

Crypto Wars

The Evolution of Military Cryptology



11/6/2020



Ralph Simpson

Ralph@CipherHistory.com

Copyright © 2022

CC Attribution 4.0 International

All images and cipher devices in this presentation are from the collection of CipherHistory.com, unless otherwise noted

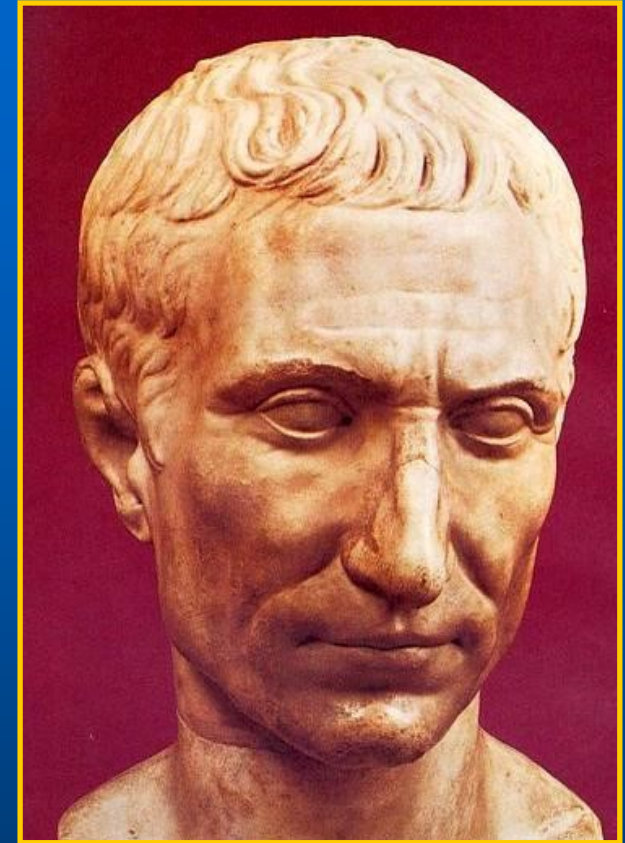
Agenda



- Caesar cipher
- Steganography
- Transpositions and grills
- Vigenère cipher disk
- Code books
- One-time pads
- Jefferson wheel cypher
- Electro-mechanical rotor ciphers
- Hagelin cipher devices
- Navajo code talkers cipher
- IFF code wheels
- Voice encryption device

Caesar Cipher

- First known use of cryptology in warfare was the Caesar cipher
- Cipher was a shift of the alphabet by 3 letters - “a” enciphered as “d”, “b” becomes “e”, etc.
- Weak cipher but effective against illiterate enemy
- No cipher device or key to be captured
- Nero apparently thought the Caesar shift too complex, he used a shift of only one character
- Any substitution of characters which is constant for an entire message is a monoalphabetic cipher
- First known codebreaking was by Al-Khalil (c. 725-790 AD) who deciphered a letter from a Byzantine emperor by guessing it contained “in the name of God”
- First systematic solution for monoalphabetic cipher was by Ibn ad-Duraihim (1312-1361) using letter frequency analysis based on the Koran



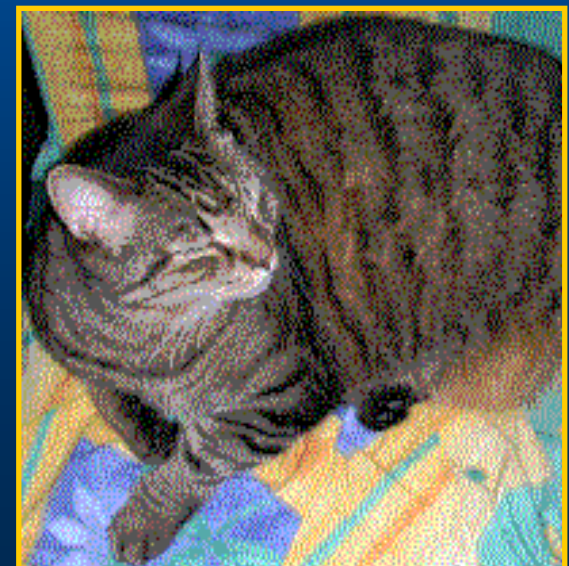
Julius Caesar (100BC – 44BC)

Steganography

- Steganography is Greek for concealed writing
- Messages were hidden inside objects, swallowed, made into a microdot, behind postage stamp, tattooed on scalp, etc.
- Both message content and parties are protected
- George Washington relied on invisible ink
- As detection techniques improved, new invisible inks were developed
- In 2011, the CIA released US invisible ink recipes from WW1
- Later technology uses random noise in jpg pictures, communication protocols, etc.



2 least significant of 256 bits per pixel removed from picture above yields the image below



Transpositions and Grills

- Transposition is a physical rearrangement of letters, making the message unintelligible
- A grill is usually a piece of paper with holes cut to write and display the message among a larger set of letters, making a transposition more user friendly
- In 1550, Girolamo Cardano suggested writing a secret message in a grill, then filling in the rest of the page so the letter looks intelligible, which combines transposition with steganography
- Transposition, by itself, is not very strong, so it is usually combined with some other type of cipher
- In WW1, the German ADFGX cipher combined transposition and a diagraphic cipher, which changed pairs of letters into another enciphered pair



KL-99 US Navy grill

Vigenère Cipher Disk

- Vigenère cipher invented in 1467 by Leon Battista Alberti, 56 years before Vigenère was born
- Polyalphabetic cipher changes cipher many times in a message – thwarting letter frequency analysis
- Alberti claimed the cipher was unbreakable, 450 years later *Scientific American* magazine agreed
- Disk with keywords simplified polyalphabetic ciphers
- Polyalphabetic ciphers broken by using letter frequency to decipher the same letter position of several messages and by deciphering keywords
- Used by South in Civil War and consistently broken by the Union Army
- Vigenère disk still used in modern times – GRA-71 burst encoder, Whiz wheel



Alberti drawing of 1467



One of 5 surviving CSA disks

Code Books

- Ciphers change each letter of message, codes change whole words or phrases
- Code books were in widespread use for centuries – until WW2
- Codes also saved money in telegraph costs
- Usually, codes were combined with other ciphers
- Code books of up to 100,000 codes are kept for years
- If code book is compromised, sending out new code books is very cumbersome and risky
- US spies copied Japanese code book before WW2

Questions.		SHIPPING.		Fop.	
No.	SENTENCES.	No. of Cipher Word.	No.	Cipher.	No. of Sentence.
3139	What vessel did you ship by ?.....		3139	Foppish	
3140	When, how, and by what route shipped ?...		3140	Forage	
3141	When and how were bills of lading forwarded ?.....		3141	Forbade	
3142	When can you ship ?.....		3142	Forbear	
3143	When will a sailing vessel clear for——?		3143	Forbid	
3144	When will you ship ?.....		3144	Forbidden	
3145	Which did you ship ?.....		3145	Fordable	
3146	Who are the consignees ?.....		3146	Forego	
3147	Will a few days delay in shipping make any difference to you ?.....		3147	Forenead.	
3148	Will you receive consignment of——?		3148	Forelock	
3149	Ship		3149	Foremost	
3150	Ship additional.....		3150	Forest	

Example from 1888 code book

One-Time Pads

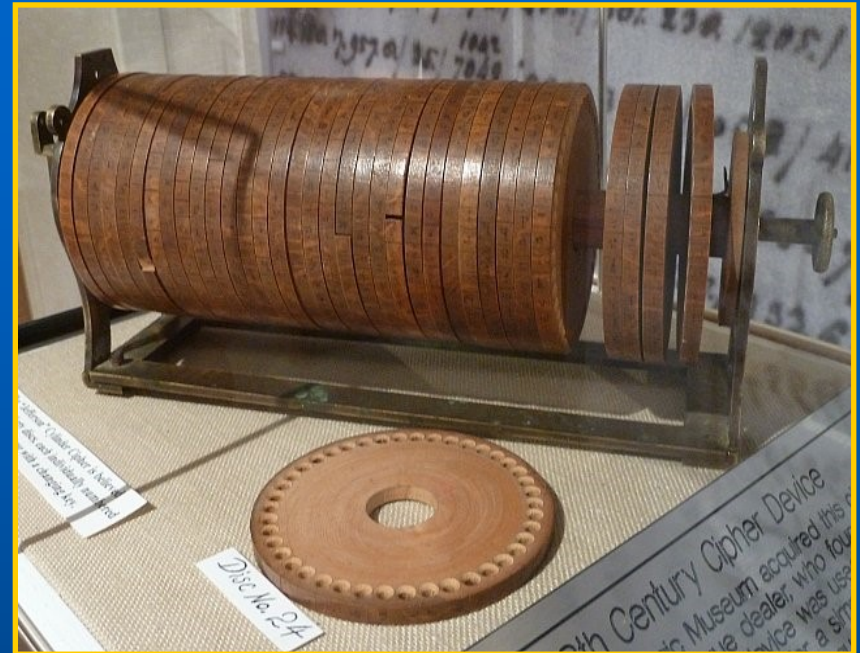
- One-time pad is the only unbreakable cipher
- Requires every letter to be changed by random number and used only once
- Popular with spies and named after small pads of random numbers
- Thought to be invented in 1919 by Gilbert Vernam and Joseph Mauborgne
- First use of one-time pad was in teletype, using Baudot codes to automatically encipher and decipher messages without operator involvement
- NSA called this patent "one of the most important in the history of cryptography"
- Used for high-level messages, transporting one-time tapes too cumbersome & risky



Hagelin one-time pad and M-209

Jefferson Wheel Cypher and M-94

- Yes, invented by our third president in mid-1790s, possibly inspired by Chinese combination locks and discovered in his writings in 1922
- Each wheel has a different random alphabet, the key is the order of wheels on spindle
- Message spelled out on one row, any other row sent for a strong and user-friendly cipher
- Coincidentally re-invented in 1922 by Parker Hitt and Joseph Mauborgne as M-94, used 1922-1943
- Mauborgne also co-invented one-time pad and demonstrated 1st aircraft use of 2-way radio



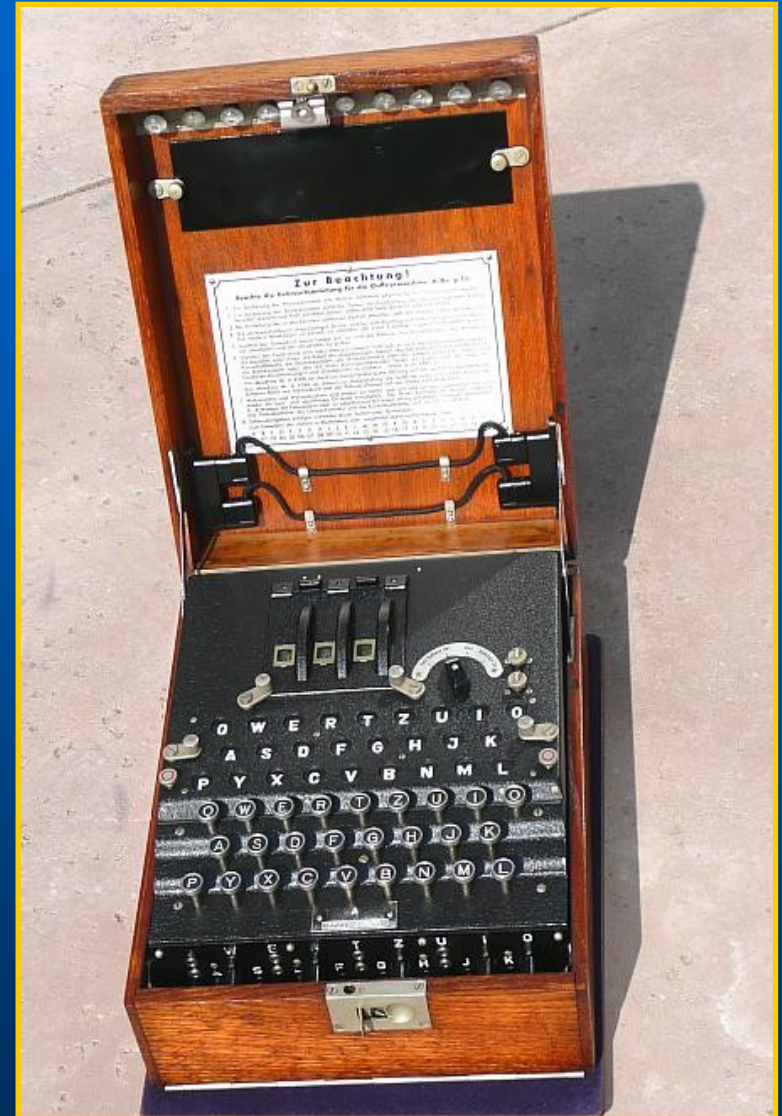
Only existing Jefferson Wheel Cypher

US Army M-94



Electro-Mechanical Rotor Ciphers

- Electro-mechanical rotor ciphers invented by 4 people in 4 countries after WW1
- Most famous was the German Enigma machine
- Current went through multiple rotors to change each letter several times
- Key was the selection and order of rotors with addition of plugboard for Enigma
- Despite overwhelming odds, Enigma was broken by Polish, British, and US code-breakers, significantly shortening WW2
- US altered British mechanical bombe, using tubes for memory - first computer
- 2003 discovery - electro-mechanical rotor cipher was first invented in 1915 by 2 Dutch Naval Officers, but kept secret



Infamous Nazi Enigma machine

Hagelin Cipher Devices

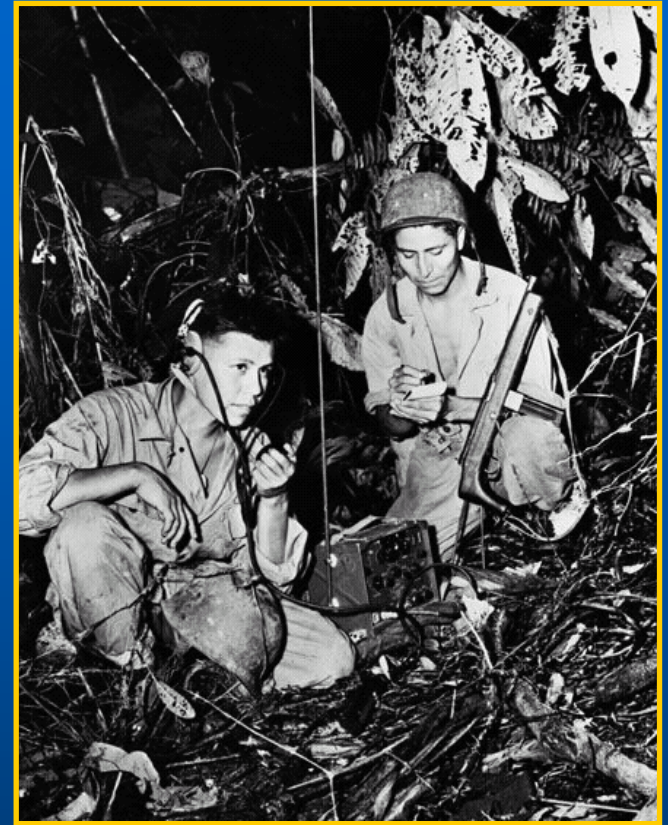
- Early Hagelin machines used electro-mechanical rotors
- Beginning with C-35, including US M-209, later Hagelin devices used mechanical means to select a reciprocal alphabet
- Inspiration for this new cryptologic technology came from coin changers
- Swedish Transvertex HC-9 used Hagelin technology, Transvertex CEO was Director in Crypto AG – “HC”- Hagelin Cipher
- Hagelin made a deal with US NSA to give access to the world’s secrets for 4 decades
- Hagelin/NSA backdoor disclosed to Russia & Israel by spies Aldrich Ames & Jonathan Pollard
- Russia told Iran, who blew the cover on this greatest sting in history in 1993



Hagelin M-209 cipher

Navajo Code Talkers

- Navajo language was oral only and hard to master and understand - 30 non-native speakers in WW2
- US Marine Corp demonstrated ciphering, sending and deciphering a message in 20 seconds by Navajos vs. 30 minutes by M-209
- One of few ciphers not broken in WW2
- Navajo code talkers were in every major battle in the Pacific
- Seven code talkers were KIA, none captured
- Navajo code talkers were used in Korea and the beginning of the war in Vietnam
- Use of Navajo code talkers was declassified in 1968 and the original 29 code talkers were awarded Congressional Gold Medals in 2000



Navajo code talker on TBY radio
Image on commemorative medal



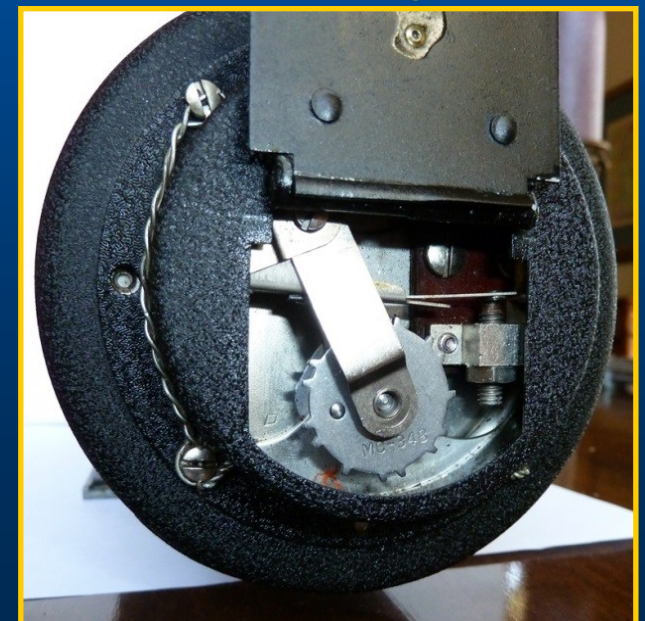
Identify Friend or Foe Cipher Wheels

- Radar and faster planes required pilots to identify enemy aircraft before visual sighting
- IFF radios were invented in WW2, but cryptology was needed to prevent the enemy from using the radio from a downed plane
- Germans were first to use IFF, but the British made a device to locate the German plane, so IFF was not used
- First US IFF radio was the ABA-1, used a cipher wheel inserted into the dynamotor of the radio
- Crypto was crude but effective, one of 10 wheels was selected for use that day
- IFF later developed into the transponder, which is in every aircraft today



P-51 Mustang

Cipher wheel in dynamotor



Voice Encryption

- Early voice scramblers added noise to a voice message or changed frequencies / time splices
- Analog technology used by Roosevelt & Churchill



MS-2001, KY-57 and KY-28

- was regularly broken by Nazis before 1943, until first digital voice encryption, SIGSALY
- Analog technology (KY-28) was upgraded to digital encryption (ex. KY-57)
- In 1993, US NSA Clipper chip planned to be mandated for all communication devices
- Design flaw of Clipper chip spurred widespread adoption of open standard, public key encryption, PGP

AT&T TSD-3600E with Clipper Chip



Download this Presentation

CipherHistory.com/slides/cryptowars.pptx

