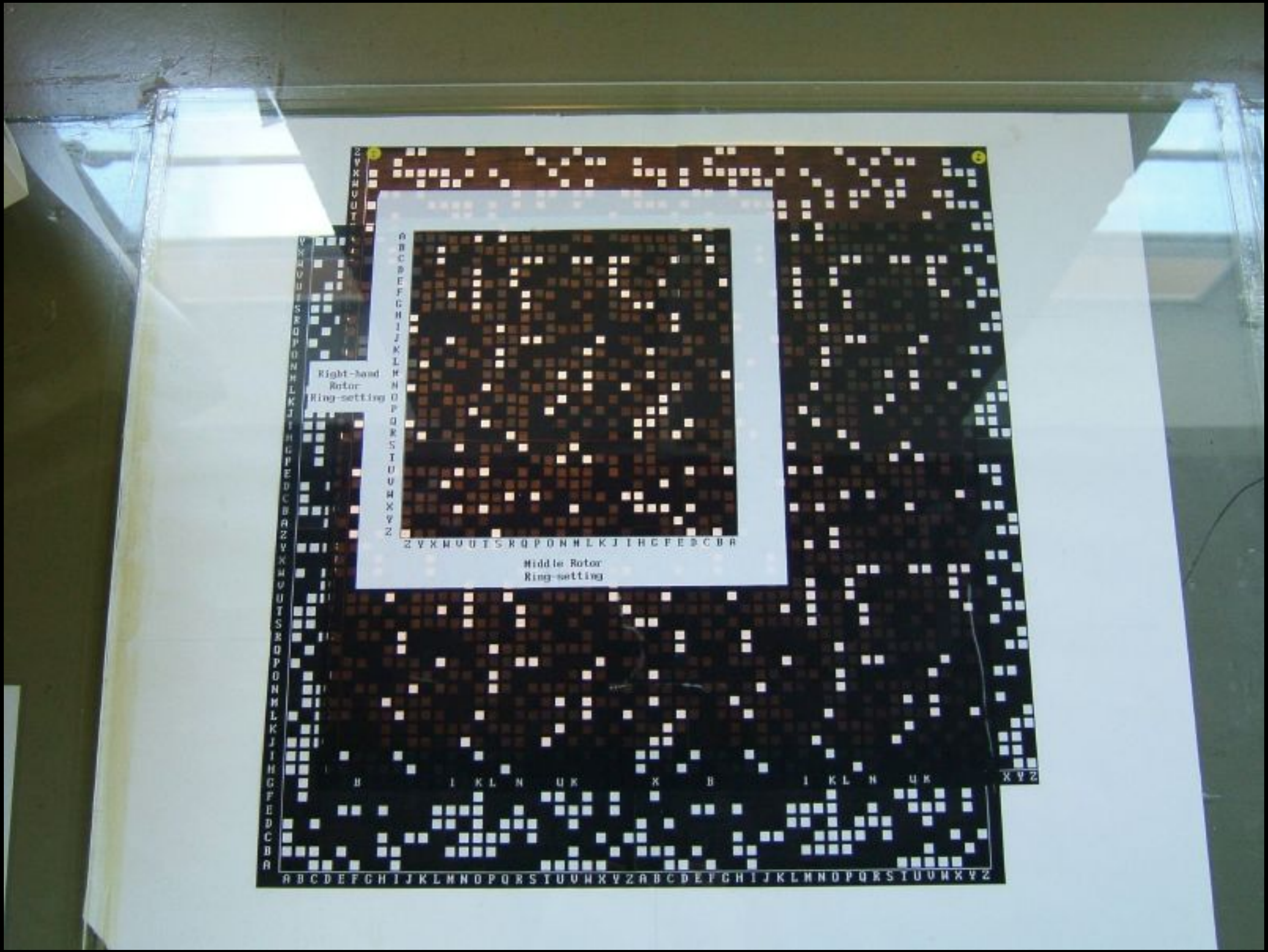
https://observablehq.com/@tmcw/enigma-machine


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

SECURITY TEAM
SECURITY TEAM
#love2 eduroam
NFC IMPLANT ACTIVATED
SAINTCON
For God and Country
GIVE TO ANYBODY
GOVERNMENT DOES
SOMEBODY ELSE.
Big Sky Racks, Inc.
BATTLE BORN
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18

World War II

- Nazi flaws, mistakes, and capture of key tables made it possible for the Allies to decrypt the majority of Nazi communications
- Was cracked as early as January 1933 by the Polish
- The French cracked it w/ the help of a Nazi traitor
- Ultra at Bletchley Park cracked improvements
    - 10,000 personal, 3/4 women, mostly mathematicians, engineers, physicists
    - Records were not declassified until 1978

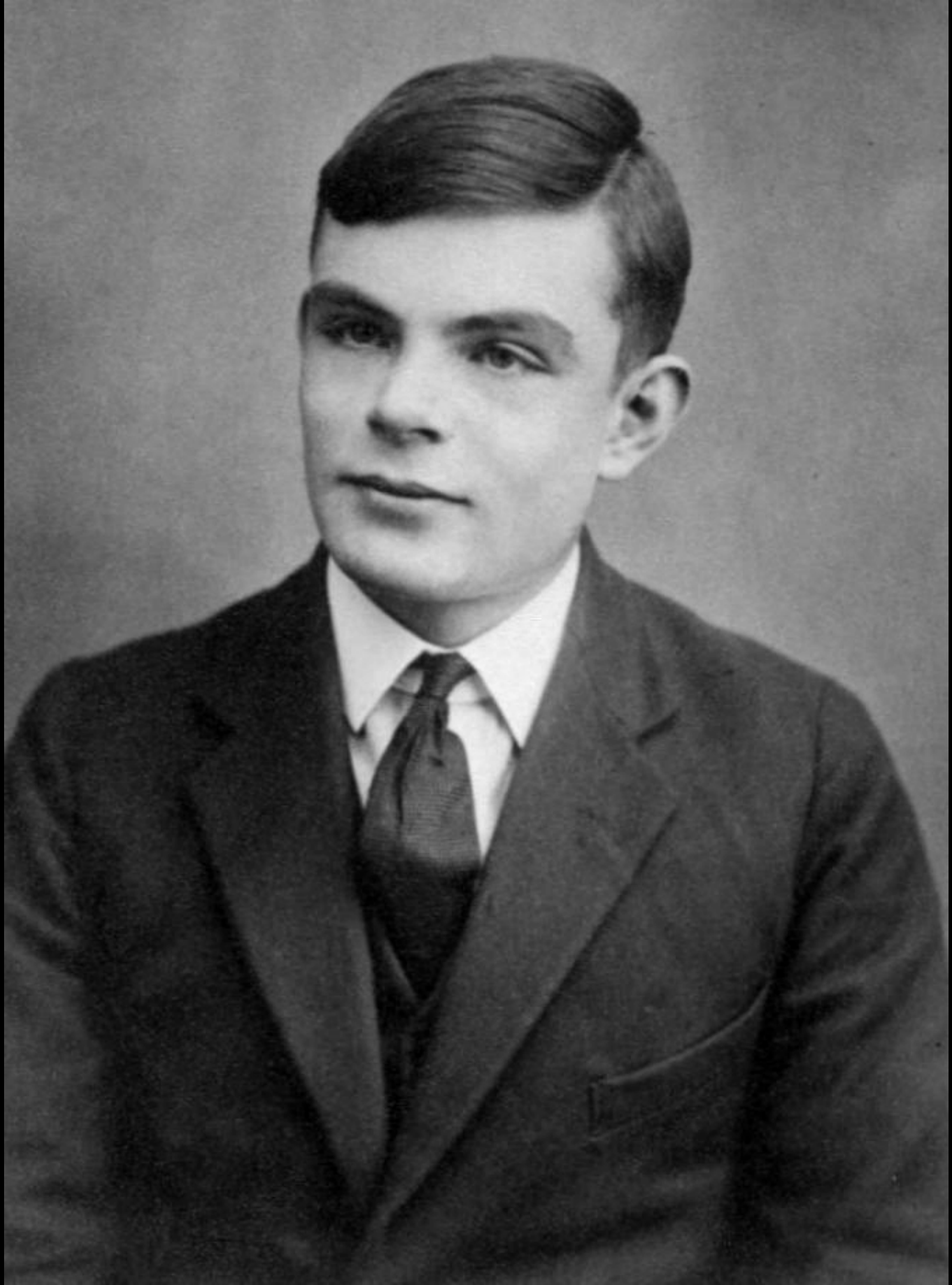

Right-hand Rotor Ring-setting
Middle Rotor Ring-setting
ZYXWVUTSRQPONMLKJIHGFEDCBA
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

Zygalski sheets

What went wrong?

- They picked bad keys:
  abcd, hit-ler, lon-don, mad-rid, swear words
- Known-plaintext attacks (KPA or “crib”)
  - “Happy B-Day Hitler”, “Heil Hitler”, weather, “Nothing to report”, etc.
  - RAF “seeded” the ocean with mines, Germans radioed in the coords
- Near duplicate messages sent w/ the same settings
- They refused to admit their “infallible” technology was cracked by “inferior” races, they believed there were spies in their High Command

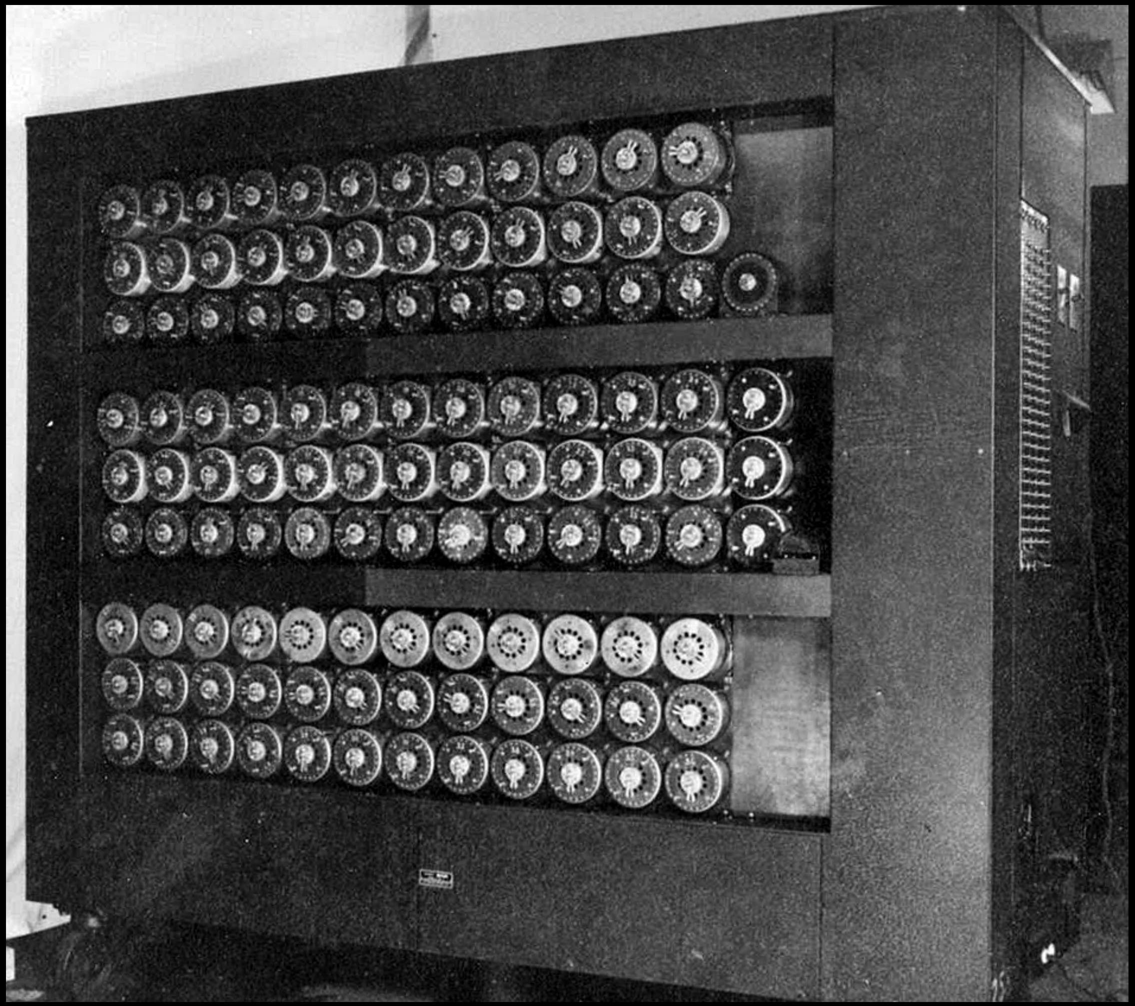
Alan Turing



Ultra at Bletchley Park

- Alan Turing made the Bombe in 1939 to crack the Enigma

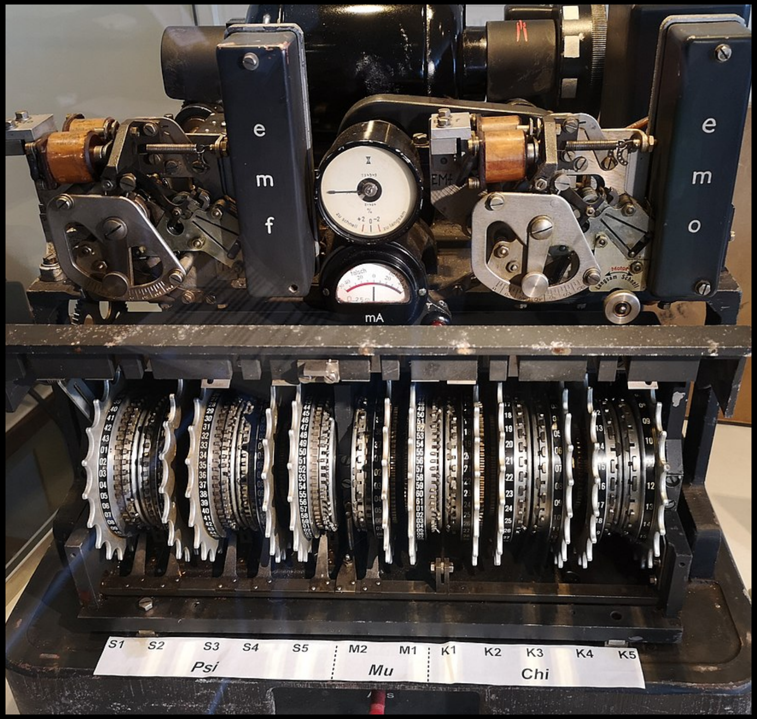
- “The misleading of the mind of Hitler became a major industry in Britain, a very elegant industry too.” — Anthony Cave Brown



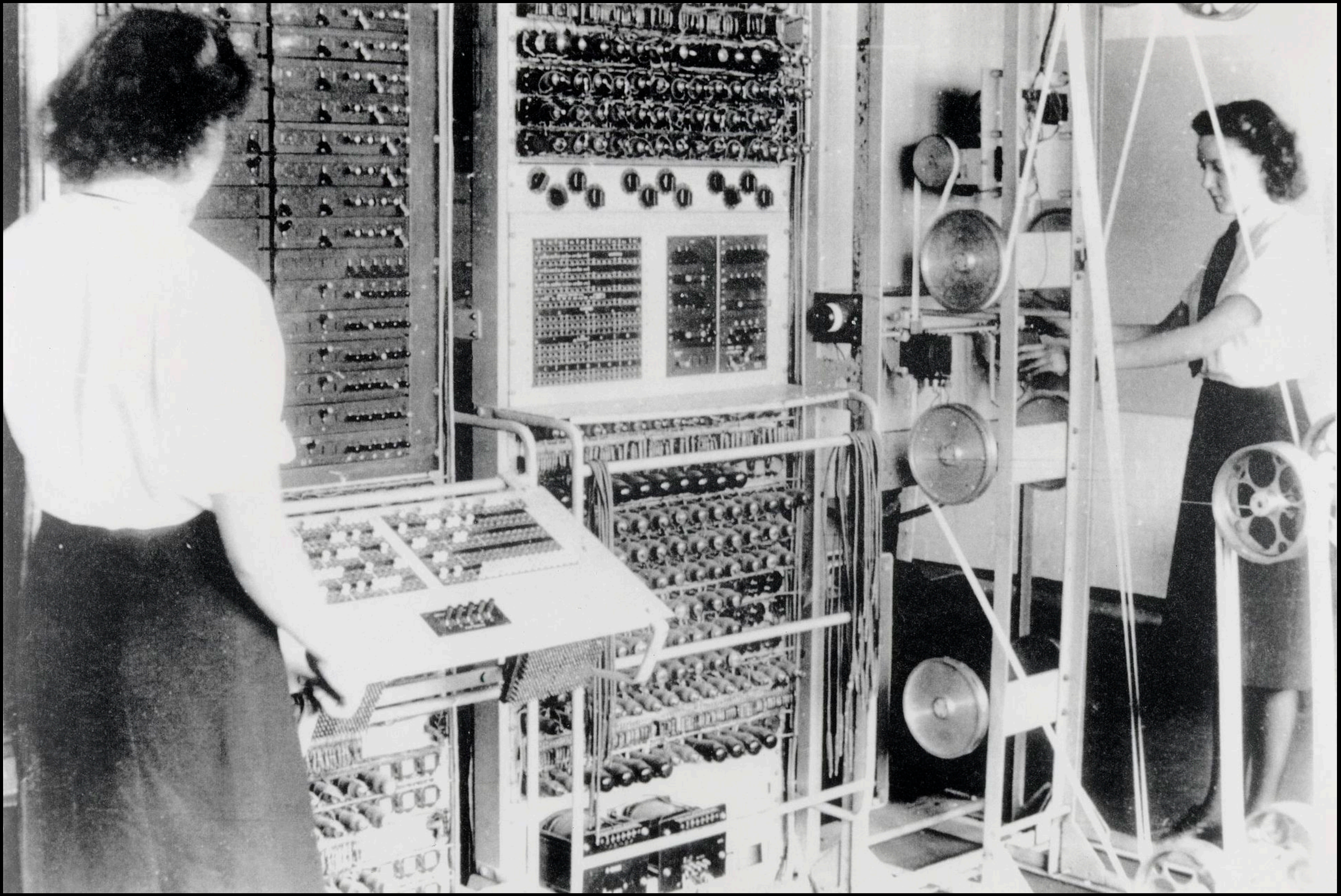
The Bombe

Also at Bletchley Park...

- Tommy Flowers made the Colossus Mk I in 1943 and Mk 2 in 1944 (in time for D-Day)
    - The first digital computer (sorry ENIAC)
    - Was not general purpose
    - Classified until mid-1970's
    - Cracked the Enigma's successor, the Lorenz
    - All 10 were destroyed in the 1960's



The Lorenz



The Colossus

Consequences

- Polish knew Hitler’s plan for world domination in 1937
- France knew Hither would invade via the Ardennes
- Dunkirk rescue
- Located the Battleship Bismarck and it was sunk (1990’s declassified)
- Saved merchant ships
- Rommel’s defeat in Africa
- D-Day

The Battleship Bismarck

Also of note

- Navajo code talkers
  - The only spoken military code never cracked
  - Faster than machine encryption
  - The Battle of Iwo Jima victory

- US cracked the Japanese code (JN-25)
  - Japanese arrogance was just like the Nazi’s
  - June 4, 1942, Battle of Midway ambush and much more

Impact

- At a minimum, saved about 2 million lives by shortening the war by 2 years
- Might have tipped the balance of power, leading to victory
- US codebreakers became the NSA and CIA
- Computers now exist
- Triumph of the Nerds indeed…

Lessons Learned?

- Don’t pick bad passwords
- Go watch history documentaries, they’re awesome
  - BTW, Hollywood isn’t very accurate, e.g. *Enigma* (2001) and *The Imitation Game* (2014)
- This is why the military is freaking out about encryption and surveillance

BACK TO THE FUTURE

Why is security important?

- Risk = Threat x Vulnerability
    - Risk - what you can potentially lose
        - Money, information, reputation, legal
    - Threat - thing that can potentially exploit you
        - Hard to determine, there are always unknowns
    - Vulnerability - how you can be exploited

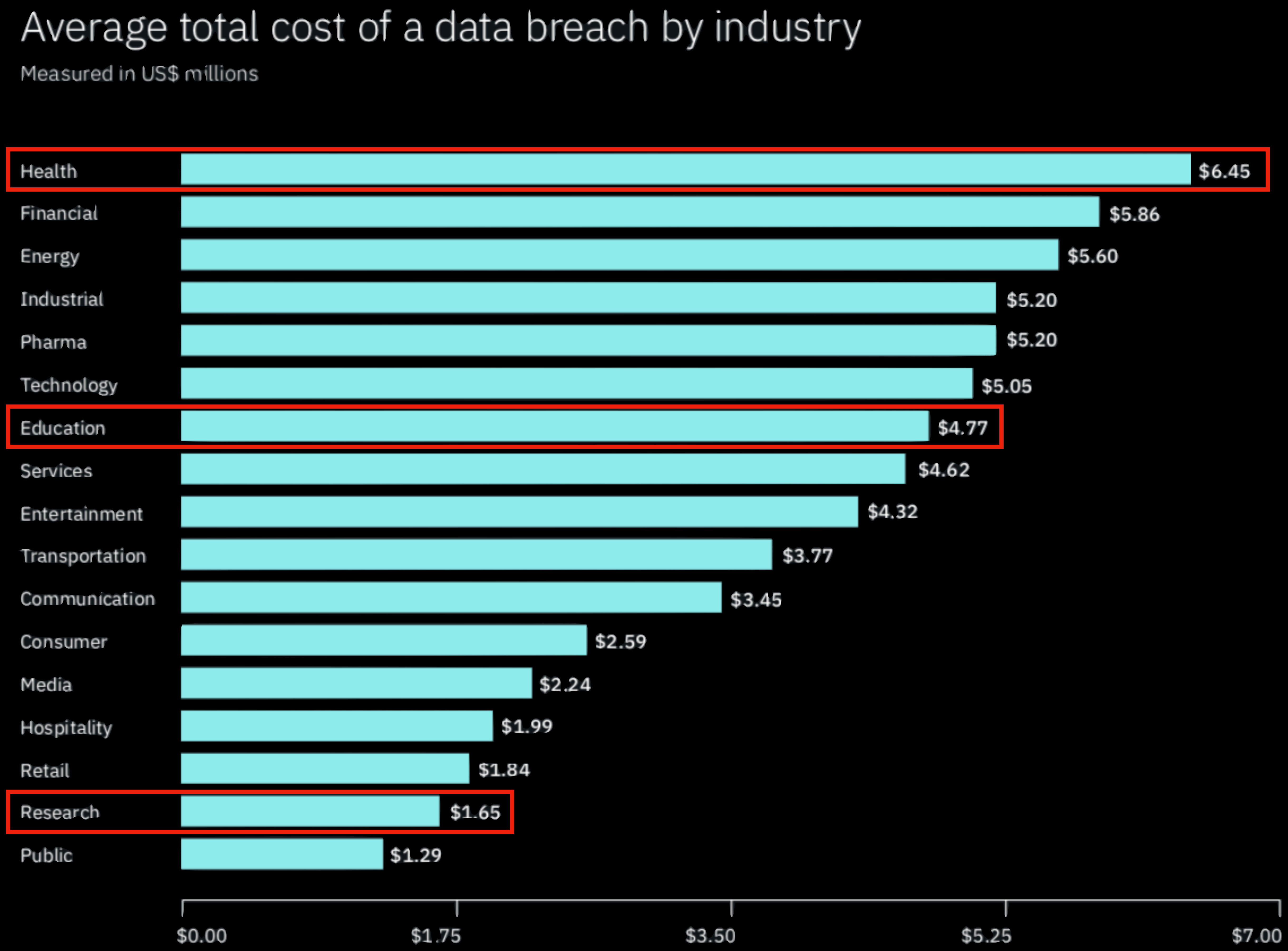
Some Risks

- Shut down services (e.g. ransomware or DDoS)
- Steal, tamper, or delete research information
    - Hello China
- The unknown (changing direct deposit was an unknown)
- Stealing PII

PII Breach Statistics

- Average of 212 days to detect a data breach (education)
- Average of 71 days to contain a breach (education)
- 53% of breach detections were by others (mostly law enforcement)
- $142/record average cost (education)

https://www.ibm.com/security/data-breach (2019 report)



Average total cost of a data breach by industry

Measured in US$ millions

https://www.ibm.com/security/data-breach (2019 report)

What is the cost?

- 31% Detection and escalation
  - Forensics, audits, crisis teams
- 6% Notification
- 27% Post breach cost
  - Help desk, credit monitoring, legal costs, fines
- 36% Lost business cost
  - Downtime, lost customers, damaged reputation

https://www.ibm.com/security/data-breach (2019 report)

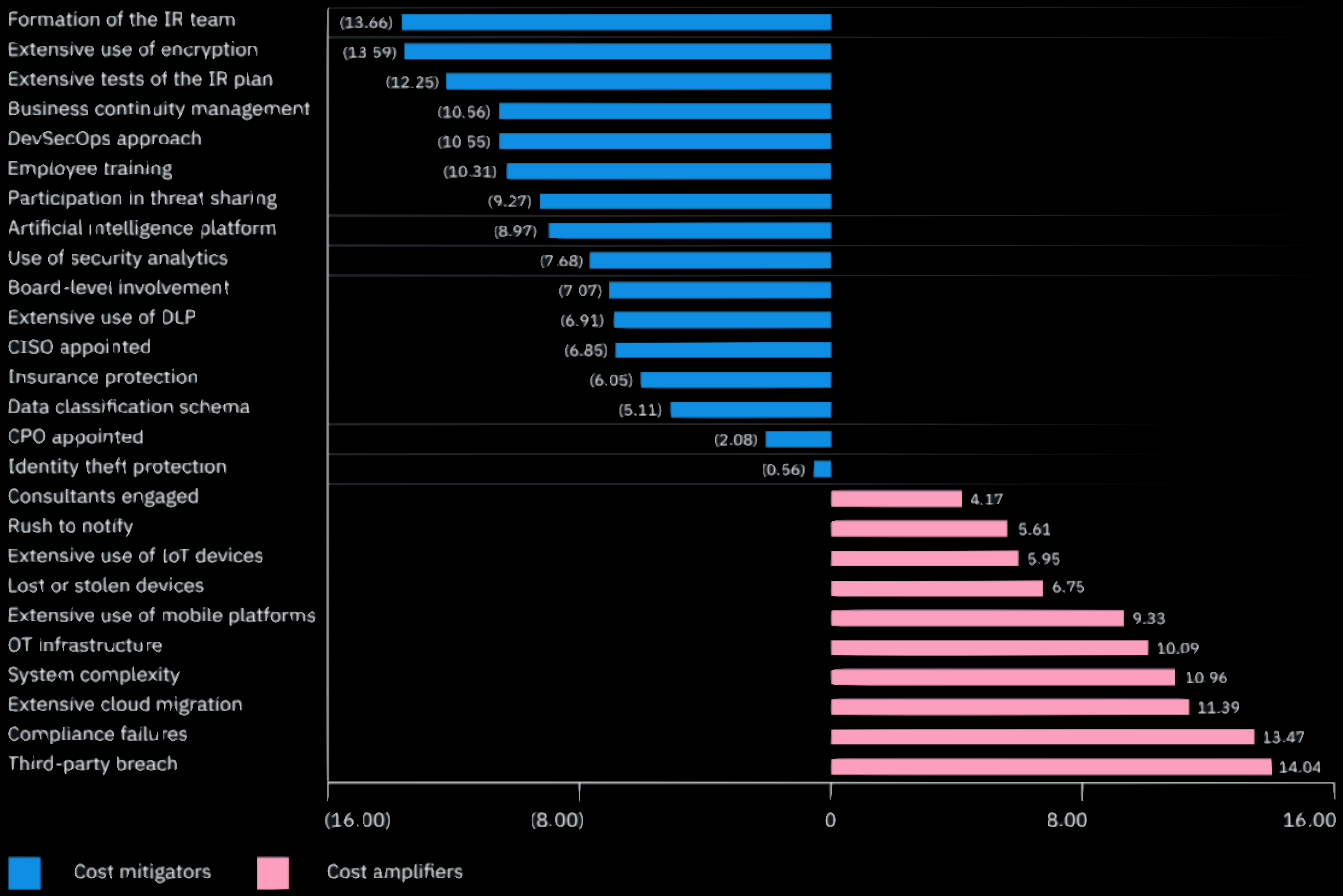
Types of breaches

- 51% of breaches from malicious or criminal attack
  - Malware, insiders, phishing/social engineering, SQL injection
- 25% from IT or process failure
- 24% from negligent employees or 3rd parties

https://www.ibm.com/security/data-breach (2019 report)

Factors impacting the per record cost of a data breach

Change in US$ from average global cost per record of US $150



https://www.ibm.com/security/data-breach (2019 report)

Factors

- Best things
  - Having an incident response team and testing them
  - Encryption
  - Security mindset
  - Employee training
- Worst things
  - IT complexity
  - Cloud migration

https://www.ibm.com/security/data-breach (2019 report)

Incident Response Team

- Researches and responds to events
- Participates in vulnerability assessment and audits
- Performs forensics, monitoring, training
- Works with law enforcement
- Basically ISO

Who is responsible?

- ISO is responsible for the entire campus
- Individual departments are responsible for the **appropriate security controls** and works with ISO when needed
- What are the appropriate security controls?
- “University of Utah Information Security Policy. Rev 4” — https://regulations.utah.edu/it/4-004.php

Video

4-004A highlights

- “The University does not, absent consent, specifically target an individual user to monitor… except…
- Utilizing Signature-based detection and automated monitoring…
- [and] based on reasonable suspicion of illegal behavior… (UIT will do this monitoring)
- [and] in the case of a user who is unable to perform University duties due to medical illness or emergency, unavailability, or refusal to perform duties.”

4-004C highlights

- Read the whole thing since this might be the most important policy
- Restricted Data (encryption required when at rest)
  - PII, PHI, PCI, financial or donor information
- Sensitive Data (encryption strongly recommended)
  - Intellectual property, employee/student info, litigation docs, contracts, building and utility details
- Public Data (encryption encouraged)
  - U of U history, business contact data, directory, maps

4-004E highlights

- The University shall ensure that no single individual can access, modify, or use information systems without authorization or detection to reduce the opportunities for unauthorized or unintentional changes

- The University shall physically, logically or virtually separate test, development and production environments to reduce the risk of unauthorized access and/or changes

4-004G highlights

- Anti-malware and/or endpoint security scanning must be configured to run automatically
- In a situation where a patch cannot be installed… an exception must be filed
- When a vendor releases a patch or update… risk mitigation shall be taken
- The University will implement the… means for authenticating authorized users, limit the number of unsuccessful log-on attempts, record unsuccessful log-on attempts, auto-lock and/or auto-logoff sessions due to inactivity, issue alarms when security requirements are breached

4-004H highlights

- Reconfiguration of a remote user's IT resource for the purpose of split-tunneling or dual-homing is not permitted at any time (Thou shalt not alter VPN settings)

- All IT resources that are connected to the University's internal network via remote access technologies must have up-to-date anti-malware software implemented.

4-004I highlights

- Risk remediation activities must be monitored periodically
- Network services agreements will include required security features
- The University will segregate groups of information assets, IT resources, servers, information systems, and users within its network.
- The network security perimeters will be configured to control access and information flow between the domains, filter traffic between the domains, block unauthorized access

4-004J highlights

- Systems that create, store, process or maintain confidential data must log
  - User ID, logins and logouts, all login attempts, file permission changes, system config changes
  - Date and time of administration event, login id, service, etc
- Audit logs… shall be reviewed periodically in accordance with published Procedures, and at a minimum on a quarterly basis
- Read/write access to the log files is a limited group of authorized personnel

4-004K highlights

- Define the required level of backup for each Information System or Server
- Establish an off-site storage location for backups
- Test, and update as necessary, backup procedures
- Test, and update as necessary, recovery procedures to ensure timeliness and effectiveness of recovery

“We aren’t a target”

- What do you do when people say they have nothing worth hacking over or that they don’t require the appropriate security controls?

Car Crash Analogy

- The risk of you killing someone while driving a car is low
- But because the worst consequences are so high, we have all kinds of rules like speeding and safety laws

House Fire Analogy

- The risk that your home will burn down is low
- But because the worst consequences are so high, we have all kinds of rules and precautions like fire alarms, fire extinguishers, fire resistant everything, power and gas regulations, etc.

Computer Analogy

- The risk of getting hacked is low, like crashes and fires
- What’s the worst consequences?
  - Doesn’t lead to deaths or physical destruction (usually)
  - Although unlikely, financial and repetitional ruin are possible
  - Even in the best case you will lose time cleaning up
- The industry ***has*** **best practices** for ***everyone***

What are the best practices?

- Assume it will happen
- Train yourself
- Increase Awareness
- Monitor
- Protect Devices
- Protect Data

Increase Awareness

- Create a policy
- Initial user training
- Annual user training
- Phishing drills
- Pentests and other drills

Monitor

- Inventory of all network devices
  - Intermapper, nmap
- Read and react to the Qualys scans
- Improved logging
  - osquery, cmdReporter, Elastic Beats
- Security Information and Event Management (SIEM)
  - Elastic SIEM

Protect Devices

- Firewall
  - Contact UIT, device firewalls
- Manage passwords
  - 1Password, KeePass, KeyChain
- Endpoint patching
  - MDM and UEM (Unified Endpoint Management)
  - Jamf, Ivanti (LANDESK), SCCM, Tanium, PDQ, FileWave

Protect Devices

- Use endpoint security software (anti-virus or other)
    - Anti-virus or Objective-see’s
- Multi-factor authentication on your servers
    - Duo
- Intrusion Detection and Prevention System (IDS/IPS)
    - Snort, Nessus

Protect Data

- Inventory and categorize information
- Backup onsite and offsite
  - TimeMachine, Arq, Amanda
- Encrypt
  - FileVault, https

- You’ve done nothing except trust the vendors

- One good fire will burn the whole thing down (except the church walls—at least the beliefs will be protected…)

- You’ve talked about it
- Initial training
- Read and react to the Qualys scans
- Basic Backup

- Has a policy and plan
- Annual training
- Inventory of all network devices
- Passwords managed
- Basic Firewall

- Endpoints patched
- Information is inventoried and categorized
- Segregated networks
- Uses endpoint security software (AV)

- Phishing drills
- Logging
- MFA
- Encrypted data

- Pentests
- SIEM
- IDS

- You work for the NSA and you should be talking, not me
- Or your users hate you and can’t get anything done

How to use the tools

- The tools shine light in the dark: network traffic and background tasks

- The goal is to find the needle in the haystack

- To find anomalies you have to know what “Normal” is

- To know what “Normal” is, you have to measure it

The goal

- Goal 1
  - Preventing breaches is a good goal, but you should plan on it happening
  - Detection time + reaction time < attack completion time

- Goal 2
  - Random attackers look for the easiest targets
  - Make yourself a difficult target

HEY, TOM, I JUST REALIZED THAT I DON'T NEED TO OUTRUN THE BEAR; I ONLY NEED TO OUTRUN YOU.

And no one ever heard from the Anderson brothers again.

- If you’re not a security expert, should you *really* decide the best practices don’t apply to you?