data-ppf.github.io 2021-02-23

lecture 7 of 14: from Bletchley Park to Bell Labs

chris wiggins + matt jones, Columbia

logistics

- hw2 assigned

logistics

- hw2 assigned
- Op-Ed assigned, due mar 12

logistics

- hw2 assigned
- Op-Ed assigned, due mar 12
- want to know more? please ask! (Slack best, email 2nd best)

logistics

- hw2 assigned
- Op-Ed assigned, due mar 12
- want to know more? please ask! (Slack best, email 2nd best)
- today: lots of material, won't read all quotes sorry

student reactions: some data on people, ideas, things

```
153 women / gender / gendered
134 computing / computer / computers / colossus / machine
50 turing
39 labor
35 abbate
35 statistics / mathematician
35 bayes / bayesian
26 wrens
14 mcgrayne
13 bletchley
11 government
3 hidden figures
```

subjective

"Turingery was a paper-and-pencil method, 'more artistic than mathematical. . . . [You had to rely on what] you felt in your bones,' according to Turingery player William T. Tutte. The first step was to make a guess and assume, as Bayes had suggested, that it had a 50% chance of being correct"

ghost work Q&A

- Q: “Who are the wrens of today’s modern computational environment and how can we recognize/celebrate/elevate their contributions and make sure that the field is equally accessible to them as to any other group?”

ghost work Q&A

- Q: “Who are the wrens of today’s modern computational environment and how can we recognize/celebrate/elevate their contributions and make sure that the field is equally accessible to them as to any other group?”
- “Who are the current equivalents of the wrens operating the Colossi?”

ghost work Q&A

- Q: "Who are the wrens of today's modern computational environment and how can we recognize/celebrate/elevate their contributions and make sure that the field is equally accessible to them as to any other group?"
- "Who are the current equivalents of the wrens operating the Colossi?"
- A1: "artificial artificial intelligence" (for example with Amazon's Mechanical Turk).

ghost work Q&A

- Q: “Who are the wrens of today’s modern computational environment and how can we recognize/celebrate/elevate their contributions and make sure that the field is equally accessible to them as to any other group?”
- “Who are the current equivalents of the wrens operating the Colossi?”
- A1: “artificial artificial intelligence” (for example with Amazon’s Mechanical Turk).
- A2: you! (cf. “Should We Treat Data as Labor? Moving beyond ‘Free’” Arrieta-Ibarra et al. 2018)

ghost work Q&A

- Q: “Who are the wrens of today’s modern computational environment and how can we recognize/celebrate/elevate their contributions and make sure that the field is equally accessible to them as to any other group?”
- “Who are the current equivalents of the wrens operating the Colossi?”
- A1: “artificial artificial intelligence” (for example with Amazon’s Mechanical Turk).
- A2: you! (cf. “Should We Treat Data as Labor? Moving beyond ‘Free’” Arrieta-Ibarra et al. 2018)
- see also “Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass” and “Temp: How American Work, American Business, and the American Dream Became Temporary” L. Hyman, 2018

CS/DS born of war

- WWII brought the fundamental achievement of data science and computer science and then expanded the idea to various disciplines

CS/DS born of war

- WWII brought the fundamental achievement of data science and computer science and then expanded the idea to various disciplines
- The birth of computer data science, mass surveillance, and the military-industrial complex can all be seen as legacies of the war.

CS/DS born of war

- WWII brought the fundamental achievement of data science and computer science and then expanded the idea to various disciplines
- The birth of computer data science, mass surveillance, and the military-industrial complex can all be seen as legacies of the war.
- the very basis of our modern computational system and theory exists as framed by the necessities of war.

CS/DS born of war

- WWII brought the fundamental achievement of data science and computer science and then expanded the idea to various disciplines
- The birth of computer data science, mass surveillance, and the military-industrial complex can all be seen as legacies of the war.
- the very basis of our modern computational system and theory exists as framed by the necessities of war.
- many of the modern fields of study we have today, such as cryptography and computing were a direct result of the war effort.

academic-military-industrial complex

from: “Mina Rees and the Funding of the Mathematical Sciences”, 2002

- During World War I, scientists were inducted into the army, and military laboratories were built to conduct war related research. By contrast, in World War II researchers remained civilians, and research was conducted under government contract at universities and institutes

academic-military-industrial complex

from: "Mina Rees and the Funding of the Mathematical Sciences", 2002

- During World War I, scientists were inducted into the army, and military laboratories were built to conduct war related research. By contrast, in World War II researchers remained civilians, and research was conducted under government contract at universities and institutes
- [In WWII,] The OSDR used the long established government method of procurement contracts to fund research and to purchase goods and equipment. Rees believed that this was the origin of university contractors.

stats as eng: what works vs what's true

- I thoroughly enjoyed reading McGrayne's piece, because I think this piece is the first reading this semester that talks about statistics as a means for decision making rather than a means for the search for truth.

stats as eng: what works vs what's true

- I thoroughly enjoyed reading McGrayne's piece, because I think this piece is the first reading this semester that talks about statistics as a means for decision making rather than a means for the search for truth.
- recall from last week: is data

stats as eng: what works vs what's true

- I thoroughly enjoyed reading McGrayne's piece, because I think this piece is the first reading this semester that talks about statistics as a means for decision making rather than a means for the search for truth.
- recall from last week: is data
  - science? (Fisher)

stats as eng: what works vs what's true

- I thoroughly enjoyed reading McGrayne's piece, because I think this piece is the first reading this semester that talks about statistics as a means for decision making rather than a means for the search for truth.
- recall from last week: is data
  - science? (Fisher)
  - math? (Neyman, E.S. Pearson)

stats as eng: what works vs what's true

- I thoroughly enjoyed reading McGrayne's piece, because I think this piece is the first reading this semester that talks about statistics as a means for decision making rather than a means for the search for truth.
- recall from last week: is data
  - science? (Fisher)
  - math? (Neyman, E.S. Pearson)
  - engineering? (today)

stats as eng: what works vs what's true

- I thoroughly enjoyed reading McGrayne's piece, because I think this piece is the first reading this semester that talks about statistics as a means for decision making rather than a means for the search for truth.
- recall from last week: is data
  - science? (Fisher)
  - math? (Neyman, E.S. Pearson)
  - engineering? (today)
  - (soon): technology?

arc this week:

1. Bletchley

arc this week:

1. Bletchley

- fuzzies->techies

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)
- labor

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)
- labor

2. .mil <->.com

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not "mathematical statistics"
    - (and math)
- labor

2. .mil <->.com

- limited in UK (GPO played the role)

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)
- labor

2. .mil <->.com

- limited in UK (GPO played the role)
- goes large in US

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)
- labor

2. .mil <->.com

- limited in UK (GPO played the role)
- goes large in US
- expands after WWII, unlike UK

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)
- labor

2. .mil <->.com

- limited in UK (GPO played the role)
- goes large in US
- expands after WWII, unlike UK

3. lasting impact

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not "mathematical statistics"
  - (and math)
- labor

2. .mil <->.com

- limited in UK (GPO played the role)
- goes large in US
- expands after WWII, unlike UK

3. lasting impact

- labor, gender, and ghost work

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)
- labor

2. .mil <->.com

- limited in UK (GPO played the role)
- goes large in US
- expands after WWII, unlike UK

3. lasting impact

- labor, gender, and ghost work

- largest focus: Bell Labs (research arm of AT&T)

arc this week:

1. Bletchley

- fuzzies->techies
- engineering, not “mathematical statistics”
  - (and math)
- labor

2. .mil <->.com

- limited in UK (GPO played the role)
- goes large in US
- expands after WWII, unlike UK

3. lasting impact

- labor, gender, and ghost work
- largest focus: Bell Labs (research arm of AT&T)
- birth of computation; rest of Part 2 (AI, BI, ML, DS)

1. Bletchley

66 Miles northeast of East Isley, where Studnet and Karl Pearson met in 1905, lay the quiet English town of Bletchley Park.

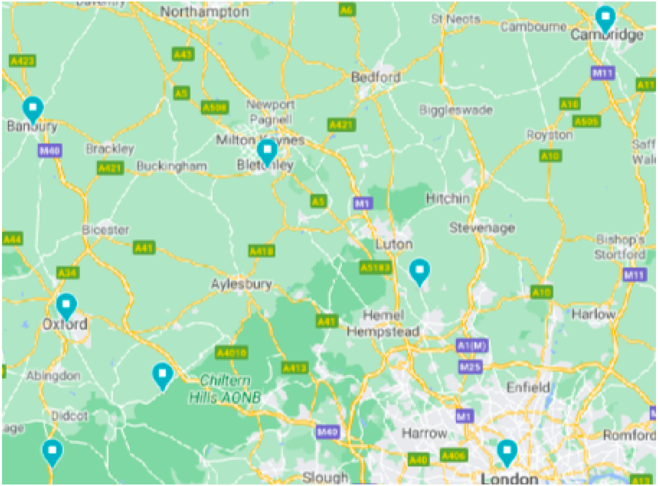


Figure 1: where it happened

1.1 British crypto: prior belief (from Copeland 2006)

> *GC & CS had begun the war with an extreme reluctance to hire anyone with a scientific or technical background at all. Recruiting was done through an old-boy network with a vengeance. . . . [WW1 cryptanalysts were] mainly linguists who were now Oxford and Cambridge dons in such fields as classics, history, and modern languages. . . . enduring British public-school prejudice against anything even remotely associated with 'trade'; properly educated boys studied Latin and Greek, not science or engineering.*

fortunately, Poland was different

"On 26 July 1939, in the Pyry Forest south of Warsaw, Polish cryptologists revealed to [.UK, .FR] they had been reading German signals traffic, transmitted by Enigma machines, since 1933" (–BBC) (recall: Enigma commercial since 1923)

we found that the Germans were well aware of the way the Enigma could be broken, but they had concluded that it would take a whole building full of equipment to do it. And that's what we had. A building full of equipment. Which they hadn't pictured as really feasible (–H. Campaigne, 28 Jun 1983 on TICOM trip '46)

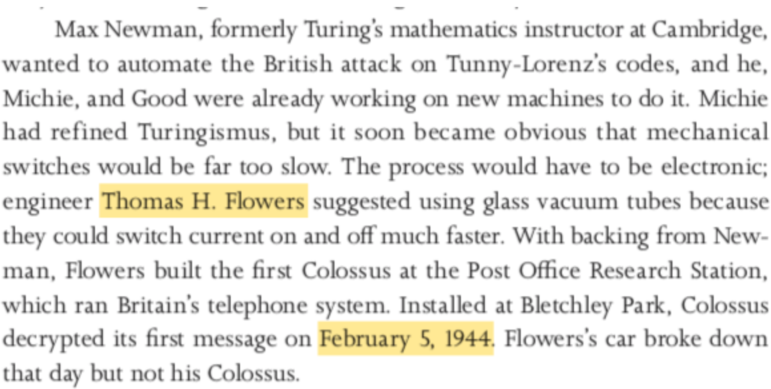
- (cf. "I told you it couldn't be done without turning the whole country into a factory" –Bohr)

fortunately, Poland was different

> *"On 26 July 1939, in the Pyry Forest south of Warsaw, Polish cryptologists revealed to [.UK, .FR] they had been reading German signals traffic, transmitted by Enigma machines, since 1933" (–BBC) (recall: Enigma commercial since 1923)*
> *we found that the Germans were well aware of the way the Enigma could be broken, but they had concluded that it would take a whole building full of equipment to do it. And that's what we had. A building full of equipment. Which they hadn't pictured as really feasible (–H. Campaigne, 28 Jun 1983 on TICOM trip '46)*

- (cf. "I told you it couldn't be done without turning the whole country into a factory" –Bohr)
- idea: a trading zone (including Bayes); contrast w/contemporary (and even post-war!) mathematical statistics a la Fisher/Neyman

Bletchley mathematicians and engineers

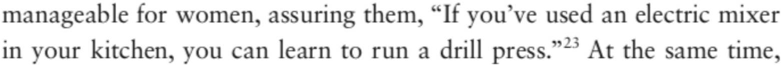


Max Newman, formerly Turing's mathematics instructor at Cambridge, wanted to automate the British attack on Tunny-Lorenz's codes, and he, Michie, and Good were already working on new machines to do it. Michie had refined Turingismus, but it soon became obvious that mechanical switches would be far too slow. The process would have to be electronic; engineer Thomas H. Flowers suggested using glass vacuum tubes because they could switch current on and off much faster. With backing from Newman, Flowers built the first Colossus at the Post Office Research Station, which ran Britain's telephone system. Installed at Bletchley Park, Colossus decrypted its first message on February 5, 1944. Flowers's car broke down that day but not his Colossus.

Figure 2: UK GPO or 'post' (telecommunications too, until 1969)

immediately: labor is segregated, gendered: prior belief

"The growing popularity of the typewriter in late Victorian offices had helped create an association of automation with feminized labor pools" -MH



manageable for women, assuring them, "If you've used an electric mixer in your kitchen, you can learn to run a drill press."[23] At the same time,

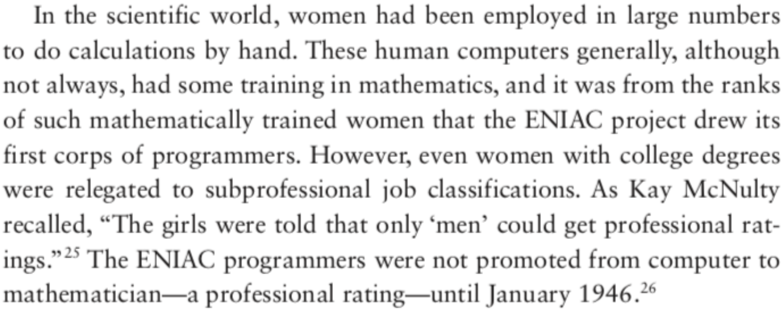
Figure 3: forced models of labor

immediately: labor is segregated, gendered

WRNS "punched each intercepted message by hand, letter by letter, into a Bandbury sheet" -SM
"the gendered nature of technical skill [and] of labor" (-Abbate)

2. labor priors become process, thereafter self-reinforcing

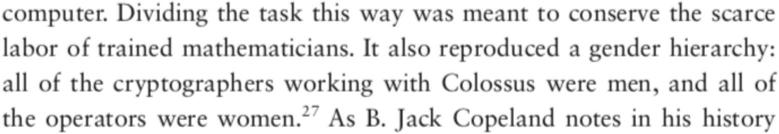
Abbate on "Women at the Dawn"



In the scientific world, women had been employed in large numbers to do calculations by hand. These human computers generally, although not always, had some training in mathematics, and it was from the ranks of such mathematically trained women that the ENIAC project drew its first corps of programmers. However, even women with college degrees were relegated to subprofessional job classifications. As Kay McNulty recalled, "The girls were told that only 'men' could get professional ratings."[25] The ENIAC programmers were not promoted from computer to mathematician—a professional rating—until January 1946.[26]

Figure 4: prior labor dynamics, and power dynamics

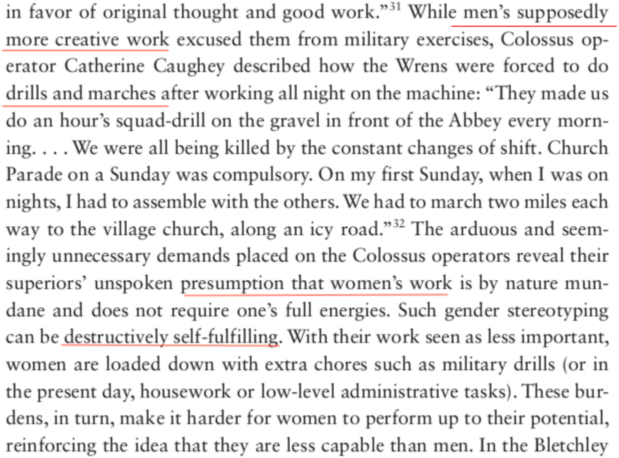
Abbate on "Women at the Dawn"



computer. Dividing the task this way was meant to conserve the scarce labor of trained mathematicians. It also reproduced a gender hierarchy: all of the cryptographers working with Colossus were men, and all of the operators were women.[27] As B. Jack Copeland notes in his history

Figure 5: org chart as weapon of oppression

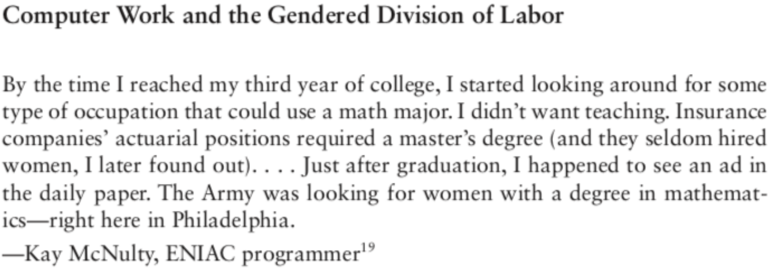
Abbate on "Women at the Dawn"



in favor of original thought and good work."[31] While men's supposedly more creative work excused them from military exercises, Colossus operator Catherine Caughey described how the Wrens were forced to do drills and marches after working all night on the machine: "They made us do an hour's squad-drill on the gravel in front of the Abbey every morning. . . . We were all being killed by the constant changes of shift. Church Parade on a Sunday was compulsory. On my first Sunday, when I was on nights, I had to assemble with the others. We had to march two miles each way to the village church, along an icy road."[32] The arduous and seemingly unnecessary demands placed on the Colossus operators reveal their superiors' unspoken presumption that women's work is by nature mundane and does not require one's full energies. Such gender stereotyping can be destructively self-fulfilling. With their work seen as less important, women are loaded down with extra chores such as military drills (or in the present day, housework or low-level administrative tasks). These burdens, in turn, make it harder for women to perform up to their potential, reinforcing the idea that they are less capable than men. In the Bletchley

Figure 6: 'destructively self-fulfilling'

Labor options for women in US 1944



Computer Work and the Gendered Division of Labor

By the time I reached my third year of college, I started looking around for some type of occupation that could use a math major. I didn't want teaching. Insurance companies' actuarial positions required a master's degree (and they seldom hired women, I later found out). . . . Just after graduation, I happened to see an ad in the daily paper. The Army was looking for women with a degree in mathematics—right here in Philadelphia.

—Kay McNulty, ENIAC programmer[19]

Figure 7: 'labor shortage'

2. Secret & Tacit knowledge: diffusion to US

- “Sinkov Mission”, Jan 1941; @ BP 1941-02-08

2. Secret & Tacit knowledge: diffusion to US

- "Sinkov Mission", Jan 1941; @ BP 1941-02-08
- Turing visit November 12, 1942 to March 1943

2. Secret & Tacit knowledge: diffusion to US

- “Sinkov Mission”, Jan 1941; @ BP 1941-02-08
- Turing visit November 12, 1942 to March 1943
- thereafter, plenty of interchange

primary readings: Turing by Hodges: US SIGINT

Alan's work on the RCA cipher seemed to show that his method would not work. He joined in the work of the 'cell' on another approach to the problem. Despite the great technical secrecy, there were enough straws in the wind for his colleagues to realise that he was doing other, top-level, work. Thus it was noted that while speaking with H. Nyquist, one of the top Bell consultants working on the X-system, Alan had met William Friedman, who was the chief American cryptanalyst.

Friedmans

Figure 8: William and Elizebeth Friedman

- couple met under patron wanting to reveal the true Shakespeare

Friedmans

Figure 8: William and Elizebeth Friedman

- couple met under patron wanting to reveal the true Shakespeare
- “Uncle Willy Friedman never would call me Moody. As long as he lived, even if we would go to a cocktail party he would introduce my husband… but he sort of founded women’s lib. “I knew her when she was a Morris. I’m never going to change that.” And he’d call Warren, my husband, Warren Morris. It was his little joke, but he never would call me Moody.”

Friedmans

- tiny US crypto community during WW1 and between wars

Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations

Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations
- William lead Army effort in WW2 against Japanese Codes

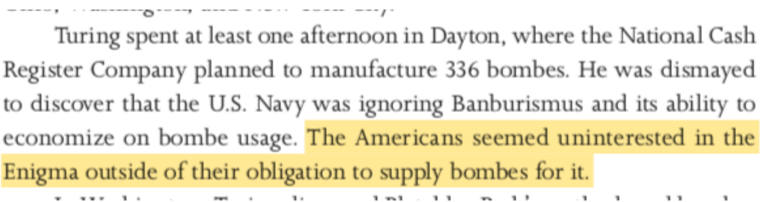
Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations
- William lead Army effort in WW2 against Japanese Codes
- help create unified NSA

Friedmans

- tiny US crypto community during WW1 and between wars
- William push mathematical crypto before WW2 with tiny organizations
- William lead Army effort in WW2 against Japanese Codes
- help create unified NSA
- push toward project of large supercomputers

primary readings: Turing by Hodges: NCR



Turing spent at least one afternoon in Dayton, where the National Cash Register Company planned to manufacture 336 bombes. He was dismayed to discover that the U.S. Navy was ignoring Banburismus and its ability to economize on bombe usage. The Americans seemed uninterested in the Enigma outside of their obligation to supply bombes for it.

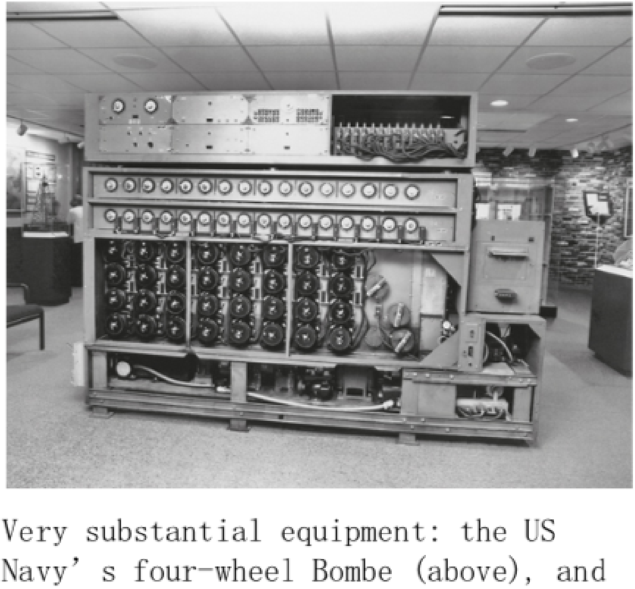
Figure 9: contractor mindset @ NCR

primary readings: Turing by Hodges: NYC

He went down to New York City, arriving at the Bell Laboratories building on West Street, by the piers, on the afternoon of 19 January 1943. And for two months he soaked himself in the electronic technology of speech encipherment.

Bell, NYC

Bell, hardware



Very substantial equipment: the US Navy' s four-wheel Bombe (above), and

Figure 11: Bell, hardware

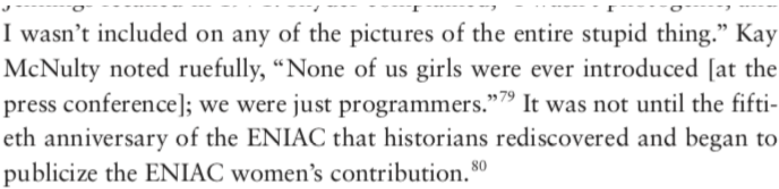
2. mil-industrial: (US & UK)

And the Army went to the telephone department to get a relay-style Bombe which eventually got called "Madame X". . . "a very large Enigma device. When I say it was large, it about the size of this house, and you know, a kind of a big mysterious thing. It worked relay speeds, relays clicking back and forth. The advantage of it was that they could simulate a large number of Enigma machines" H. Campaigne (USN, 1910-1988)

Flowers built the first Colossus at the Post Office Research Station, which ran Britain's telephone system

3.1 lasting impacts: labor

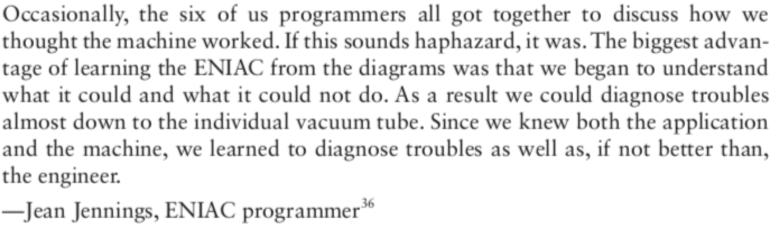
"girl hours" (IBM UK, Mar Hicks)



I wasn't included on any of the pictures of the entire stupid thing." Kay McNulty noted ruefully, "None of us girls were ever introduced [at the press conference]; we were just programmers."[79] It was not until the fiftieth anniversary of the ENIAC that historians rediscovered and began to publicize the ENIAC women's contribution.[80]

Figure 12: erasure

not just UK. . . . Abbate on “Women at the Dawn”

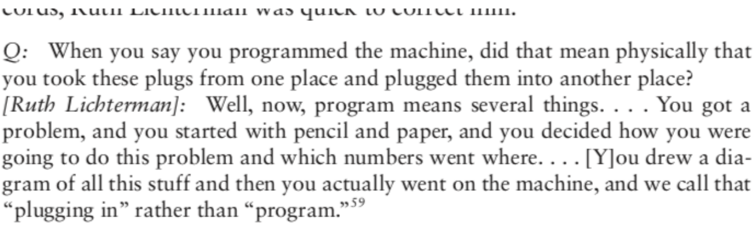


Occasionally, the six of us programmers all got together to discuss how we thought the machine worked. If this sounds haphazard, it was. The biggest advantage of learning the ENIAC from the diagrams was that we began to understand what it could and what it could not do. As a result we could diagnose troubles almost down to the individual vacuum tube. Since we knew both the application and the machine, we learned to diagnose troubles as well as, if not better than, the engineer.

—Jean Jennings, ENIAC programmer[36]

Figure 13: depth of understanding

and yet



cords, Ruth Lichterman was quick to correct him.

Q: When you say you programmed the machine, did that mean physically that you took these plugs from one place and plugged them into another place?
[Ruth Lichterman]: Well, now, program means several things. . . . You got a problem, and you started with pencil and paper, and you decided how you were going to do this problem and which numbers went where. . . . [Y]ou drew a diagram of all this stuff and then you actually went on the machine, and we call that "plugging in" rather than "program."[59]

Figure 14: programming and plugging

3.1 lasting impact: homophobia in US, too. . .

From Juanita Moody (1924-2015),

[Tom Wagner] got a citation after the war from the Secretary of War due to the people in G2 having known that he was the person who was leading this effort. . . [In 1944, He] turned out to be a gay and was asked to leave the agency. That was his reward. And I turned out to be the person that .was chosen to tell him that he must either volunteer to leave or. . . now, I had known ever since I met the man that he was gay. Fortunately in the beginning nobody had ever come around and told me that there was - anything wrong with it, or I should go running off and tattle. But he never hid the fact either, so I always felt that there was clearly a case that the basis for this decision, however sound it might have been, certainly didn't apply in his case, because he didn't hid the fact that. . . so anyway.

(Tangent: JN-25/JN-19 story also incredible, e.g., "But they told me that the invasion of Japan as planned was called off because of the information that we got out of this material.")

3.2 lasting impact: US vs UK secrecy and consequences (TW)

"my parents never knew what I did" (-Eleanor Ireland, Colossus)
My great sadness is that my beloved husband died in 1975 without knowing what I did in the war. (- Catherine Caughey, Colossus
These extreme security measures continued to influence the historiog- raphy of labor and technology for decades after the war, paradoxically ensuring that British accomplishments went down in history as also-rans in a US-centric story of early electronic computing. - Hicks

Postwar NSA norms

1963, Fort Meade area: if you're opening a bank account:

- where does your husband work?

Postwar NSA norms

1963, Fort Meade area: if you’re opening a bank account:

- where does your husband work?
- ‘my husband has a civilian job with the department of defense.’

Postwar NSA norms

1963, Fort Meade area: if you’re opening a bank account:

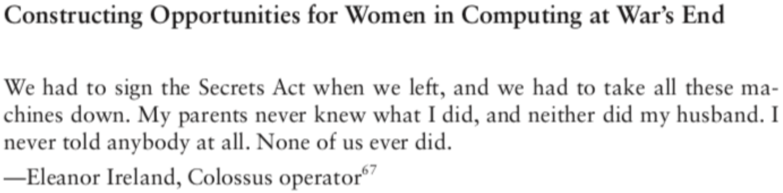
- where does your husband work?
- ‘my husband has a civilian job with the department of defense.’
- oh he’s at NSA”

Postwar NSA norms

1963, Fort Meade area: if you're opening a bank account:

- where does your husband work?
- ‘my husband has a civilian job with the department of defense.’
- oh he's at NSA”
- pers. comms

Abbate on “Women at the Dawn”



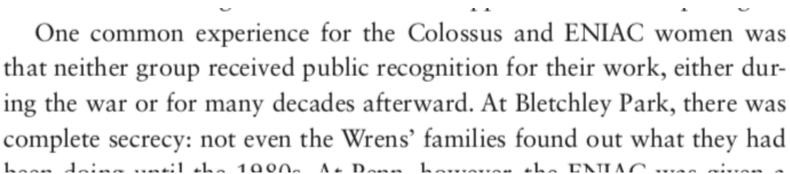
Constructing Opportunities for Women in Computing at War’s End

We had to sign the Secrets Act when we left, and we had to take all these machines down. My parents never knew what I did, and neither did my husband. I never told anybody at all. None of us ever did.

—Eleanor Ireland, Colossus operator[67]

Figure 15: secrecy

Abbate on “Women at the Dawn”

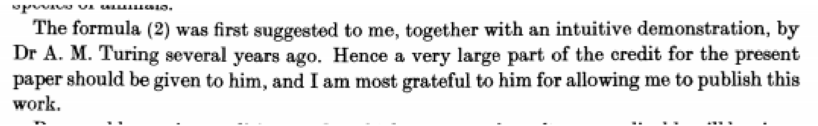


One common experience for the Colossus and ENIAC women was that neither group received public recognition for their work, either during the war or for many decades afterward. At Bletchley Park, there was complete secrecy: not even the Wrens’ families found out what they had been doing until the 1980s. At Penn, however, the ENIAC was given a

Figure 16: secrecy and un-history

ideas outside the fence

- contrast I. J. Good vs contractors; “inside the fence” and tacit knowledge obfuscated for open academic publications



species of animals.

The formula (2) was first suggested to me, together with an intuitive demonstration, by Dr A. M. Turing several years ago. Hence a very large part of the credit for the present paper should be given to him, and I am most grateful to him for allowing me to publish this work.

Figure 17: 1953

3.3 lasting impact: .mil<->.com (declassified 2016-11-21)

Both the [US] bombe and ENIAC had been developed through classified wartime military contracts. Thus computing in the United States began in the rarified atmosphere of tight security. Though the cryptanalytic aspects were not publicized, the Army relationship with the Moore School became a matter of public knowledge in 1946 when the inventors of ENIAC, John Mauchly and J. Presper Eckert, gave a series of lectures on electronic computers. As the two men left the Moore School to establish a computer manufacturing company, they dispersed their knowledge nationwide in what became known as the Moore School Lectures. Many felt that this lecture series launched the computer industry in the United States.

- American Cryptology during the Cold War, 1945-1989 Book I: The Struggle for Centralization, 1945-1960 Thomas R. Johnson (“top secret ultra”)

3.3 lasting impact: .mil funded startups (e.g., ERA)

As the war ended, Wenger felt that he was afraid that all this talent he had collected would be dissipated. And he came up with the idea of having them form an independent, private organization which would keep them together. And if the Navy would support them, the Navy would help them stay together and they'd be available there anytime an emergency arose.

IC “became computer specialists”

- OSS ('42-'45) ->NSA ('52), CIA ('47) established
  Certainly, when an engineer sees a technique which he thinks has possibilities, he looks for ways to apply it. I mean, that's what happened with the computer. We saw an opportunity to apply it to cryptography and we were off after computers. . . . We saw a chance and so we became computer specialists – Campaigne

eventually .com outstrips .gov

> *Conventional wisdom about NSA and computers has it, as a retired NSA senior officer once wrote me, "In the early days, NSA and its predecessor organizations drove the computer industry. In the 1960s, we kept pace with it. We started losing ground in the '70s, and in the '80s we struggled to keep up with the industry.*

from NSA "It wasn't all magic" Colin B Burke, 1994, dec. 2002, declassified 2013-05-29

Not just Bell, e.g., IBM, Philco, Lincoln Labs. . .

“Was there a great deal of cooperation between IBM and the military?”; “Yes there was.”; “In early days?”; “Yes there was. IBM, stemming from Mr. Watson I guess, was very cooperative and patriotic. They would do anything they could do, they would do it. And they would do it without pay if we didn’t want to pay them”

- e.g., Harvest 1962-1972 “more powerful than the best commercially available machine by a factor of 50 to 200”

Not just Bell, e.g., IBM, Philco, Lincoln Labs. . .

"Was there a great deal of cooperation between IBM and the military?"; "Yes there was."; "In early days?"; "Yes there was. IBM, stemming from Mr. Watson I guess, was very cooperative and patriotic. They would do anything they could do, they would do it. And they would do it without pay if we didn't want to pay them"

- e.g., Harvest 1962-1972 "more powerful than the best commercially available machine by a factor of 50 to 200"
- "NSA scientists were among the first to apply the new transistor technology to computers, and in the mid-1950s it developed an in-house computer called SOLO, the world's first computer to be entirely transistorized. SOLO was subsequently marketed commercially by the contractor, Philco, as the Transac S-1000."

. . . but Bell impacted greatly

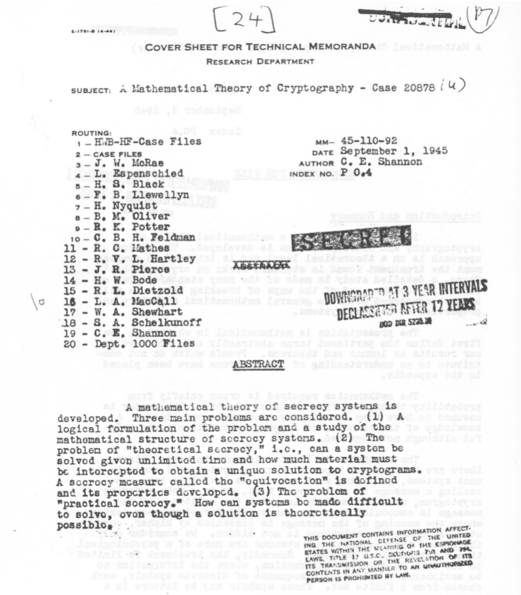
"By the middle of 1940, the research department at Bell Labs stopped doing research as nearly all of the Labs' work—about 75 percent of it—was redirected toward developing electronic devices for wartime" – Gertner *the Idea Factory*

> *We [NSA] had very close contacts with the Bell Laboratories. They were very, let's say, willing to work along with us. - Solomon Kullback (1907-1994), who spent 1942 at Bletchley*

Bell's Tukey and IC work

> *[Tukey] was indeed active in the analysis of the Enigma system and then of course was part of our force in the fifties which did the really historic work on the Soviet codes as well. So he was very effective in that whole operation.*

Bell's Shannon: mathematical theory of crypto/communications



[24]

~~CONFIDENTIAL~~ (P7)

E-1751-B (4-44)

COVER SHEET FOR TECHNICAL MEMORANDA

RESEARCH DEPARTMENT

SUBJECT: A Mathematical Theory of Cryptography - Case 20878 (u)

ROUTING:
1 – HWB-HF-Case Files
2 – CASE FILES
3 – J. W. McRae
4 – L. Espenschied
5 – H. S. Black
6 – F. B. Llewellyn
7 – H. Nyquist
8 – B. M. Oliver
9 – R. K. Potter
10 – C. B. H. Feldman
11 - R. C. Mathes
12 - R. V. L. Hartley
13 - J. R. Pierce
14 - H. W. Bode
15 - R. L. Dietzold
16 - L. A. MacCall
17 - W. A. Shewhart
18 - S. A. Schelkunoff
19 - C. E. Shannon
20 - Dept. 1000 Files

MM– 45-110-92
DATE September 1, 1945
AUTHOR C. E. Shannon
INDEX NO. P 0.4

SECRET

~~ABSTRACT~~

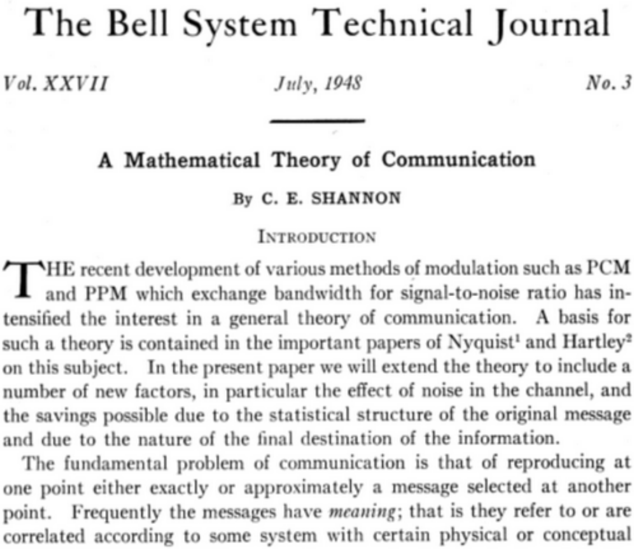
DOWNGRADED AT 3 YEAR INTERVALS
DECLASSIFIED AFTER 12 YEARS
DOD DIR 5200.10

ABSTRACT

A mathematical theory of secrecy systems is developed. Three main problems are considered. (1) A logical formulation of the problem and a study of the mathematical structure of secrecy systems. (2) The problem of "theoretical secrecy," i.e., can a system be solved given unlimited time and how much material must be intercepted to obtain a unique solution to cryptograms. A secrecy measure called the "equivocation" is defined and its properties developed. (3) The problem of "practical secrecy." How can systems be made difficult to solve, even though a solution is theoretically possible.

THIS DOCUMENT CONTAINS INFORMATION AFFECTING THE NATIONAL DEFENSE OF THE UNITED STATES WITHIN THE MEANING OF THE ESPIONAGE LAWS, TITLE 18 U.S.C. SECTIONS 793 AND 794. ITS TRANSMISSION OR THE REVELATION OF ITS CONTENTS IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY LAW.

Shannon: conversion to civilian



The Bell System Technical Journal

Vol. XXVII *July, 1948* *No. 3*

A Mathematical Theory of Communication

By C. E. SHANNON

Introduction

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual

Shannon: mathematical theory of communications

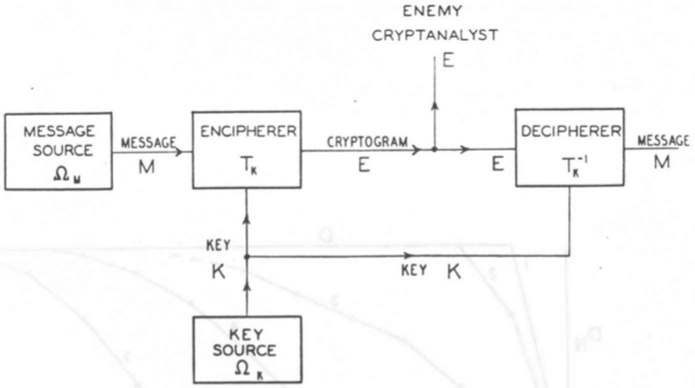


FIG. 6

Figure 20: Shannon crypto diagram

Shannon: from interception to communications

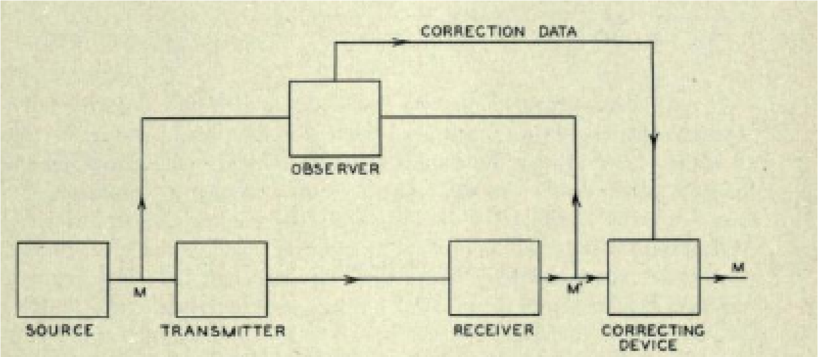


Fig. 8—Schematic diagram of a correction system.

Figure 21: Shannon communications diagram

Bell, Shannon, and Intelligence

some saw that computers would soon be a type of “thinking”:

- michie and shannon (met w/Turing on US visit) will be next week

Bell, Shannon, and Intelligence

some saw that computers would soon be a type of “thinking”:

- michie and shannon (met w/Turing on US visit) will be next week
- shannon 9/1/45 math theory of crypto but also automata and brains

appendix

- 2021-01-12: intro to course (Part 1)

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)
- 2021-03-09: birth and death of AI (light...)

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)
- 2021-03-09: birth and death of AI (light. . .)
- 2021-03-16: big data, old school (1958-1980) (. . . heat, 1/3)

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)
- 2021-03-09: birth and death of AI (light. . .)
- 2021-03-16: big data, old school (1958-1980) (. . . heat, 1/3)
- 2021-03-23: ML=AI2.0 (. . . heat, 2/3)

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)
- 2021-03-09: birth and death of AI (light…)
- 2021-03-16: big data, old school (1958-1980) (…heat, 1/3)
- 2021-03-23: ML=AI2.0 (…heat, 2/3)
- 2021-03-30: data science, 1962-2017 (…heat, 2/3)

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)
- 2021-03-09: birth and death of AI (light…)
- 2021-03-16: big data, old school (1958-1980) (…heat, 1/3)
- 2021-03-23: ML=AI2.0 (…heat, 2/3)
- 2021-03-30: data science, 1962-2017 (…heat, 2/3)
- 2021-04-06: ethics (Part 3)

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)
- 2021-03-09: birth and death of AI (light...)
- 2021-03-16: big data, old school (1958-1980) (...heat, 1/3)
- 2021-03-23: ML=AI2.0 (...heat, 2/3)
- 2021-03-30: data science, 1962-2017 (...heat, 2/3)
- 2021-04-06: ethics (Part 3)
- 2021-04-13: present problems: attention economy+VC=dumpsterfire

appendix

- 2021-01-12: intro to course (Part 1)
- 2021-01-19: setting the stakes
- 2021-01-26: risk and social physics
- 2021-02-02: statecraft and quantitative racism
- 2021-02-09: intelligence, causality, and policy
- 2021-02-16: data gets real: mathematical baptism
- 2021-02-23: WWII, dawn of digital computation (Part 2)
- 2021-03-09: birth and death of AI (light...)
- 2021-03-16: big data, old school (1958-1980) (...heat, 1/3)
- 2021-03-23: ML=AI2.0 (...heat, 2/3)
- 2021-03-30: data science, 1962-2017 (...heat, 2/3)
- 2021-04-06: ethics (Part 3)
- 2021-04-13: present problems: attention economy+VC=dumpsterfire
- 2021-04-15: future solutions

references

[1] https://history.blog.gov.uk/2019/07/26/whats-the-context-polish-cryptologists-reveal-they-have-cracked-the-enigma-code-26-july-1939/ ; see also Erskine, R. (2006). The poles reveal their secrets: Alastair denniston's account of the july 1939 meeting at pyry. Cryptologia, 30(4), 294-305. Retrieved from http://ezproxy.cul.columbia.edu/login?url=https://www-proquest-com.ezproxy.cul.columbia.edu/scholarly-journals/poles-reveal-their-secrets-alastair-dennistons/docview/213045718/se-2?accountid=10226