Pioneering Women in Cryptology

UNIVERSITY OF CALGARY

Lauren DeDieu

March 2018

Impact on Women Mathematicians on Research and Education in Mathematics

The Last of the Paper and Pencil Heroes

Agnes Meyer Driscoll (1889 – 1971)

Elizebeth Smith Friedman (1892 - 1980)

The Last of the Paper and Pencil Heroes

- School Teachers
- Learned cryptology during WWI
- Headed their cryptology division in U.S. Government for 20+ years
- Trained men who would go on to become leaders in cryptology
- Forgotten by history (…*until recently*)

The Last of the Paper and Pencil Heroes

Agnes Meyer Driscoll

- **Career Highlights:**
  - Developed new cipher machines
  - Broke several important Japanese Naval systems between the wars (US Navy)

The Last of the Paper and Pencil Heroes

Elizebeth Smith Friedman

- **Career Highlights:**
  - Co-created books that became “foundational stones of the modern science of cryptology”
  - Helped catch gangsters and smugglers during Prohibition years (U.S. Coast Guard)
  - Exposed a Nazi Spy Ring in South America

Elizebeth Smith Friedman

Elizebeth Smith Friedman

- Born in Huntington, Indiana (1892)
- Graduated from Hillsdale College in Michigan (1915)
  - Majored in English literature
- Substitute High School Principal (1915)

- Newberry Library, Chicago – the First Folio

Riverbank Laboratories

- Think-tank outside of Chicago, IL
- Mrs. Gallup and Fabyan believed *Sir Francis Bacon* was the true author of Shakespeare's works

Elizebeth & George Fabyan, 1916

Riverbank Laboratories

- Think-tank outside of Chicago, IL
- Mrs. Gallup and Fabyan believed *Sir Francis Bacon* was the true author of Shakespeare's works

---

- Bilateral cipher (Bacon, 1605):

'K*nowledg*e i*s* po*we*r'

decrypts to

'RUN'

(a=*italic*, b=normal)

Letter	Code	Letter	Code
A	aaaaa	N	abbaa
B	aaaab	O	abbab
C	aaaba	P	abbba
D	aaabb	Q	abbbb
E	aabaa	R	baaaa
F	aabab	S	baaab
G	aabba	T	baaba
H	aabbb	U, V	baabb
I, J	abaaa	W	babaa
K	abaab	X	babab
L	ababa	Y	babba
M	ababb	Z	babbb

World War I

- William Friedman
  - Studied genetics at Riverbank.

Elizebeth & William, 1920

World War I

- William Friedman
  - Studied genetics at Riverbank.
- During the first 8 months of the war, Elizebeth, William, and their team at Riverbank team did ALL of the code breaking for every part of the U.S. government (1917)
- Published 8 pamphlets that described new kinds of codebreaking strategies (1917-1920)

Elizebeth & William, 1920

World War I

"The modern day universe of codes and ciphers began in a cottage on the prairie, with a pair of young lovers smiling at each other across a table and a rich man urging them to be spectacular."

Elizebeth & William, 1920

World War I

"The modern day universe of codes and ciphers began in a cottage on the prairie, with a pair of young lovers smiling at each other across a table and a rich man urging them to be spectacular."

- Transposition cipher
  - Permute letters of plaintext (SIHT DAER UOY NAC)
- Substitution cipher
  - Swap letter according to a fixed rule (CAT --> DBU)

Elizebeth & William, 1920

World War I

- Scotland Yard: 38425, 97-2-14, 73-5-3

Elizebeth & William, 1920

World War I

- Scotland Yard: 38425, 97-2-14, 73-5-3
  - **Code 1:** *Key Word:* LAMP
    Encrypt: “C”:
    C is 13 and L is 25 (grid)
    C encrypts to: 13+25 = 38

	1	2	3	4	5	6	7
1	A	B	C	D	E	F	G
2	H	I	J	K	L	M	N
3	O	P	Q	R	S	T	U
4	V	W	X	Y	Z		

Elizebeth & William, 1920

World War I

- Scotland Yard: 38425, 97-2-14, 73-5-3
  - **Code 1:** *Key Word:* LAMP
    Encrypt: "C":
    C is 13 and L is 25 (grid)
    C encrypts to: 13+25 = 38

	1	2	3	4	5	6	7
1	A	B	C	D	E	F	G
2	H	I	J	K	L	M	N
3	O	P	Q	R	S	T	U
4	V	W	X	Y	Z		

  - **Code 2:** pg. 97, column 2, 14th word in column
  - **Code 3:** pg 73, 5th line, 3rd letter

Elizebeth & William, 1920

World War I

- Elizebeth described solving these messages as

"The thrill of your life. The skeletons of words leap out, and make you jump."

Elizebeth & William, 1918

World War I

- Elizebeth described solving these messages as

"The thrill of your life. The skeletons of words leap out, and make you jump."

"At the time they didn't know what was supposed to be hard and no one was around to tell them."

Elizebeth & William, 1918

After the War…

- Elizebeth worked for Army Signal Corps (1920)
  - In today's money, her pay was ~$28,000 and his ~$58,000
- In 1920, only ~50 government employees working in cryptology
  - Army, Navy, Black Chamber

After the War…

- Quit army to have children/ write books (1922)

After the War…

- Quit army to have children/ write books (1922)

"When they couldn't get him, I'd be offered a job."

- Worked for Navy for 5 months (1922)
  - Designed codes for sailors (… replaced Driscoll)

Prohibition Era

- U.S. Coast Guard (1925)
  - Rum-runners
  - Solved 2 years worth of backlogged messages in first 3 months
  - 25,000 messages per year

"Even though I have never seen your code book, I may read your thoughts."

Prohibition Era

From Halifax, Nova Scotia:

AWJTSSK JQS GBQKWSK LYMSE EJBCG SPEC QPFYEYQD MYHGC PRPYC JWKSWE CWI PQTGJW EPFS VBSM AWAJASTCE HJJS

To decode: A -> P, B -> U, C -> T, D -> K, E -> S, F -> V, etc.

PROCEED ONE HUNDRED MILES SOUTH EAST NAVISINK LIGHT AWAIT ORDERS TRY ANCHOR SAVE FUEL PROSPECTS GOOD

Mrs. Elizabeth Friedman, who is chief of the Cryptanalytic Section of e Coast Guard Intelligence Division, is a veritable nemesis for smugglers.

Trials

- New Orleans Trial (1933)
  - Testimony helped put away 5 ringleaders of rum-running organization
  - Gave jurors a “Class in Cryptology”

Trials

- New Orleans Trial (1933)
  - Testimony helped put away 5 ringleaders of rum-running organization
  - Gave jurors a “Class in Cryptology”

- Vancouver Trial (1938)
  - Helped expose smuggling ring that traded Canadian weapons to Hong Kong in exchange for drugs

F10 6 CABLE F HONGKONG 26 715 PM CDE WATSING VANCOUVER

IMUMO IISOP ESAPU UAKON

I M U M	O I I S	O P E S	A P U U	A K O N
2 9 4 9	0 2 3 4	0 6 9 4	6 6 4 3	6 0 1 0
款	借	否	速	覆
FUND	LOAN	OR NOT	QUICK	REPLY

Mrs. Elizabeth Friedman, who is chief of the Cryptanalytic Section of e Coast Guard Intelligence Division, is a veritable nemesis for smugglers.

Agnes Meyer Driscoll

Agnes Meyer Driscoll

- Born in Geneseo, Illinois (1889)
- Graduated from Ohio State University (1911)
  - Majored in math, music, physics, & foreign languages

- Music director at a military school (Texas, 3 yrs)
- Head of high school math department (Texas, 3yrs)

Agnes Meyer, age 21

Agnes Meyer Driscoll

- Enlisted in US Naval Reserve during WWI (1918, age 29)
  - Began studying Cryptology
  - Highest rank possible for a woman at the time (chief yeoman)
  - Code and Signal section
- Hired by Navy as a civilian (1920)

Agnes Meyer, age 21

Agnes Meyer Driscoll

- Began the U.S. Navy's first real efforts in cryptography
  - Received training from Riverbank Laboratories (1920)
  - Co-created the "*Cipher Machine*" (issued to each major ship and station for 15 yrs)

Agnes Meyer Driscoll

- Began the U.S. Navy's first real efforts in cryptography
  - Received training from Riverbank Laboratories (1920)
  - Co-created the "*Cipher Machine*" (issued to each major ship and station for 15 yrs)
- Left Navy to launch cipher machine factory (1923)
  - Catalyst for the Navy to realize how badly it needed cryptologic expertise

Madame X – Japanese Naval Systems

- **Red Book**
  - Driscoll figured out the key (1926)
  - Messages revealed details about naval maneuvers, fuel supplies, advances in aviation, etc.
  - Discovered Japan knew about their Japanese war plan, “Orange” (…which convinced government to invest more in radio intelligence)

Madame X – Japanese Naval Systems

- **Blue Book**
  - "This isn't the same code. This is a new code." - 1930
  - Cracked it three years later.
  - Revealed that Japan had battleships that could reach 26 knots (*so U.S. made a ship that could travel 28 knots*)
  - "The Navy cryptanalysts, spear-headed by Mrs. Driscoll, accomplished the impossible." – *Laurance Safford*

NSA Director Lt. Gen. John Samford, Hellen Talley, and Driscoll (right), 1958

Agnes Driscoll

- Driscoll's team grew from 6 officers (1931) to 40 (1937)
- Worked for AFSA and NSA
- 1959: Retired at age 70 (maximum retirement age)
- Madame X, the "first lady of naval cryptology", died in 1971

Elizebeth Smith Friedman

(*continued*)

The Invisible War (1939-45)

- South American, WWII
  - U.S. worried that if Nazi ships set up base there, then U.S. coastal cities would be vulnerable
  - Millions of Germans already lived in South America
- Counterespionage
  - Elizebeth was counterspying on foreign spies

Elizebeth (U.S. Coast Guard Cryptanalyst-in-Charge) & junior cryptanalyst Robert Gordon (1940)

The Invisible War (1939-45)

- Training
  - Elizebeth trained the FBI's first codebreaking team
  - Put together a cryptology team for the Office of the Coordinator of Information (predecessor of the CIA)

Elizebeth (U.S. Coast Guard Cryptanalyst-in-Charge) & junior cryptanalyst Robert Gordon (1940)

The Invisible War (1939-45)

From Mexico to Germany, 1940:

UHHNR LNDAL NURND WCNCK NRHLN DNRAN CHNDR UNDEN

The Invisible War (1939-45)

From Mexico to Germany, 1940:

UHHNR LNDAL NURND WCNCK NRHLN DNRAN CHNDR UNDEN

Only 11 letters: N, R, H, A, D, K, U, C, W, E, L

The Invisible War (1939-45)

From Mexico to Germany, 1940:

UHHNR LNDAL NURND WCNCK NRHLN DNRAN CHNDR UNDEN

Only 11 letters: N, R, H, A, D, K, U, C, W, E, L

- N most frequent… so space bar. Others digits 0-9.

The Invisible War (1939-45)

From Mexico to Germany, 1940:

UHHNR LNDAL NURND WCNCK NRHLN DNRAN CHNDR UNDEN

Only 11 letters: N, R, H, A, D, K, U, C, W, E, L

- N most frequent… so space bar. Others digits 0-9.
- Took 11 letters and rearranged them: DURCHWALKEN
  ("to give a good beating")

The Invisible War (1939-45)

From Mexico to Germany, 1940:

UHHNR LNDAL NURND WCNCK NRHLN DNRAN CHNDR UNDEN

Only 11 letters: N, R, H, A, D, K, U, C, W, E, L

- N most frequent… so space bar. Others digits 0-9.
- Took 11 letters and rearranged them: DURCHWALKEN
  ("to give a good beating")

255-38 178-23 164-49 358-1 37-45 132-10

The Invisible War (1939-45)

From Mexico to Germany, 1940:

UHHNR LNDAL NURND WCNCK NRHLN DNRAN CHNDR UNDEN

Only 11 letters: N, R, H, A, D, K, U, C, W, E, L

- N most frequent… so space bar. Others digits 0-9.
- Took 11 letters and rearranged them: DURCHWALKEN
  ("to give a good beating")

255-38 178-23 164-49 358-1 37-45 132-10

- Looks like a book cipher… (e.g. 255-38 -> E)
- Some number combinations appeared more often… played with frequent combinations until saw names of two German cities: Berlin, Bremen.

The Invisible War (1939-45)

- **Enigma**
  - Polyalphabetic cipher
  - At least 15 billion billion keys
  - Each key uses 16,900 alphabets before repeating

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

The Invisible War (1939-45)

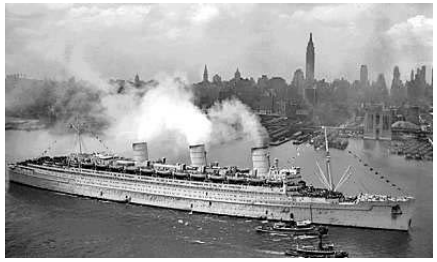
- **Enigma**
  - The strength of a cryptographic system usually has less to do with its design than with the way people tend to use it…

1	2	3	4	5	6	7
D	X	J	X	L	H	N
L	W	S	X	I	Y	F
M	H	O	S	S	L	C

  - Elizebeth and her team figured out the wiring of the rotors, and hence were able to recreate the machine (in both 1940 & 1942)

The Invisible War (1939-45)

- **RMS Queen Mary**
  - Elizebeth solved a sinister series of intercepts
  - Suggested Nazis were preparing to destroy the RMS Queen Mary (8398 American servicemen)
  - Captain was able to take evasive maneuvers to sneak past a U-boat



The Invisible War (1939-45)

- **Legacy**
  - Elizebeth deciphered codes for FBI
  - She made special devices and tools for FBI agents
  - The Coast Guard shared all of Elizebeth's decrypted codes with the FBI (dozens per week)

The Invisible War (1939-45)

- **Legacy**
  - Elizebeth deciphered codes for FBI
  - She made special devices and tools for FBI agents
  - The Coast Guard shared all of Elizebeth's decrypted codes with the FBI (dozens per week)
  - The FBI took credit
  - Original files weren't declassified until 2000… revealing the truth.

After WWII

- Elizebeth retired after the war (1946)
  - Final salary: $67,000 (in today's dollars)
  - Wrote a book with William to put the Bacon-Shakespeare conspiracy to rest

After WWII

"There came a day when Elizebeth just thinks: no. There is nothing wrong with me. What's wrong is with other people. This is the moment that hurls her into the rest of her life. The savaging of Nazis, the birth of a science: It begins on the day when a twenty-three-year-old American woman decides to trust her doubt and dig with her own mind."

- William died in 1969
- Elizebeth died in 1980

Thank You

References

- Fagone, J. (2017). *The Woman Who Smashed Codes*. New York, NY: HarperCollins Publishers.

- Johnson, K. W. (2015). *The Neglected Giant: Agnes Meyer Driscoll*. National Security Agency, Center for Cryptologic History.

- To hear audio interviews with Elizebeth:

George C. Marshall Foundation Library:

https://marshallfoundation.org/library/collection/elizebeth-smith-friedman-collection/elizebeth-smith-friedman-interviews