CIS 3362 9/16/24

① Breaking of Enigma

② Navajo Code

French secret agent bribed Hans Thilo Schmidt. Hans met agent allowed him to take pics of blueprints (~1929)

French made no progress

Gave blueprints to Polish because of a peace time pact.

~~Maj~~ Marian Rejewski (Polish mathematician)

Msg code →

R	J	U	R*	J	U		
A	Z	M	N	P	C		
			4th			4th	4th
						N	Y
						Y	R
R→A			R→N			N→Y	Y→R

R→N→Y→R (3)

3, 9, 2, 7, 5

⇒ 2, 3, 5, 7, 9

list book

102,000 entries

2, 3, 5, 7, 9 : DQR, S2, S1, S3

S1 S2 S3
S1 S3 S2
S2 S1 S3
S2 S3 S1
S3 S1 S2
S3 S2 S1

S1 S2 S3

$26^3 \times 6 \sim 102{,}000$ settings

Rejewski took 1 year to make his book. Then the Polish were reading Enigma messages from 1934/5 - 1939.

Germans added Scrambler Rotor #4 and Scrambler Rotor #5.

5 choices × 4 choice × 3 choice = 60

1, 2, 3
1, 3, 2
3, 1, 2
3, 2, 1
2, 1, 3
2, 3, 1

6

Instead of book needing 102,000 entries it needed 1 million entries!

Polish —shared→ British

Bletchley Park (British code breakers) has this info ~ 1940.

Turing mechanized the process of "making" the book so that process didn't take so long. (finished ~ 1 yr or a bit less)

Allies were reading Enigma messages!

things that helped:

① German weather report went out at the same time everyday + had a fixed format

② Many operators used the same msg code over and over again

(3) No letter ~~even~~ ever encrypted to itself.

Same time WWII (Navajo Code)

US enters war late 1941.

Most encryption techniques US used were believed to be secure but very slow.

On battlefield this was problematic.

Can we find something faster? grew up on Philip Johnston - retired military, Navajo reservation.

He knew Navajo was completely unlike English.

Pushed to create a code based on a Native American language.

Criteria for choice

1) Lack of evidence that any Japanese had learned it.
2) Enough men who were fit AND knew BOTH English + their native language.

Navajo chosen

Recruit Navajo

30 recruits found who passed their "tests". Sent them to San Diego for training to creak the code. 1 person dropped out + 3 people who were already in military who knew Navajo joined. 32 total.

3 months 32 men devised a code.

If there was a Navajo translation, that was used.

SPELLING WORDS LETTER BY LETTER, assigned a Navajo word to each letter

A - "Wolla ehe" - APPLE

274 common military words - "code words"

Version 1

⇒ Sent into Pacific theater late 1942

US often confused has thought Japanese had infiltrated radios.

* PROGRAM PAUSE

Set up demonstration otter US system vs Navajo code (40 sec) (30 min)

PROGRAM BACK ON ⇒ WORKED NOTIFY OTHER PARTS OF MILITARY

While 30 in Pacific, 2 stayed back to train the next batch.

CHANGES TO CODE

More code words added (~700)

Letter codes to thwart freq analysis

multiple codes for each letter, especially common ones.

A=	WOL-LE-CHE	ANT
	BE-LA-SANA	APPLE
	TSE-NILL	AXE