The Unknown Story of the First American Female Codebreaker
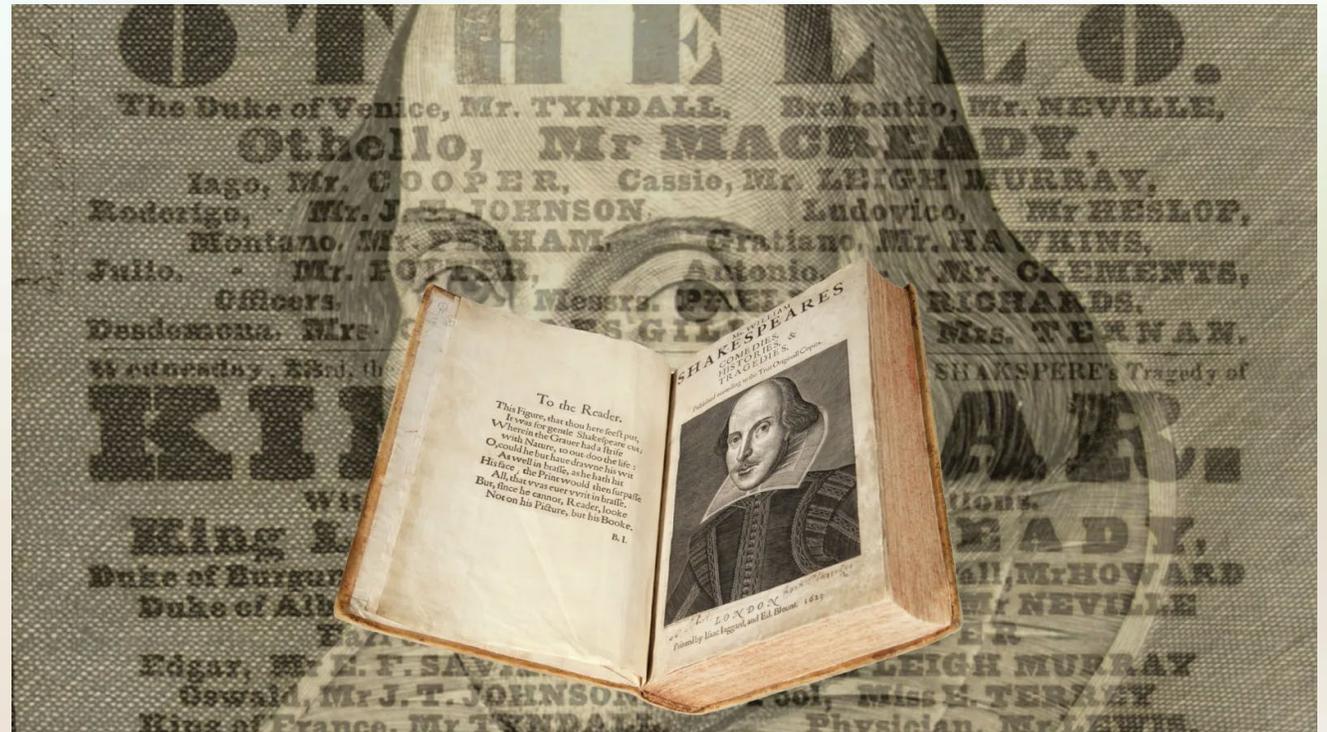
Elizebeth Smith Friedman

- Went to Wooster College – 2 years (1911-1913)
- Graduated from Hillsdale in 1915
- Fall of 1915 – Substitute Principal at Public HS in Wabash Indiana

© George C. Marshall Foundation

Newberry Library - Chicago

George Fabyan

Riverbank 1916

- Worked on Baconian Project
- Assistant to Elizebeth Wells Gallup

Riverbank Investigators - 1916

Riverbank Laboratories

- Working on the Baconian cipher of Shakespeare's works

- Met William Friedman who joined Riverbank as head of genetics department in 1915

© George C. Marshall Foundation

Riverbank 1917

Elizabeth and William Friedman - 1917

Riverbank

Riverbank Laboratories had a host of scientific and research facilities

Baconian Ciphers (1)

Letter	Code	Binary	Letter	Code	Binary
A	aaaaa	00000	N	abbaa	01100
B	aaaab	00001	O	abbab	01101
C	aaaba	00010	P	abbba	01110
D	aaabb	00011	Q	abbbb	01111
E	aabaa	00100	R	baaaa	10000
F	aabab	00101	S	baaab	10001
G	aabba	00110	T	baaba	10010
H	aabbb	00111	U, V	baabb	10011
I, J	abaaa	01000	W	babaa	10100
K	abaab	01001	X	babab	10101
L	ababa	01010	Y	babba	10110
M	ababb	01011	Z	babbb	10111

Baconian ciphers are categorized as both a substitution cipher (in plain code) and a concealment cipher (using the two typefaces).

To encode a message, each letter in the message is replaced by it's assigned group of five of the letters 'a' or 'b'. This replacement is a 5-bit binary encoding and is done according to the alphabet of the Baconian cipher (from the Latin Alphabet)

For example: **DOG** would be encoded to:
aaabbabbabaabba

Baconian Ciphers (2)

- Prepare a false message with the same number of letters as all of the 'a's and 'b's in the real secret message.

  - If the number of 'a's and 'b's was 50 – the false message had to have 50 letters in it.

- Two typefaces are chosen, one to represent '*a's* and the other '*b's*.

- Then each letter of the false message must be presented in the appropriate typeface, according to whether it stands for an '*a'* or a '*b'*.

Baconian Ciphers (3)

- Message :

ENJOYING THE LECTURE TODAY ABOUT ELIZEBETH
FRIEDMAN HER LIFE STORY AND HER CODEBREAKING
ACCOMPLISHMENTS

- To decode the message, each "typeface 1" letter in the false message is replaced with an *A* and each "typeface 2" letter is replaced with a *B*. The Baconian alphabet is then used to recover the original message.

Baconian Ciphers (4)

- TYPEFACE 1 (A) = Georgia Pro Cond Semibold, TYPEFACE 2 (B) = Berlin Sans FB

ENJOYING THE LECTURE TODAY ABOUT ELIZEBETH FRIEDMAN HER LIFE STORY AND HER CODEBREAKING ACCOMPLISHMENTS

Baaabaab bba abaabaa baabb ababb ababaabaa abbabbab bab aaab baaaa aba abb ababbaaaabaa bababaaabaabbab

Baconian Ciphers (5)

- The letters are then paired in groups of '5' and the Baconian alphabet is then used to recover the original message (5 characters per letter)

_____

baaab aabbb aabaa baaba abbab abbab abaab aaabb abbab babaa

abbaa aaaba abbab abbaa aabaa babab aaaba abbab

Baaab = S , aabbb = H

- This is now deciphered to:

SHE TOOK DOWN CONEXCO

Zimmerm

"We intend to begin on the first [...]
submarine warfare. We shall end [...]
United States of America neutral [...]
succeeding, we make Mexico a p[...]
following basis: make war togeth[...]
generous financial support and a[...]
that Mexico is to reconquer the l[...]
Mexico, and Arizona. The settlem[...]
will inform the President of the a[...]
the outbreak of war with the Uni[...]
and add the suggestion that he s[...]
invite Japan to immediate adhere[...]
mediate between Japan and ours[...]
attention to the fact that the rutl[...]
submarines now offers the prosp[...]
few months to make peace."

Signed, ZIMMERMANN.
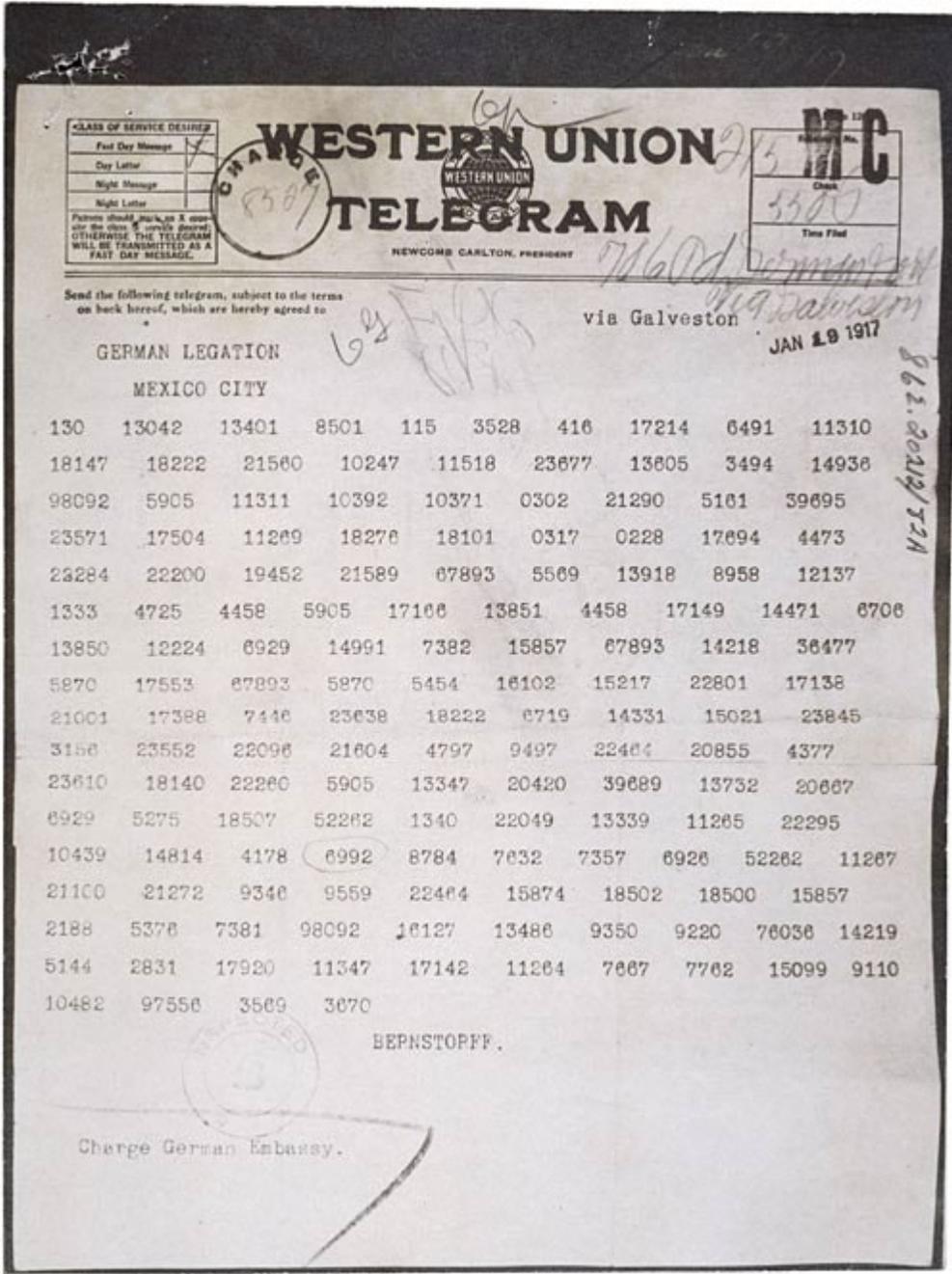
WWI - Codebreaking

- Fabyan established a new Riverbank Department of Ciphers
- Friedmans were in charge and Fabyan offered their services to the government.
- The code was a polyalphabetic substitution cipher. Used the Vigenère table.
  - Number of alphabets used was dependent on the key word
- During the war, the Friedmans developed many of the principles of modern cryptology.

Vigenère Cipher

	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

WWI – Cypher Training Class
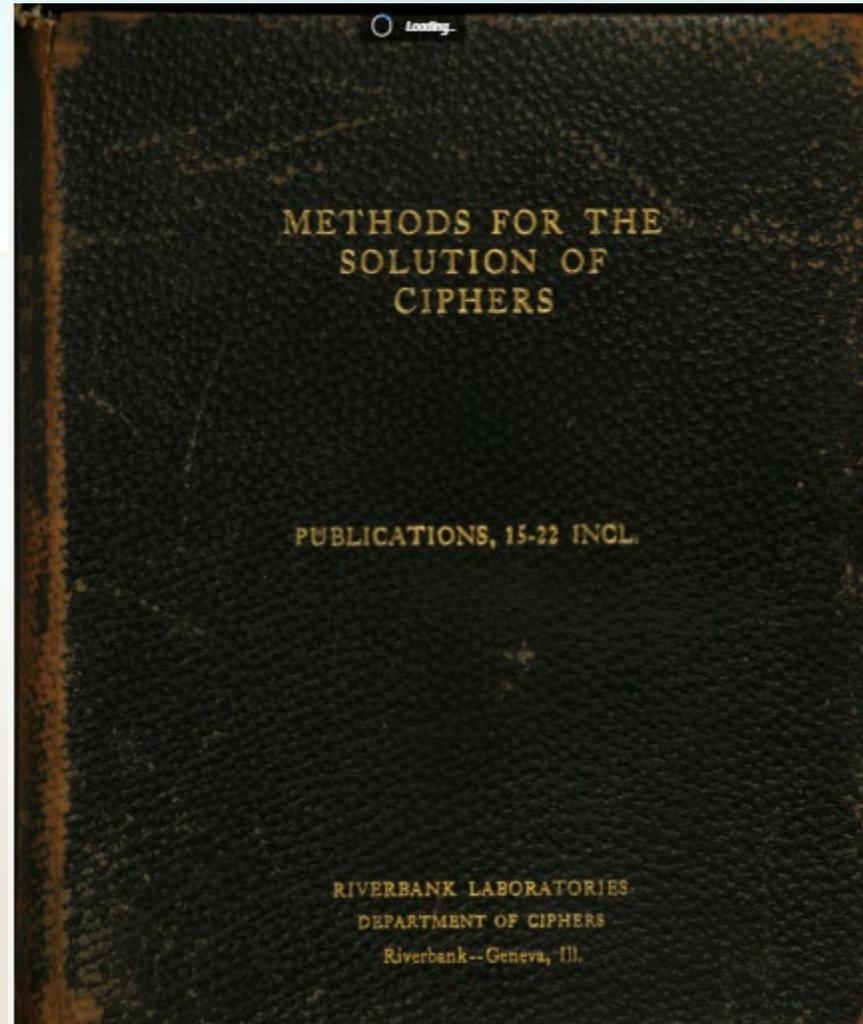
William Friedman - WWI

- In 1918 – William Friedman went into service

- William was commissioned to first lieutenant military intelligence

- At the end of the war, Friedman was asked to stay behind and write the history of the section.

  - He didn't return to the United States until April of 1919

After the War

- Elizebeth and William Friedman wanted to leave Riverbank
- Fabyan controlled a lot of their lives, promised more money (they never got) and they went back
- The last time, they didn't tell Fabyan until everything was packed and gone, and they were ready to leave

Life After Riverbank

- In 1921, the Friedmans left Riverbank to work for the War Department (Signal Corps) in Washington, D.C.
  - This was the last time the Friedmans would work together
- In late 1922 – Elizebeth took a Navy potion as a Cryptographer (pay was $1900/year)
  - She left this job after 5 months (she was pregnant)
- She had a daughter in 1924 and a son in 1926

28

August 1924

© George C. Marshall Foundation

Volstead Act

- Enacted in 1919 to enforce the [18th Amendment](#), which prohibited the manufacture, sale, and transportation of alcoholic beverages containing more than 0.5 percent alcohol.

- Act led to widespread violations, including bootlegging, the rise of organized crime, and increased corruption.

- The 18th Amendment, and consequently the Volstead Act, was repealed by the 21st Amendment in 1933.

Capt. Charles Root

- U.S. Coast Guard Intelligence Officer
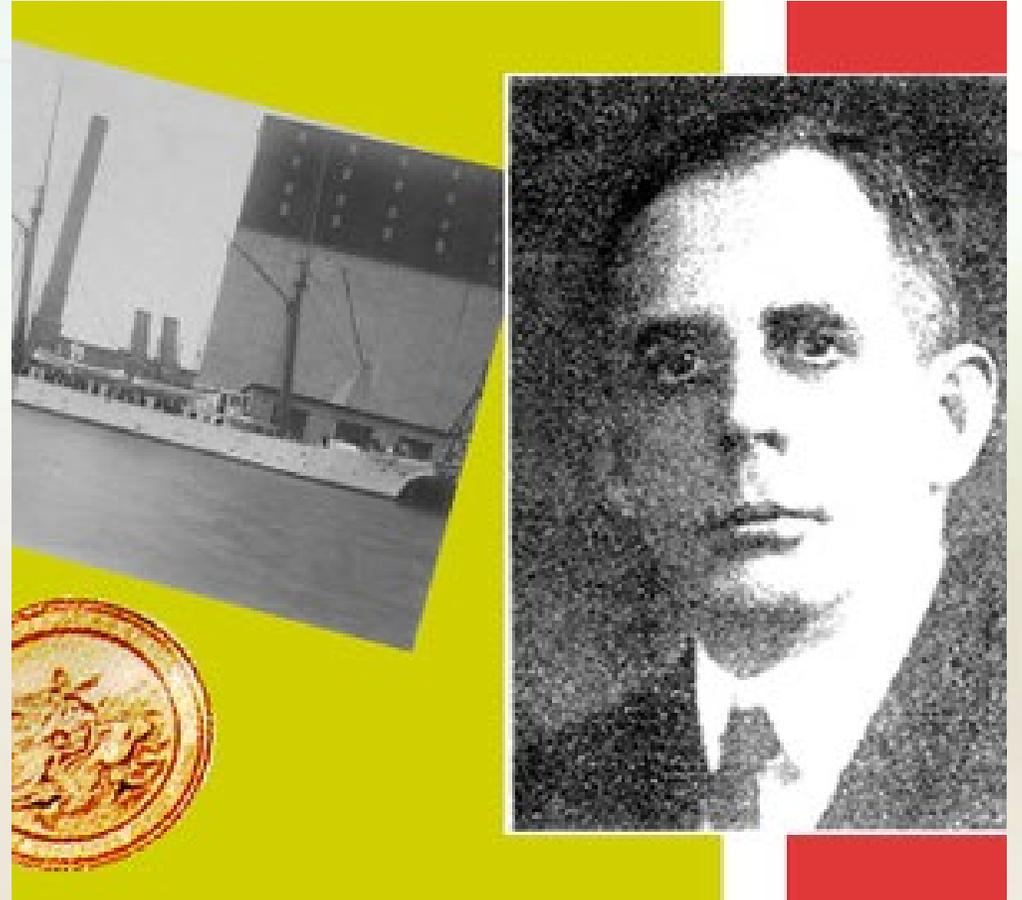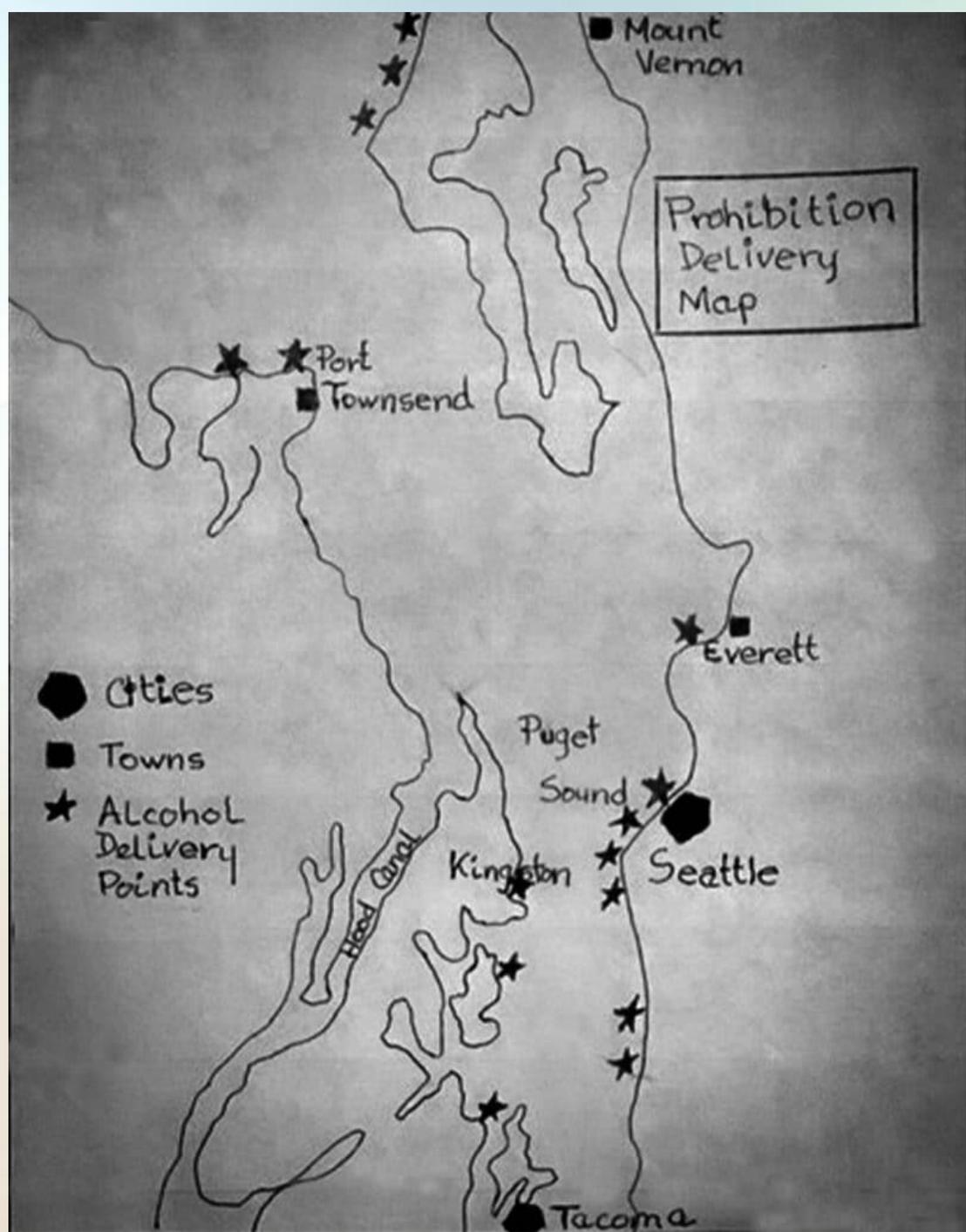
Elizebeth – 1920's

- In 1927, she was appointed 'Crypt Analyst' in the Bureau of Prohibition.

- 1928 – 1930 – Rum Smuggling was high in Gulf of Mexico and Pacific

- She appears in trials of smugglers in Galveston, Houston and New Orleans

- 1930 – Treasury Dept approved creation of a cryptanalytic unit – headed by Elizebeth Friedman -

The American Black Chamber

- 1931 – This book by Yardley was published that shook the cryptology world and government.

- Yardley – fired from State Dept

- Book disclosed US was reading diplomatic messages of Japanese Ambassadors

BLUEJACKET BOOKS

THE AMERICAN BLACK CHAMBER

HERBERT O. YARDLEY
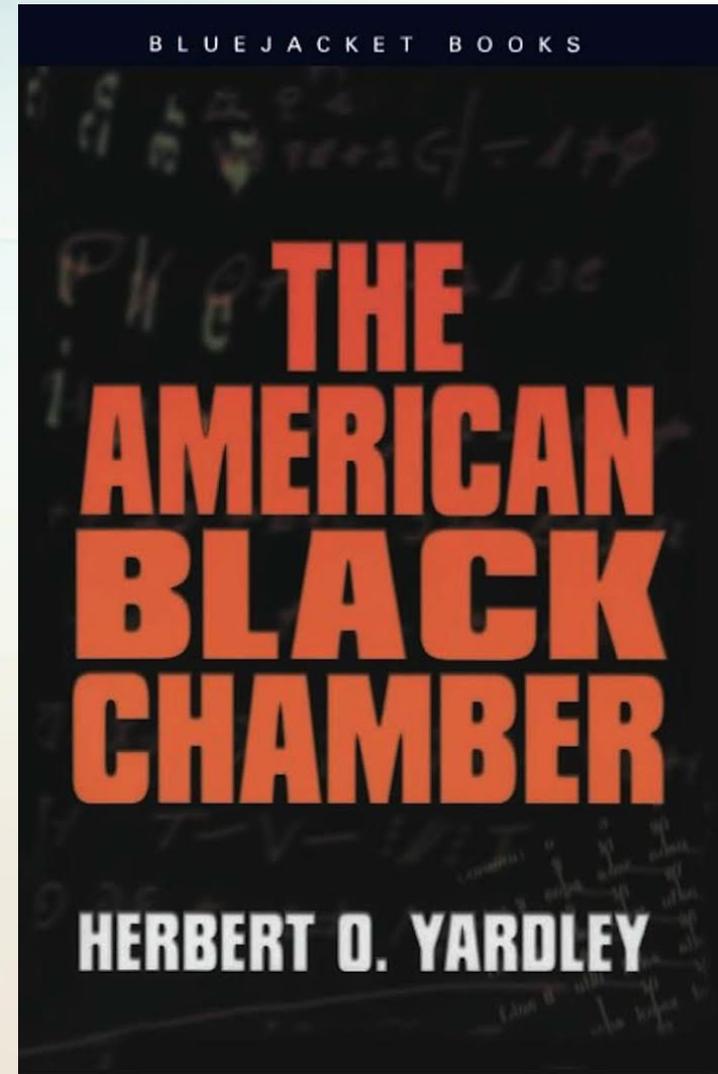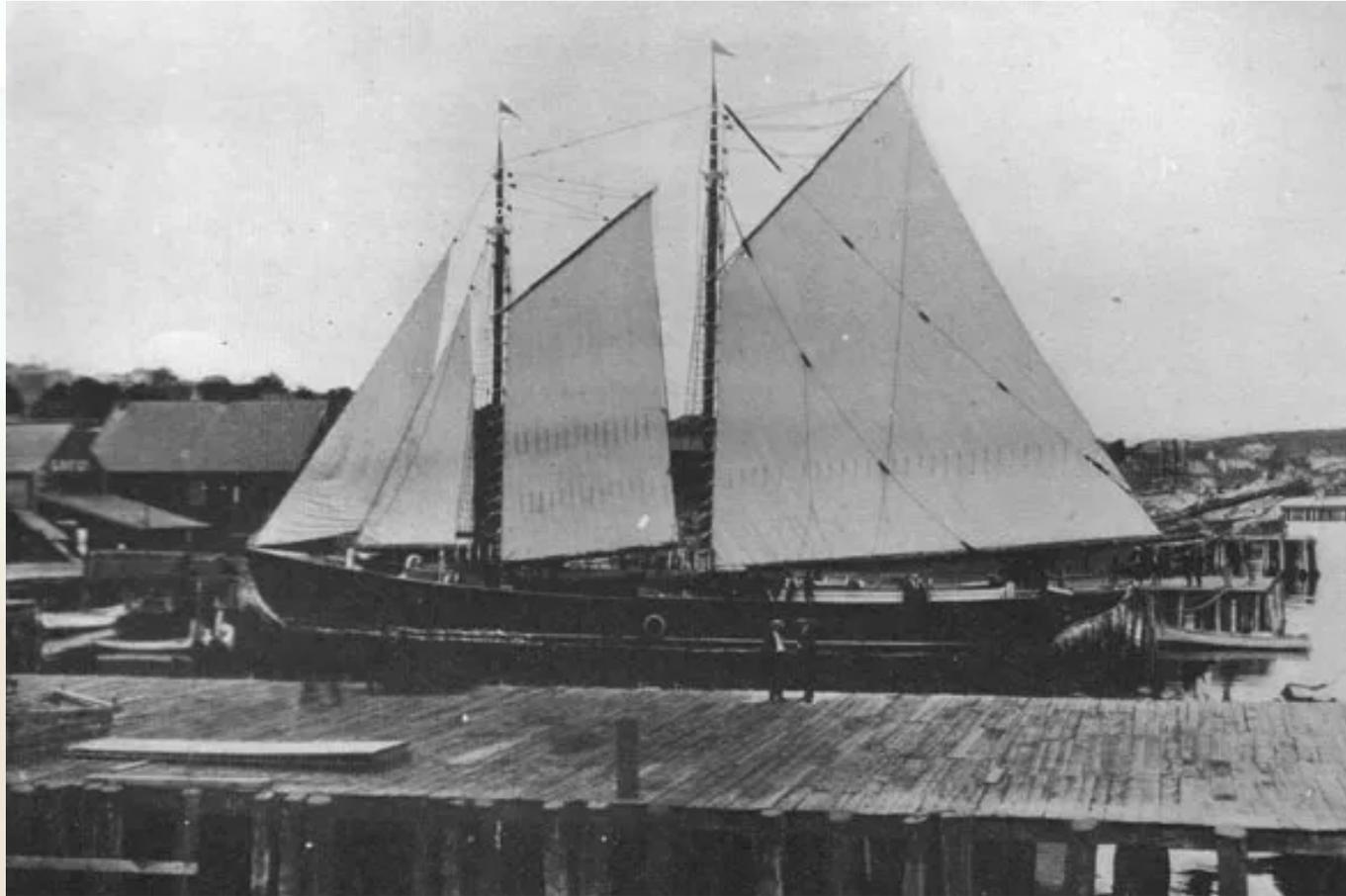
I'm Alone

Crew of the I'm Alone

I'm Alone: Deciphered Message
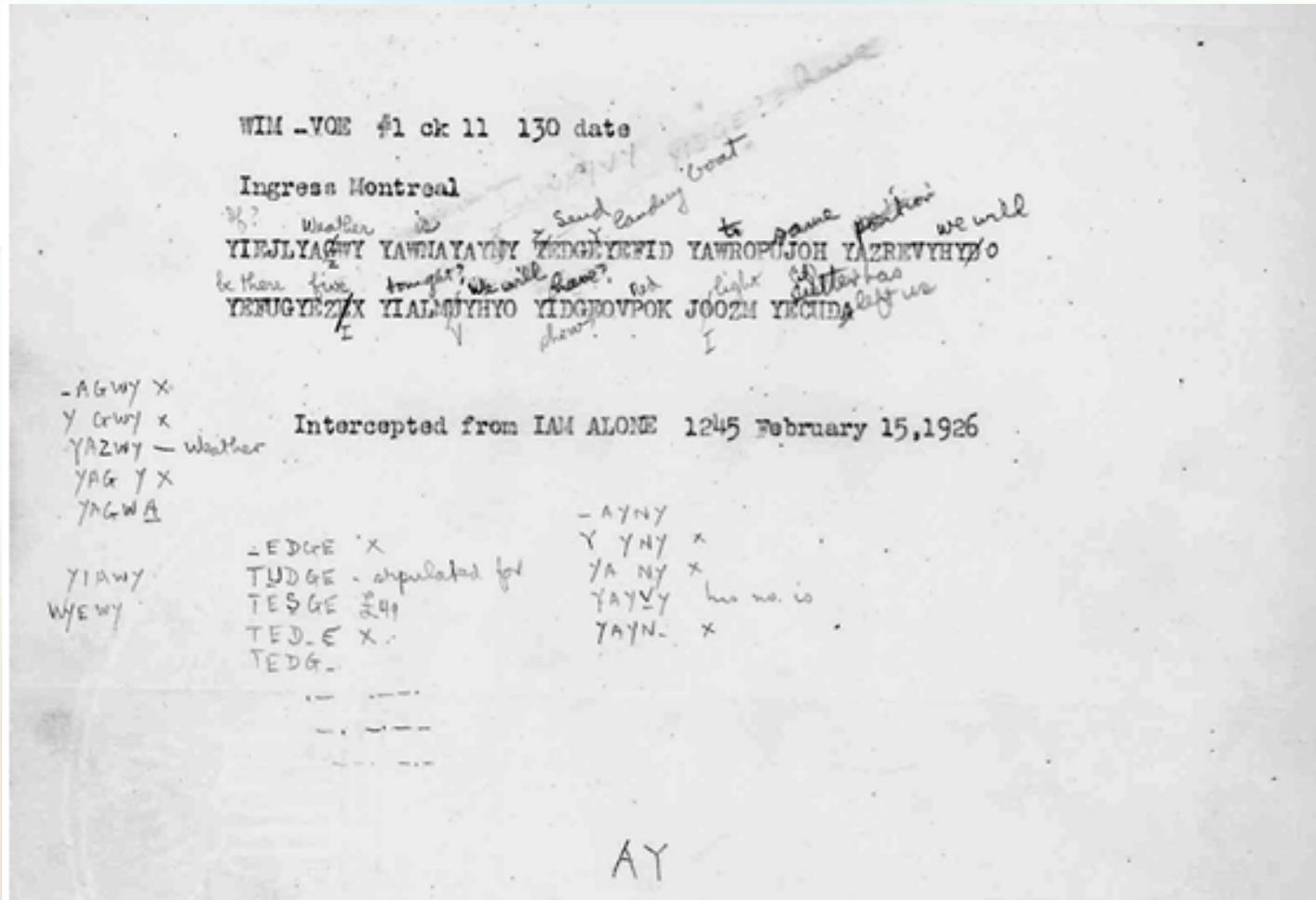
If weather is ---, send landing boat to same position. We will be there five tonight. We will have red light. Cutter has left us

I'm Alone

- Four year diplomatic incident
- The two governments agreed to submit the matter to **international arbitration**
  - Supreme Court Justice Willis Van Devanter serving as arbiter for the U.S.
  - Supreme Court of Canada Chief Justice Lyman Poore Duff appointed by Canada.
- International Arbitration took place in 1933
- Commission did recommend that the United States formally acknowledge its wrongdoing in sinking the ship with an apology to the government of Canada and a $25,000 payment.

CONEXCO and the Canadian Role

- Consolidated Exporters Corporation (CONEXCO) of Vancouver, Canada was run by George and Henry Reifel
- Messages gave little to no aid in figuring out who was running CONEXCO
- Connected to organized crime in the US

Example of Deciphered Message created by Consolidated Exporters

	MJFAK	ZYWKB	QATYT	JSL	QATS		QXYGX	OGTB
Message as sent:								
Cipher alphabet applied resulting								
in Acme lets	BARRY	OIJYS	where	and	when		WINUM	fuel
Acme code nos.	08033	53725					25536	
subtract 1000	07033	52725					24536	
ABC Code, 6th.	anchored							
		in harbor					are you sending	

Consolidated Exporters Company (CONEXCO)
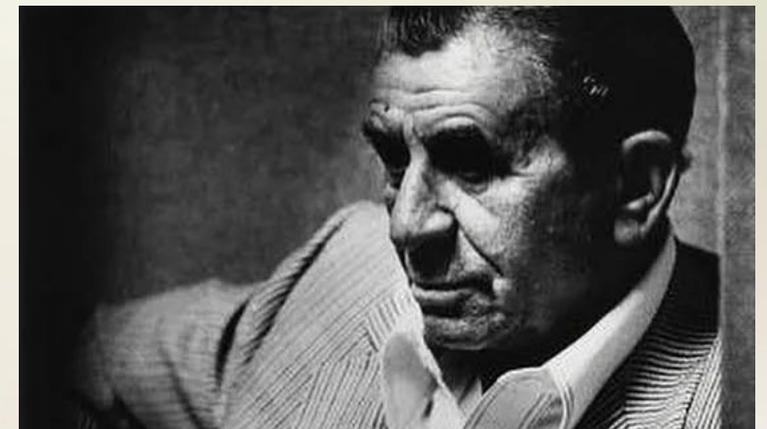
CONEXCO

- She went to the Grandy Jury to testify on this case.
- In 1933 – She received subpoena to appear in New Orleans at the trial of Bert Morrison and other alleged conspirators of Conexco, including Al Capones brother
- Elizebeth called to testify, defense objected
  - Her work was personal opinion, not based on science.
  - Judge allowed her to testify
  - Defense attorneys tried to trick her
  - To silence them, she asked the judge for a blackboard
  - She demonstrated the validity of the cipher method she used
- Morrison and other defendants were convicted – received max sentence
- This evidence was also used in later trials of CONEXCO members

Few persons in the present day realize anything of the enormity of the situation in the United States while the Volstead act was in effect. Government law enforcement agencies had no more taste for it than the public who loved their drink but government officials who with minor exceptions were honest at least had no choice but to pursue the rigid torturous paths of attempting to defeat the operations of these criminal gangs

Elizebeth Smith Friedman, 1970 interview

EZRA Brothers Opium Smuggling Ring

- In 1933 she also helped to bust an opium smuggling ring that was operated by the Ezra brothers out of Shanghai.

- They had created an opium combine.

- The Ezra brothers worked directly with Charles Luciano, Frank Costello and Meyer Lansky.

- The brothers were arrested in May of 1933.

THE ACCIDENT - 1937:
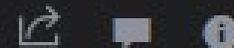
Gordan Lim

- Gordon Lim was a wealthy Chinese businessman

- He was suspected for years of operating a large drug smuggling ring by the Canadian authorities.

- Requested the U.S. Coast Guard's help in tracking the operations of Gordon Lim.

- Over 40000 cables were examined by Canadian intelligence agents. Of all these, 26 were forwarded to Elizebeth Friedman's office for decryption.

- The decryption took months

Gordon Lim

- 4 different systems of encipherment
- One of toughest ciphers she had ever come across
- Took more than 4 months to break these messages
- Testified in Jan 1938

WOMAN WINS FAME AS CRYPTANALYST; Mrs. Friedman 'Lent' by Coast Guard to Canada to Decode Opium-Ring Messages

By Winifred Mallon

Feb. 13, 1938

Share full article

Prohibition

- Elizebeth Smith Friedman testified in at least 33 cases as an expert witness during Prohibition, many of which involved rum smuggling
  - In many cases, federal agents were deployed as bodyguard to protect her.
  - Between 1920 and 1933 – 97 agents were lost (killed) so it was a threat not to be taken lightly.

Friedman Family

Duquesne Spy Ring

THE 33 CONVICTED MEMBERS OF THE DUQUESNE SPY RING

Johannes Becker

WWII

- During World War II, Friedman's Coast Guard unit was transferred to the Navy, where they were:
  - Principal U.S. source of intelligence on Operation Bolivar, the clandestine German network in South America.
  - Concern that Germany could eventually attack the U.S. via Latin America

- The FBI was given responsibility for countering this threat:
  - The one U.S. agency with staff experienced in detecting and monitoring clandestine spy transmissions was the Coast Guard, due to its earlier work against smugglers
  - Friedman's team was its sole cryptanalytic asset.

Elizebeth and Robert Gordon - 1940

© George C. Marshall Foundation

A spy who speaks in broken code is 'the goose that lays the golden egg. If you want to keep gathering the eggs, you must not frighten the goose.'

William Friedman

Hellmuth Incident

- Argentine Envoy Osmar Hellmuth travel to Germany

- Arrange secret weapons deal

- Britain took him off his ship

- British officers got him to confess to working with the SS

- Done without Germany knowing their code had been broken

It is now known that Elizebeth helped to smash a network of Nazi spies trying to foment fascist revolutions in South America - their goal being an attack on the US. Many of these spies were arrested as a direct consequence of her and her team's work.

Her work allowed the US to win the Battle of the Atlantic

J. Edgar Hoover and FBI

- Elizebeth Friedman had to sign an oath promising her silence of her wartime accomplishments until death.

- She had to watch as J. Edgar Hoover, the FBI Director at the time, take credit for her and her team's successes.

- At the end of World War II, Hoover began a public media campaign claiming that the FBI led the code-breaking effort that resulted in the collapse and arrest of the German spy network in South America.

  - This effort included a story in *The American Magazine* titled "How the Nazi Spy Invasion Was Smashed"

  - A publicity film called *The Battle of the United States.*

  - Neither mentioned Friedman or the Coast Guard

After WWII

- When her unit was disbanded in 1945, Friedman worked for the International Monetary Fund

- She continued to keep code breaking in her life by publishing a book with her husband further disproving the theory Bacon authored Shakespeare's plays.

- When her husband grew ill, she cared for him until his death in 1969.

The Shakespearean Ciphers Examined

An Analysis of Cryptographic Systems Used as Evidence that Some Author other than William Shakespeare Wrote the Plays Commonly Attributed to him

William F. Friedman and
Elizebeth S. Friedman

© George C. Marshall Foundation

Recognitions

- Friedman's contributions received increasing recognition after her death.

- In 1999, she was inducted to the [NSA Hall of Honor](#).

- The NSA auditorium, which had been named after William in 1975, was renamed in 1999 the "William and Elizebeth Friedman Auditorium."

- In 2002 NSA's OPS1 building was dedicated as the William and Elizebeth Friedman Building

- On June 17, 2014, the Bureau of Alcohol, Tobacco, and Firearms named its national headquarters auditorium after Elizebeth Smith Friedman.

- In April 2019, the Senate passed a resolution "Honoring the life and legacy of Elizebeth Smith Friedman, Cryptanalyst".

References