

Hagelin Cipher Machines

The World's Most Successful and Controversial



December 15, 2022



Ralph Simpson

Ralph@CipherHistory.com

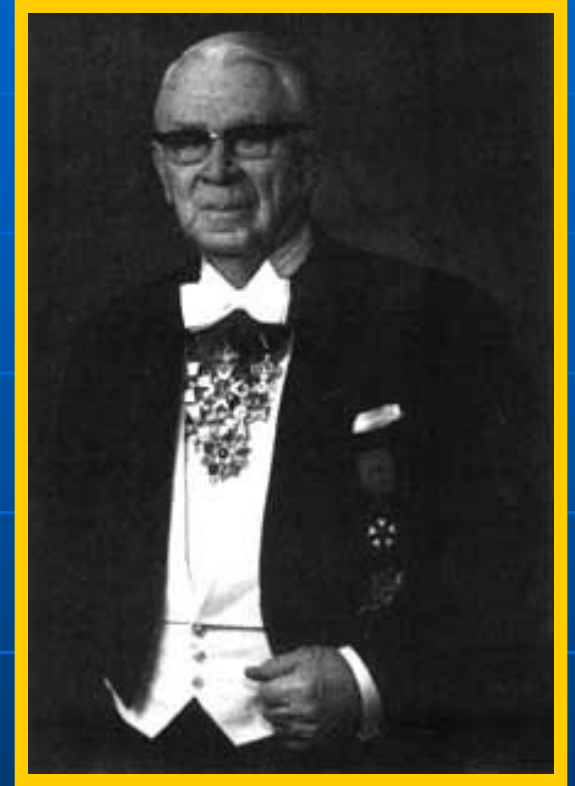
Copyright © 2022

[CC Attribution 4.0 International](#)

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

Agenda

- Early rotor cipher machine by Arvid Damm
- Hagelin joins Damm to sell rotor machines
- Hagelin invents “pin and lug” cipher machine
- US adopts Hagelin M-209 for WW2
- Germany steals “pin and lug” technology
- Transvertex “pin and lug” technology
- Crypto AG moves to Switzerland
- NSA/Hagelin backdoor used for 35 years
- Iran kidnaps Crypto AG salesman
- Fugitive billionaire buys Crypto AG



**Boris Hagelin
(1892-1983)**

Electro-Mechanical Rotor Ciphers



Arvid Damm

B-21 cipher machine



- Electro-mechanical rotor ciphers invented and patented by 4 people in 4 countries after WW1
- Most infamous was the German Enigma machine
- Arvid Damm of Sweden invented the second most successful rotor cipher device
- Damm cipher used 2 rotors and pin wheels for irregular stepping, but it performed erratically
- Emanuel Nobel (nephew of Alfred) and K.W. Hagelin were investors, hired son Boris to join firm in 1922
- Boris Hagelin sold large order to Swedish Army in 1926, Damm dies later that year
- B-211 hand-held cipher device made for French Army, another large order

Hagelin “Pin and Lug” Cipher

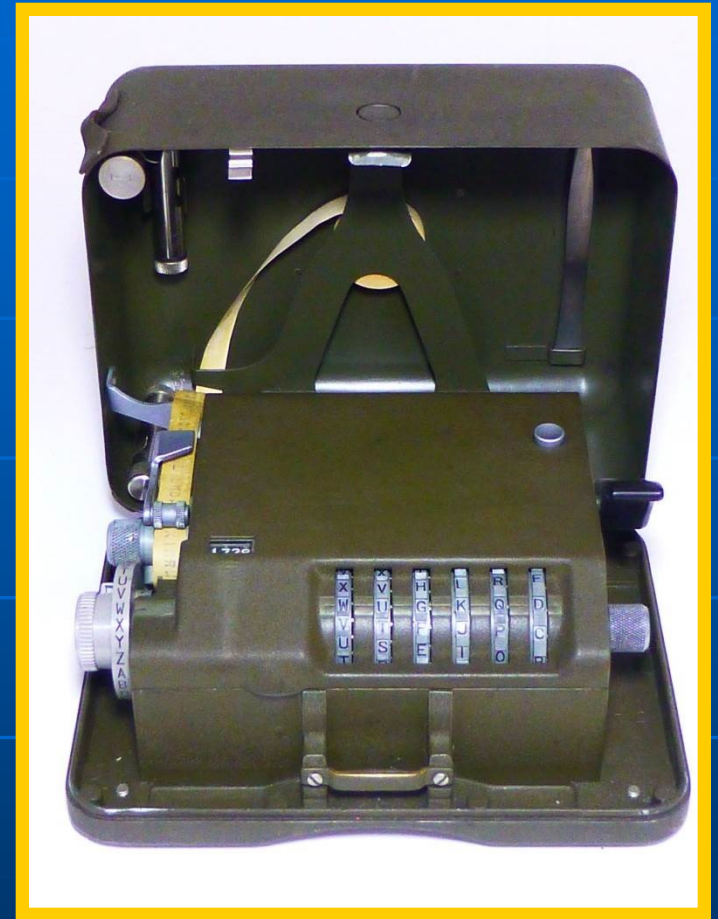
- Hagelin develops coin changer, customer reneges on contract
- Coin changer adding function gives Hagelin inspiration for a new cipher technology
- Hagelin invents the first “pin and lug” cipher device, the C-35 in 1935
- Entirely mechanical addition function to select reciprocal alphabet
- 5 wheels all advance one character at a time
- Wheels have mutually prime number of letters for a longer message depth
- After C-35 improved versions C-36, C-37 and C-38
- Sold C-38 to US military, made changes and named M-209 in 1942
- Made compatible cipher, C-446 for Allies



Hagelin C-35 cipher

US M-209 Cipher Machine

- Light, portable, easy-to-use, printed output
- M-209 replaces M-94 in 1942, used until mid 1960s
- M-209 cipher was broken by Germans in WW2 in about 4 hours
- Used as battlefield cipher only
- 140,000 were made on royalty basis by LC Smith & Corona Typewriter Co. (\$64 each)
- Hagelin became the first millionaire from cipher technology
- Switch for cipher/decipher mode
- “Z” is deciphered to a space, so the printed output is easier to read



Hagelin M-209 cipher

US M-209 How it Works

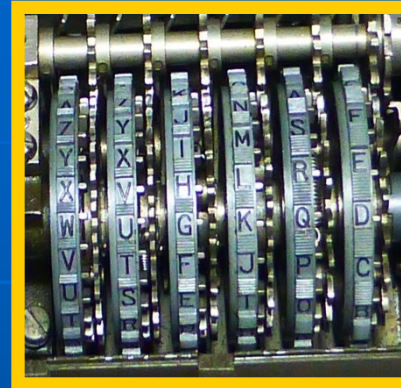
- 6 wheels have different number of letters (l-r)
26-25-23-21-19-17
- All wheels rotate one space at a time
- Mutually prime wheels give a message depth of 101+ million
- Each wheel has a pin at each letter, which is set to active (right) or inactive (left)
- Large drum behind 6 wheels has 27 bars with 2“lugs” on each bar
- Lugs can be set to one of the wheels or to an inactive position
- Active pins and active lugs are added for a shift value to encipher or decipher
- Print wheel has a fixed reciprocal alphabet



M-209 with inner lid open to reveal 6 wheels and drum

US M-209 Key Length

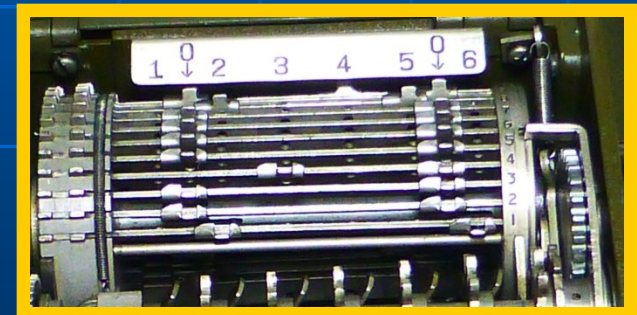
- Key length contributed by pins:
 - # Settings = $W! / (A! \times (W-A)!)$
 - W = # wheels, A = # active pins



Pin set left (inactive) or right (active) for each letter

# Active Pins	# Settings
0	1
1	6
2	15
3	20
4	15
5	6
6	1
Total	64

- Key length contributed by lugs:
 - 2 lugs on 27 bars, set to two of 8 positions (6 wheels and 2 inactive)
 - $8! / (2! \times (8-2!)) = 28$ settings for each bar
 - 28 settings X 27 bars = **756** total



2 lugs set on 8 positions per bar

- Key length contributed by wheels: $26 \times 25 \times 23 \times 21 \times 19 \times 17 = 101,405,850$
- Total key length = $64 \times 756 \times 101,405,850 = 4,906,420,646,400$ or 4.9×10^{12}
- Compared to M-94 key length = 6.7×10^{24} , Enigma key length = 10^{23}

German SG-41



German SG-41

- In 1941, Germany copied the Hagelin pin and lug technology, called the Schlüsselgeraet-41
 - SG-41 used 6 wheels, printed both cipher and plain text
 - 6th wheel used for irregular stepping for the other 5
 - Intended to replace the Enigma, but only 500 were manufactured
-
- Nicknamed “Hitler Mill” since mill is German slang for typewriter
 - Hagelin was upset over the German theft of his design, calling it a “C-41”

Crypto AG moves to Zug



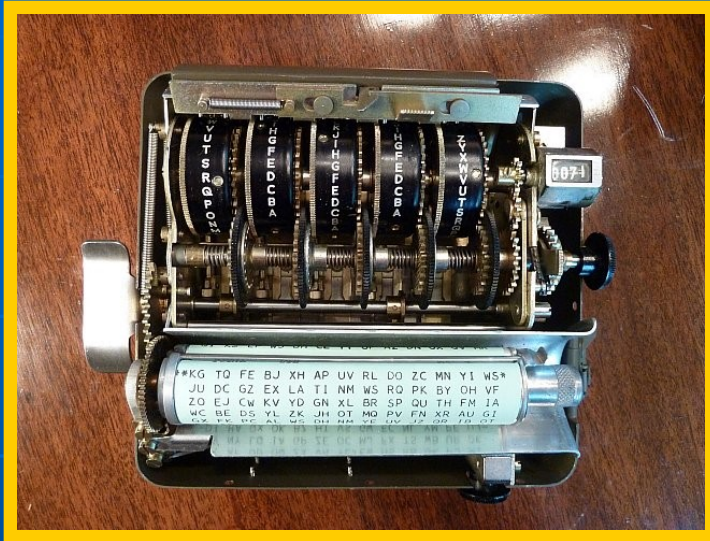
Zug, Switzerland



Hagelin in Zug factory

- After WW2, Sweden declared crypto technology as munitions, outlawed sales outside Sweden
- Cryptoteknik moves to Zug, Switzerland in 1952
- Hagelin renames company **Crypto AG**
- Zug gave image of precision of a Swiss watch and neutrality of a Swiss bank

Transvertex



HC-9 with cover removed



Rear card of HC-9

- Transvertex formed in Sweden in 1951, remained in business until 1969
- Hagelin's Technical Director, Vigo Lindstein, became CEO
- Transvertex quickly produced teletype cipher and "pin and lug" cipher, HC-9
- HC-9 may be a tribute to Hagelin, HC = Hagelin cipher & 9th cipher machine
- Punched card replaced pin and lugs, second card has 16 reciprocal alphabets
- No printing capability but strong and easy to use cipher
- Curiously, did not allow a letter to cipher to itself, reducing its strength

Hagelin Cipher Machines after WW2



CX-52 and CD-57

- Crypto AG sells the most widely used cipher machines in history
- 120 different countries adopt CX-52 for military, diplomatic and business use
- CD-57 hand-held cipher compatible with CX-52

- T-52 and T-55 teletype ciphers were compatible with CX-52 and also worked with one-time tapes
- CX-52-RT used for manual one-time tapes
- CX-52 finally replaced by electronic cipher machines in the 1970s



T-55 teletype cipher

Iran Kidnaps Crypto Salesman



Hans Buehler

- In 1992, Iran kidnapped Crypto salesman, Hans Buehler, accused of spying for US/Germany
- Buehler interrogated 5 hours per day for 9 months but had no knowledge of rigged Crypto AG devices
- Crypto AG and Siemens paid the million dollar ransom
- Siemen's Director calls Crypto AG, "secret Siemen's daughter"
- After release from Iran, Crypto AG fired Buehler and billed him for ransom!
- Buehler discovers truth about backdoor, sues Crypto AG, settles out of court
- Buehler wrote a book about his ordeal and discoveries
- Boris Hagelin admits to backdoor to Hagelin engineer, but Crypto AG denies it
- The greatest sting in modern history was finally revealed after 35 years

Hagelin/NSA Backdoor Revealed

- Hagelin/NSA backdoor disclosed to Israel by spy Jonathan Pollard in 1983
- Israel discloses Hagelin backdoor to Russia in exchange for increase in refugees of Soviet Jews
- Russia already knew about backdoor from spies Aldrich Ames and Robert Hanssen
- Russia likely told Iran about the backdoor
- In 1988, messages to Iranian embassies decoded about the bombing of Pan Am 103 over Lockerbie
- Former Iranian Prime Minister Shahpour Baktiar assassinated in 1991
- The day of the assassination, but before his body was found, US decoded a message to Iranian embassies, "Is Bakhtiar dead?"
- US knowledge of these messages confirmed Hagelin backdoor to Iran

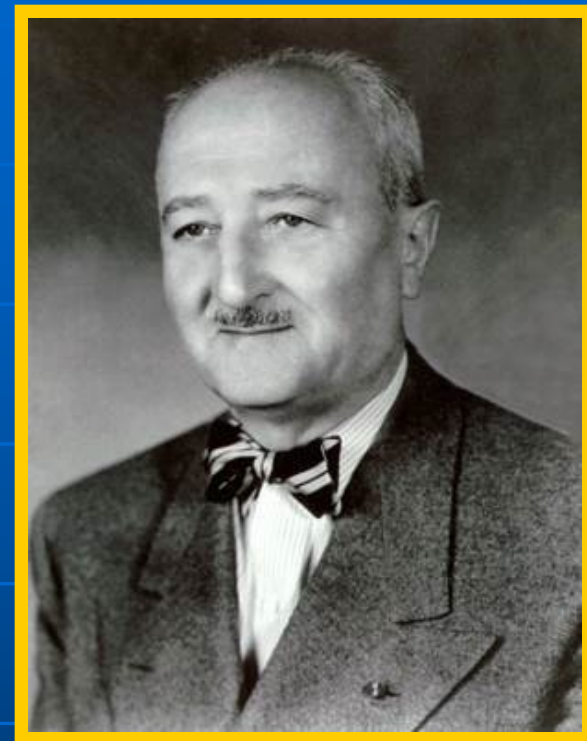


Shahpour Baktiar

Origins of NSA Backdoors

- In 1957, William F. Friedman was called out of retirement to negotiate backdoor for NSA
- Friedman was the renown cryptographer who solved the Japanese Purple cipher and invented the Sigaba cipher machine
- Boris Hagelin personally negotiated the agreement
- In exchange, Crypto AG was given export licenses around the world and sold to 130 countries

Official NSA PR photo: agency gets message from above

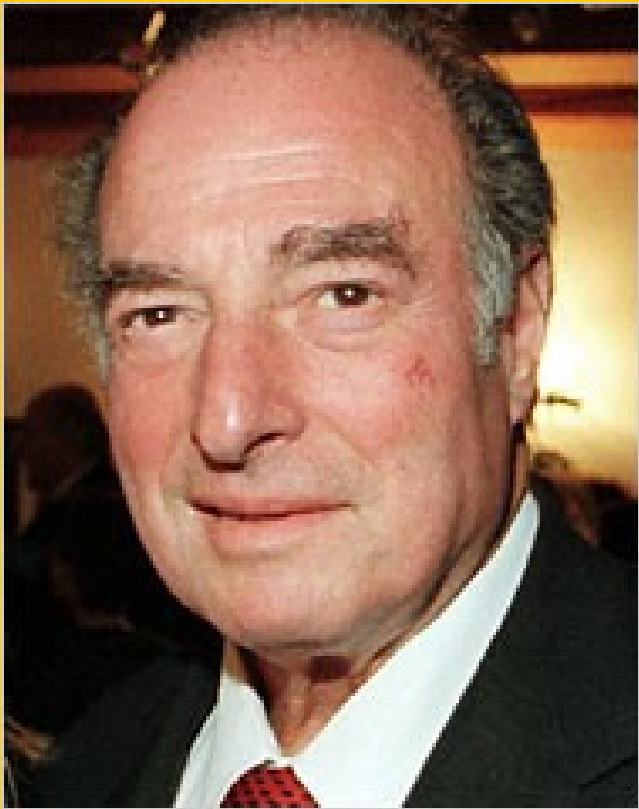


**William F. Friedman
1891-1969**



- UK gave her colonies surplus CX-52s for free
- Crypto AG's machines went digital in 1970s, backdoor in EPROM negotiated by NSA's Nora Mackabee

Crypto AG bought by Marc Rich



**Marc Rich
(1934-2013)**

- Revelation of NSA backdoor in 1993 caused Crypto AG sales, stock price to plummet
- Faced with bankruptcy, Crypto AG saved by angel investor, Marc Rich
- Rich was a resident of Zug and a fugitive billionaire with ties to Israeli Mossad
- Speculated he used the backdoor for financial gain and to aid Israeli intelligence
- Clinton pardoned Rich in his last hours in the White House, 2001
- Rich's attorney was Scooter Libby, later Cheney's Chief of Staff, who outted CIA agent Valerie Plame and later convicted of 4 felonies
- In 2002, another Crypto AG salesman was mysteriously murdered in Saudi

Arabia after revelations of theft of money from Swiss banks

Download this Presentation

CipherHistory.com/hagelin.ppt

