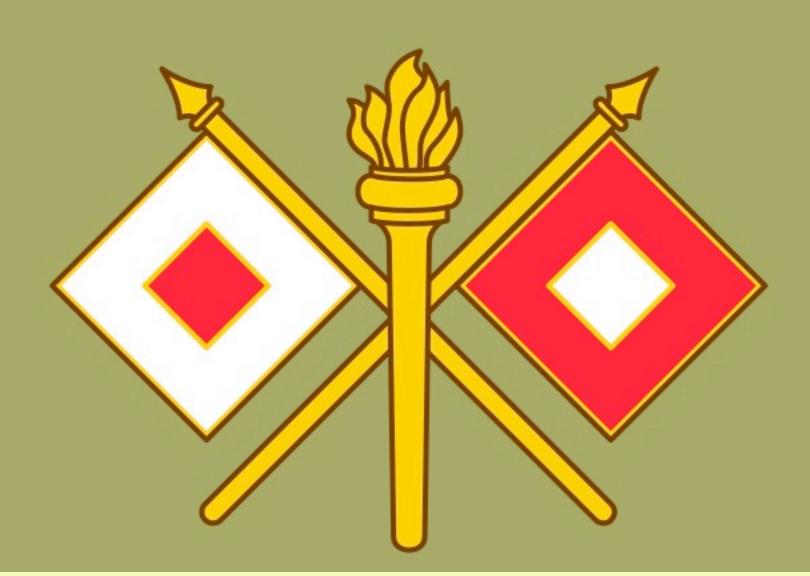
CONVERTER M-209-B



MARK J. BLAIR, NF6X MAY 1, 2009

INTRODUCTION

- Description
- History
- Operation
- Q&A
- Demonstration



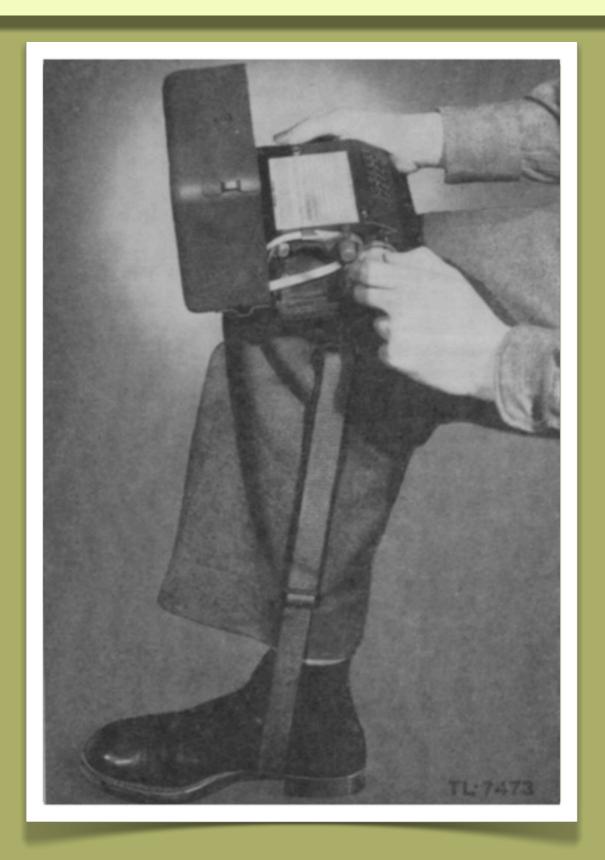
DESCRIPTION

- Mechanical cipher machine
- Prints plaintext/ciphertext on paper tape
- Light and compact, usable in the field
- No electricity needed
- Simple to operate once keyed

DESCRIPTION



DESCRIPTION



HISTORY

- Model C-35 Hagelin Cryptograph invented by Swedish cryptographer Boris Hagelin around 1934-1935
- Improved models C-36 and C-38 followed
- Hagelin promoted his machines to U.S. government in 1940
- U.S. licensed C-38 with minor modifications, called it Converter M-209

HISTORY

- Over 140,000 machines produced during World War 2 by many companies
- Several versions with minor production variations, including M-209, M-209-A,
 M-209-B and CSP-1500 (Navy version)
- Used for encryption of low-level tactical traffic throughout World War 2 and the Korean War

OPERATION

- Machine must first be programmed with proper key... more on this later
- Operator sets machine to Cipher or Decipher mode
- Operator dials in each letter with setting knob on left, then turns drive knob on right
- Machine prints each enciphered or deciphered letter on paper tape

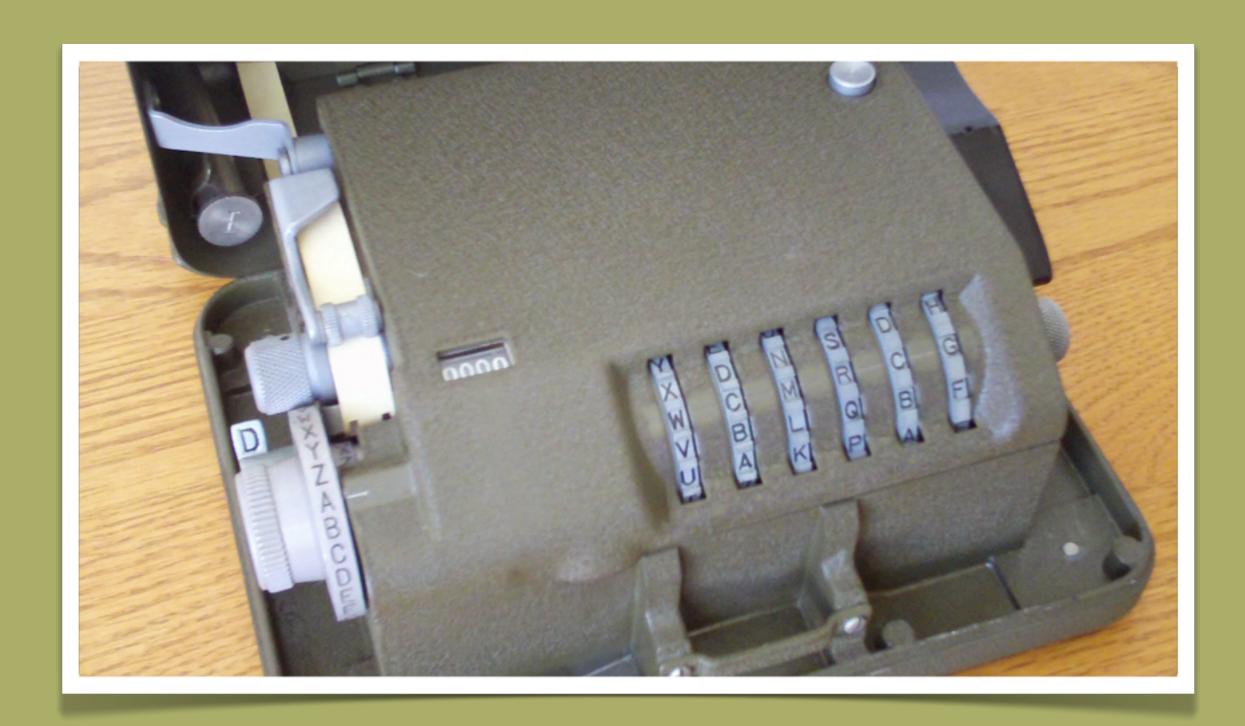
OPERATION

- When ciphering, enter 'Z' in place of space
- Ciphertext automatically printed as 5-letter groups
- When deciphering, ignore spaces
- Deciphered 'Z' printed as space
- Text may be read from wheel if out of ink/ paper

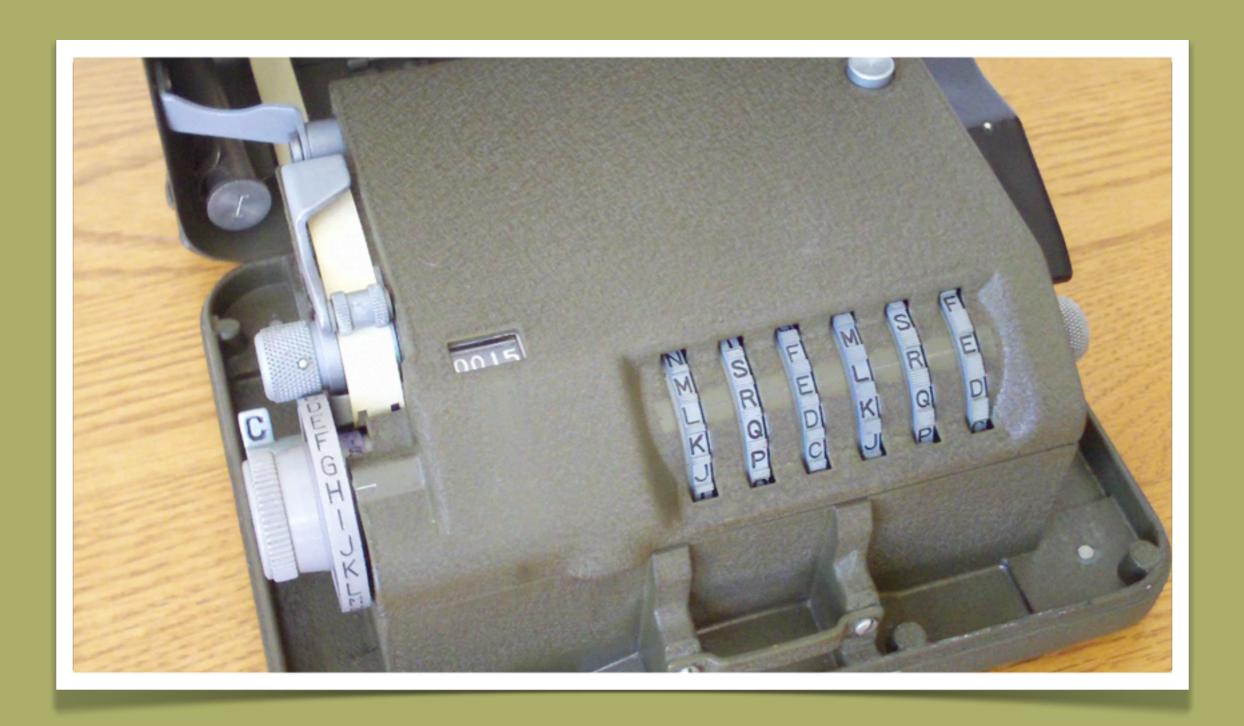
OPERATION

- Drive knob locks after each letter, until setting knob is turned:
 - If setting knob is already set to next letter, turn it back and forth to unlock drive knob

CIPHERING



DECIPHERING



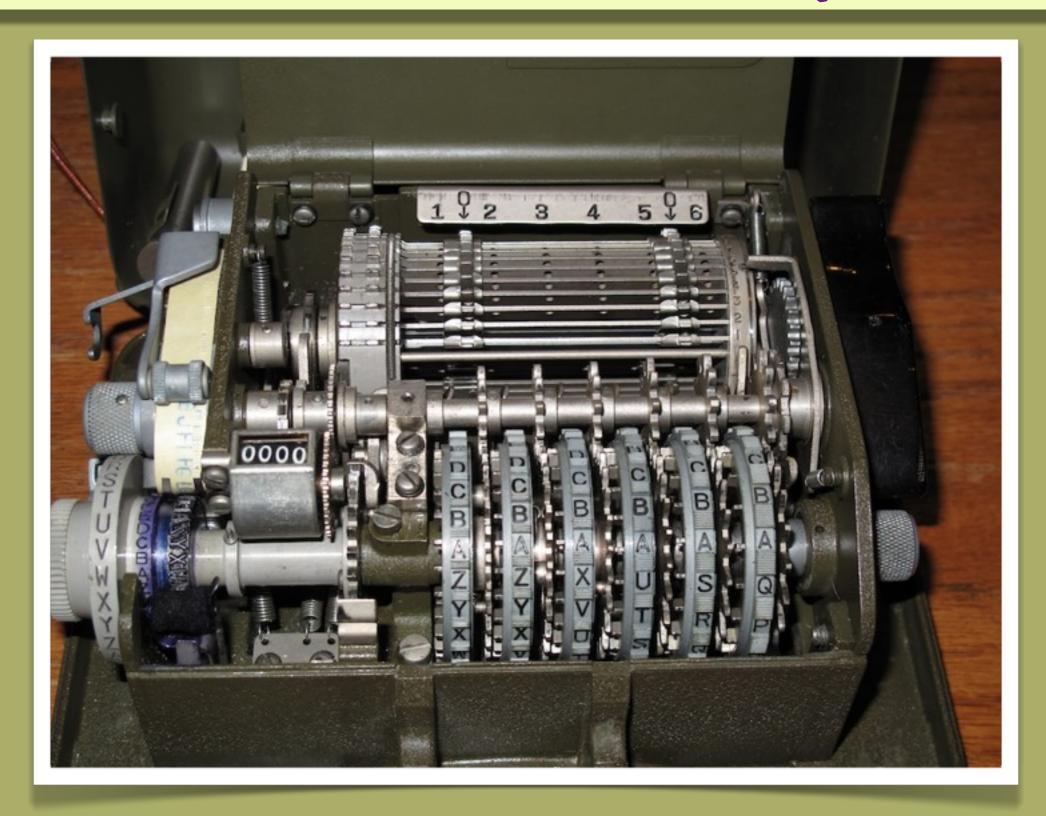
KEYING

Cipher key consists of two parts:

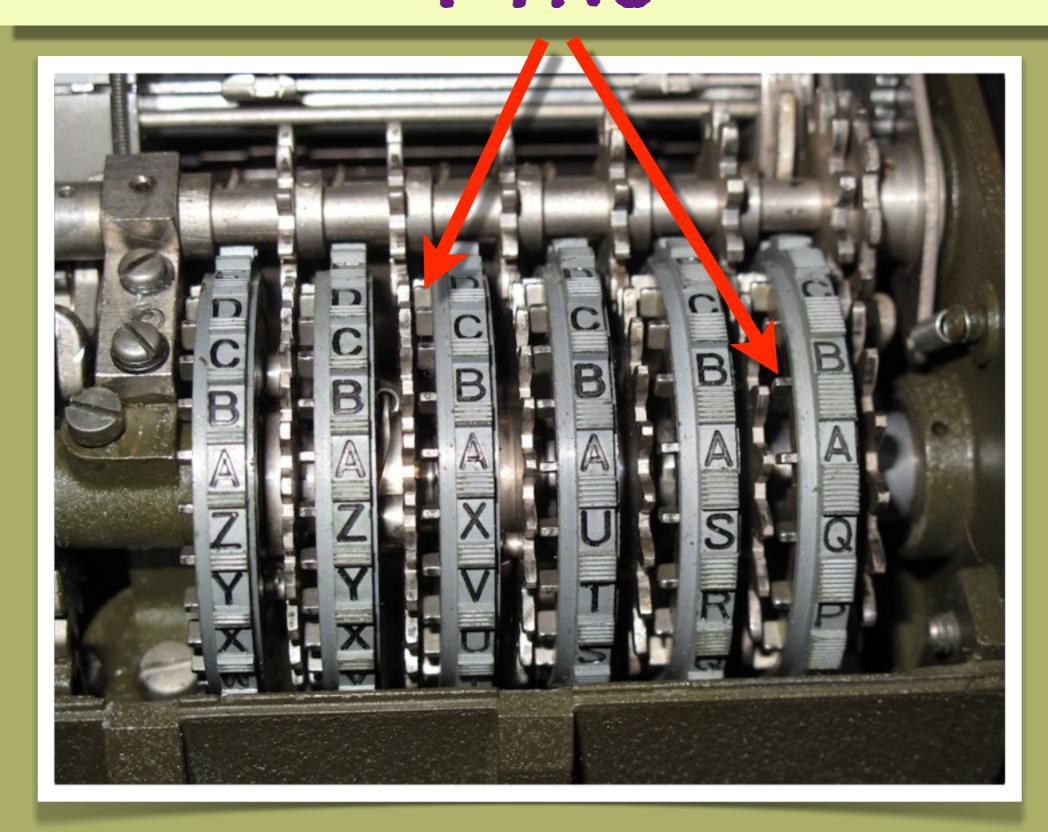
 Internal pin and lug settings (changed daily on pre-arranged schedule)

 External key wheel settings (selected randomly for each message)

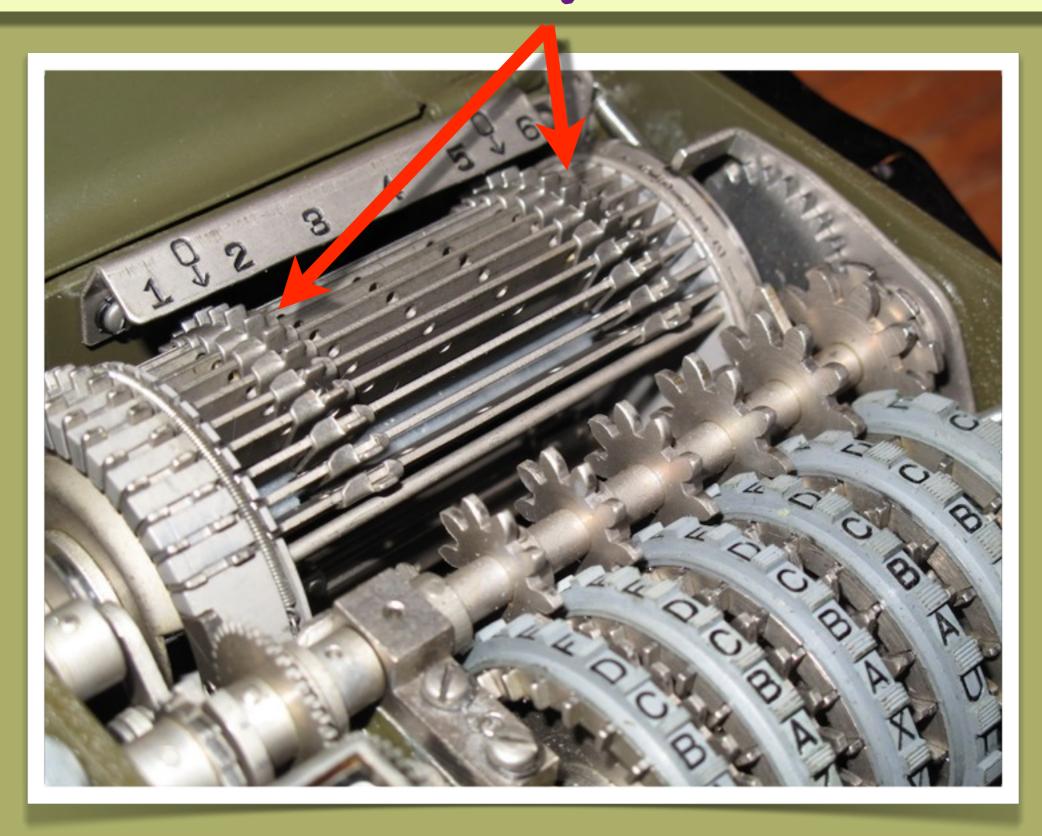
PINS AND LUGS



PINS



LUGS



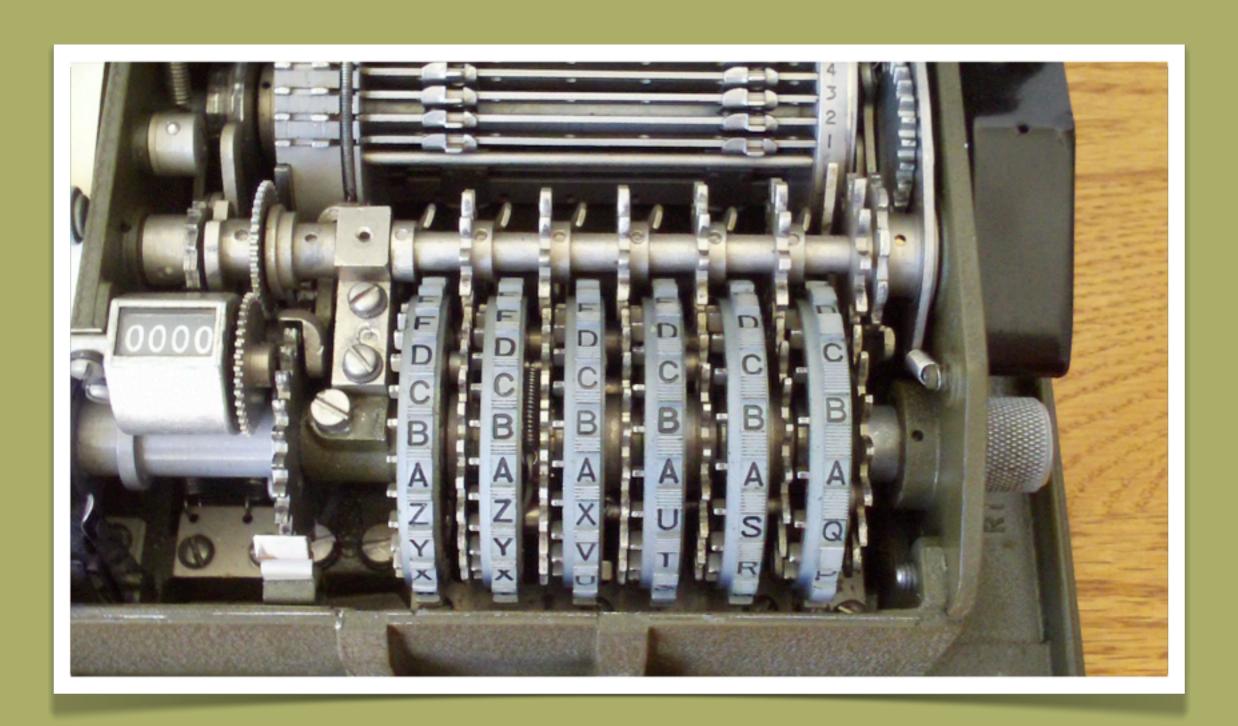
KEY LIST

| M-209 KE | Y L | IST | : B | R | | | |
|----------|-----|-----|-------|-------|----------|---|--|
| NR LUGS | 1 | 2 | 3 | 4 | 5 | 6 | |
| 01 0-1 | | | А | А | | | |
| 02 0-1 | | В | | | _ | _ | |
| 03 0-1 | C | C | C | - | - | _ | |
| 04 0-1 | D | _ | D | D | _ | _ | |
| 05 0-1 | _ | _ | _ | _ | _ | E | |
| 06 0-2 | F | F | _ | _ | F | F | |
| 07 0-2 | - | - | - | - | G | G | |
| 08 0-2 | H | Η | - | Η | Η | _ | |
| 09 0-2 | _ | _ | _ | I | I | _ | |
| 10 0-2 | J | J | J | _ | J | _ | |
| 11 0-2 | K | _ | K | K | - | _ | |
| 12 0-2 | L | _ | _ | _ | L | L | |
| 13 0-3 | M | M | M | _ | _ | M | |
| 14 0-3 | - | - | N | N | - | N | |

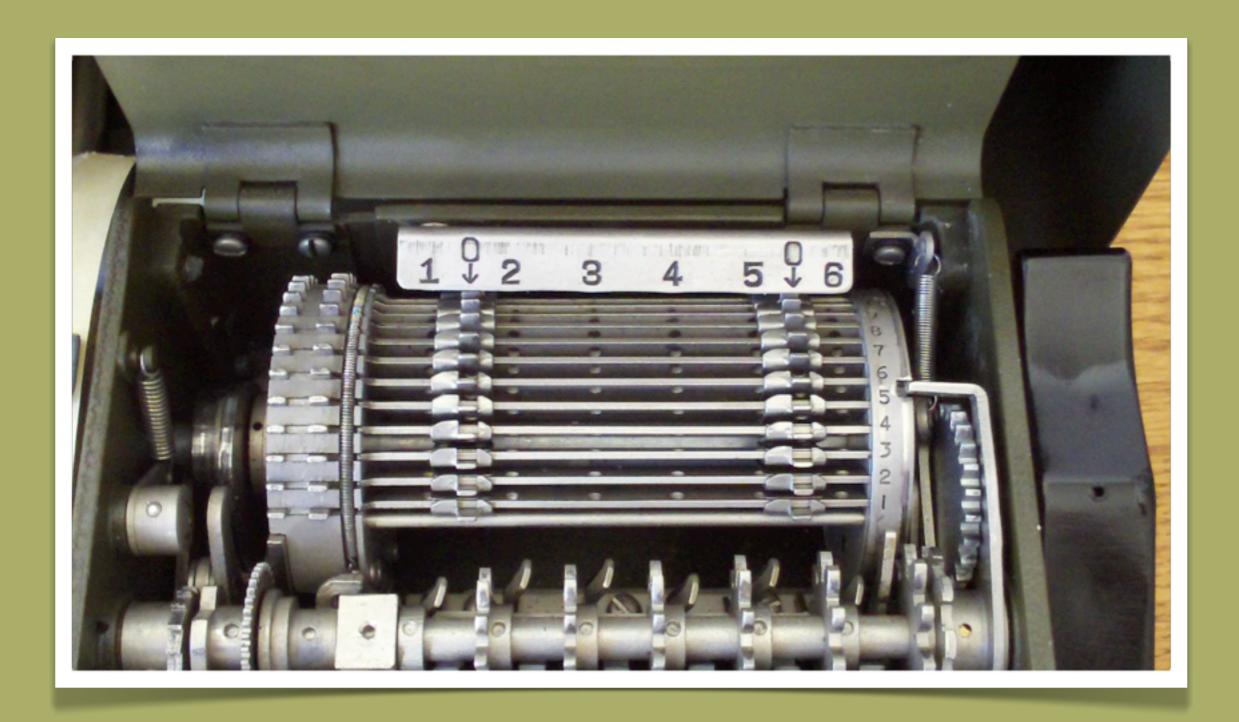
```
15 0-4 0 0 - - 0
16 0-4 - - P P P
17 0-4 - - - Q Q
18 0-4 - R - - -
19 0-4 S - S S S
20 0-4 - - -
21 0-4 - U - -
22 0-4 V V V
23 \ 0-4 - X X
24 0-5 X -
25 0-6 Y -
26 1-3 Z
27 3-5
26 LETTER CHECK
```

LJEWC FWIPR RAZRH BXKNO QGSRK P

SETTING PINS



SETTING LUGS



26 LETTER CHECK

- Easy to make mistakes while setting pins and lugs!
- Key list includes 26 letter test sequence:
 - Set all six key wheels to 'A'
 - Cipher letter 'A' 26 times
 - Compare results to key list

26 LETTER CHECK

LJEWC FWIPR RAZRH BXKNO QGSRK P

- Six key wheels must be set randomly for each ciphered message
- Never use same settings for more than one message!
- Each wheel has different number of positions: 26, 25, 23, 21, 19, 17
- Each wheel advances one position for each ciphered/deciphered letter

- How to securely send each message's key wheel settings to receiving operator?
- Many methods:
 - Include in message in the clear
 - Use pre-arranged schedule
 - Encipher into the message

 Set wheels to random positions: "External Message Indicator"



Select a random letter, then cipher it 12 times







 Select first six valid key wheel settings to get "Internal Message Indicator"

 Use the resulting key wheel settings to cipher the message



- Ciphertext will include information to let receiving operator recover the key:
 - External Message Indicator (six random letters)
 - Random letter used to generate Internal Message Indicator
 - Key List Indicator (two-letter code which identifies the key list)

| TIME FILED 1300 | msg cen no. 383 | HOW SENT RADIO |
|-----------------------------------|--|---|
| NF6X V KE6 | | PRIORITY |
| N | MESSAGE (SUBMIT TO MESSAGE CENTER IN DUPLICATE | CLASSIFICATION) |
| No. 42 | DATE | 1 MAY 2009 |
| TO MRCG PR | RESENTATION | |
| | | |
| OOZHS D | NABR REKGT MIHE | Z KRKMR |
| ANMVL G | NMYA DPXRL BFCE | RQ XQJGL |
| OVRIX Z | VHUJ AMSPN SXDE | KN GZCCN |
| FRKGM D | WBHO AXNNN EBZ | ZV FHKMT |
| YTNDQ N | AZRJF WORGH BRO | ZQ BFNHB |
| HOSZH A | VSKX DNQTQ NSY | QS AGQFW |
| OOZHS D | NABR | |
| | | |
| OFFIC | CIAL DESIGNATION OF SENDER | 1243 TIME SIGNED |
| AUTHORIZED TO BE SENT IN CLEAR | SIGNATURE OF OFFICER SI | Mark J Blair GNATURE AND GRADE OF WRITER |

| | THESE SPACES FOR MESSAGE | E CENTER ONL | . Y | |
|-----------------------------------|--------------------------------|---------------------|----------------------|-----------------------|
| TIME FILED 130 | MSG CEN NO. | 83 | HOW SENT | RADIO |
| NF6X V K | E6MYK | | PRIC | RITY |
| | MESSAGE (SUBMIT TO I | MESSAGE PLICATE) | (CLASSIF | ICATION) |
| No. 42 | DATE | 1 / | 1AY 20 | 009 |
| TO MRCG | PRESENTATION | | | |
| | | | | 0 |
| OOZHS | DNABR REKGT N | NIHBZ | KRKMF | 2 |
| ANMVL | QNMYA DPXRL | BFCBQ | XQJG | L |
| OVRIX | ZVHUJ AMSPN S | SXDKN | GZCC | N |
| FRKGM | DWBHO AXNNN | EBZZV | FHKM | Т |
| YTNDQ | MZRJF WORGH | BROZQ | BFNH | B |
| HOSZH | AVSKX DNQTQ | NSYQS | AGQF | W |
| OOZHS | DNABR | | | |
| | | | | |
| | OFFICIAL DESIGNATION OF SENDER | | | 1243 TIME SIGNED |
| AUTHORIZED TO BE SENT IN CLEAR | SIGNATURE OF OFFICER | SIGNATU | Mark 9 RE AND GRA | Blair DE OF WRITER |

| ME FILED 1300 | мѕ | G CEN NO. | 383 | HOW SENT | RADIO |
|------------------|----------------|--------------|-----------------------|---------------|---------------------|
| NF6X V KE | 6MYK | | | PRIO | RITY |
| | MESSAGE | (SUBMIT TO | MESSAGE OUPLICATE) | (CLASSIFIC | CATION) |
| o. 42 | | DAT | E 1 N | MAY 20 | 09 |
| MRCG P | RESENTA | TION | | | |
| | | | | | |
| OOZHS 1 | DNABR | REKGT | MIHBZ | KRKMR | <u> </u> |
| ANMVL | QNMYA | DPXRL | BFCBQ | XQJGL | |
| OVRIX 2 | ZVHUJ / | AMSPN | SXDKN | GZCCN | L |
| FRKGM 1 | OMBHO | AXNNN | EBZZV | FHKM | |
| YTNDQ | MZRJF | WORGH | BROZQ | BFNH | В |
| HOSZH / | AVSKX 1 | DNQTQ | NSYQS | AGQFV | V |
| OOZHS 1 | DNABR | | | | |
| | | | | | |
| OFF | ICIAL DESIGNAT | ION OF SENDE | R | | 1243 TIME SIGNED |
| AUTHORIZED TO BE | | | | Mark 9 | Plain |

| ME FILED 1300 | MSG CEN NO. | 383 | HOW SENT | RADIO |
|---------------|-----------------------|----------------------|-----------|-----------------------|
| NF6X V KE6M | YK | | PRIO | RITY |
| ME | SSAGE (SUBMIT TO | MESSAGE (PLICATE) | (CLASSIFI | CATION) |
| . 42 | DATE | 1/ | MAY 20 | 09 |
| MRCG PRE | SENTATION | | | |
| | | | | |
| OOZHS DN | ABR REKGT I | MIHBZ | KRKMR | |
| MVL QN | MYA DPXRL | BFCBQ | XQJGL | |
| VRIX ZV | HUJ AMSPN | SXDKN | GZCCN | |
| DW. | BHO AXNNN | EBZZV | FHKM' | Т |
| MZ | RJF WORGH | BROZQ | BFNH | В |
| AV | SKX DNQTQ | NSYQS | AGQFV | N |
| DN | ABR | | | |
| Q | | | | |
| R | DESIGNATION OF SENDER | | | 1243 TIME SIGNED |
| | NATURE OF OFFICER | SIGNATI | Mark 9 | Blair DE OF WRITER |

| | THESE SPACES FOR MESSAGE CE | NTER ONLY |
|-----------------------------------|--------------------------------|---|
| TIME FILED 1300 | MSG CEN NO. 383 | HOW SENT RADIO |
| NF6X V K | E6MYK | PRIORITY |
| | MESSAGE (SUBMIT TO MESS | ATE) (CLASSIFICATION) |
| No. 42 | DATE | 1 MAY 2009 |
| TO MRCG | PRESENTATION | |
| 10 | | |
| OOZHS | DNABR REKGT MIH | BZ KRKMR |
| ANMVL | QNMYA DPXRL BF | CBQ XQJGL |
| OVRIX | ZVHUJ AMSPN SXI | DKN GZCCN |
| FRKGM | DWBHO AXNNN EB | ZZV FHKMT |
| YTNDQ | MZRJF WORGH BR | ROZQ BFNHB |
| HOSZH | AVSKX DNQTQ NS | YQS AGQFW |
| OOZHS | DNABR | |
| | | |
| | OFFICIAL DESIGNATION OF SENDER | 1243 TIME SIGNED |
| AUTHORIZED TO BE SENT IN CLEAR | SIGNATURE OF OFFICER | Mark 9 Blair SIGNATURE AND GRADE OF WRITER |

| The second secon | FOR MESSAGE CENTER ONLY |
|--|--|
| TIME FILED 1300 MSG | CEN NO. 383 HOW SENT RADIO |
| NF6X V KE6MYK | PRIORITY |
| MESSAGE : | (SUBMIT TO MESSAGE (CLASSIFICATION) CENTER IN DUPLICATE) |
| No. 42 | 1 MAY 2009 |
| TO MRCG PRESENTAT | TION |
| | |
| OOZHS DNABR R | EKGT MIHBZ KRKMR |
| ANMY QNMYA I | PXRL BFCBQ XQJGL |
| OVRI ZVHUJ A | MSPN SXDKN GZCCN |
| FRK M DWBHO A | XNNN EBZZV FHKMT |
| Y7.VDQ MZRJF W | ORGH BROZQ BFNHB |
| | NQTQ NSYQS AGQFW |
| TE OB | |
| S D N A | |
| R C M Q | N OF SENDER TIME SIGNED |
| Q B L | FFICER SIGNATURE AND GRADE OF WRITER |

| IME FILED 1300 | MSG CEN NO. | 883 | HOW SENT | RADIO |
|---------------------------------------|-----------------------|---------------------|------------|-----------------------|
| NF6X V KE6M | YK | | PRIO | RITY |
| ME | SSAGE (SUBMIT TO | MESSAGE PLICATE) | (CLASSIFIC | CATION) |
| lo. 42 | DATE | 1 1 | 1AY 20 | 09 |
| MRCG PRE | SENTATION | | | |
| | | | | |
| OOZHS DN | ABR REKGT N | NIHBZ | KRKMR | |
| ANMVL QN | MYA DPXRL | BFCBQ | XQJGL | |
| OVRIX ZV | HUJ AMSPN | SXDKN | GZCCN | <u> </u> |
| FRKGM DW | BHO AXNNN | EBZZV | FHKM | Г |
| YTNDQ MZ | RJF WORGH | BROZQ | BFNH | В |
| HOSZH AV | SKX DNQTQ | NSYQS | AGQFV | V |
| OOZHS DN | ABR | | | |
| | | | | |
| OFFICIAL | DESIGNATION OF SENDER | | | 1243 TIME SIGNED |
| AUTHORIZED TO BE SENT IN CLEAR SIG | NATURE OF OFFICER | | Mark 9 | Blair DE OF WRITER |

| THESE SPACES FOR MESSAGE CENTER | ONLY — |
|---|---|
| TIME FILED 1300 MSG CEN NO. 383 | HOW SENT RADIO |
| NF6X V KE6MYK | PRIORITY |
| MESSAGE (SUBMIT TO MESSAGE CENTER IN DUPLICATE) | (CLASSIFICATION) |
| No. 42 DATE 1 | MAY 2009 |
| TO MRCG PRESENTATION | |
| | |
| OOZHS DNABR REKGT MIHBZ | KRKMR |
| ANMVL QUAYA DPXRL BFCBC | XQJGL |
| OVRIX _VHUJ AMSPN SXDKN | N GZCCN |
| FRKG DWBHO AXNNN EBZZ | V FHKMT |
| YTHIOQ MZRJF WORGH BROZ | Q BFNHB |
| DOCTH AVERY DNQTQ NSYQ | S AGQFW |
| M-209 KEY LIST: BR | |
| NR LUGS 1 2 3 4 5 6 | 1243 |
| 01 0-1 - A A | TIME SIGNED |
| 02 0-1 B B - B OF OFFICER SIGN | Mark J Blair ATURE AND GRADE OF WRITER |

| ME FILED 1300 | мѕо | CEN NO. | 383 | HOW SENT | RADIO |
|---------------|--------------------|---------------------------|----------------------|---------------|---------------------|
| NF6X V KE | 6MYK | | | PRIO | RITY |
| | MESSAGE | (SUBMIT TO CENTER IN D | MESSAGE UPLICATE) | (CLASSIFIC | CATION) |
| o. 42 | | DATE | 1 1 | MAY 20 | 09 |
| MRCG P | RESENTA | TION | | | |
| | | | | | |
| OOZHS | DNABR F | REKGT | MIHBZ | KRKMR | |
| ANMVL | QNMYA | DPXRL | BFCBQ | XQJGL | |
| OVRIX | ZVHUJ A | MSPN | SXDKN | GZCCN | <u></u> |
| FRKGM | DWBHO I | NNNXA | EBZZV | FHKM | Γ |
| YTNDQ | MZRJF \ | VORGH | BROZQ | BFNH | В |
| HOSZH | AVSKX D | NQTQ | NSYQS | AGQFV | V |
| OOZHS | DNABR | | | | |
| | | | | | |
| OF | FICIAL DESIGNATION | ON OF SENDE | R | | 1243 TIME SIGNED |
| 330 | | | 1/ | Mark 9 | - |

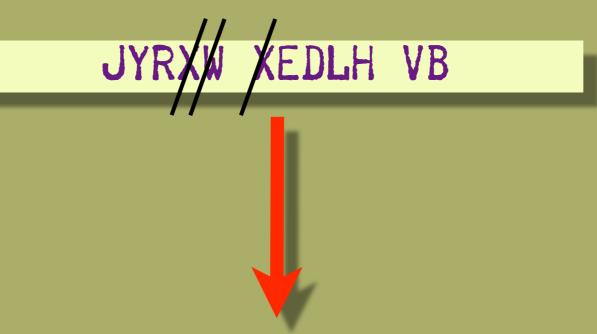
8 4

| TIME FILED | 1300 | 1 | MSG CEN NO. | 202 | HOW SENT | RADIO |
|-----------------------|------------------|---------------|----------------|-------------------------|----------|------------------------|
| NF6 | X V K | E6MYK | | | PRIC | ORITY |
| | | MESSAC | GE CENTER IN | O MESSAGE DUPLICATE) | (CLASSIF | FICATION) |
| No | 42 | | DA | те 1 | MAY 2 | 009 |
| то | MRCG | PRESEN' | TATION | 141.83 | | |
| 1000000 | | | | | | |
| 0 | OZHS | DNABR | REKGT | MIHBZ | KRKMI | R |
| A | NMVL | QNMYA | DPXRL | BFCBQ | XQJG | L |
| 0 | VRIX | ZVHUJ | AMSPN | SXDKN | GZCC | N |
| FI | RKGM | DWBHC | AXNN | EBZZV | FHKN | NT |
| Y | TNDQ | MZRJF | WORGH | BROZ | Q BFNI | I B |
| H | OSZH | AVSKX | DNQTQ | NSYQS | AGQF | W |
| 0 | OZHS | DNABR | | | | |
| | | | | | | |
| | 0 | FFICIAL DESIG | NATION OF SEND | ER | | 1243 TIME SIGNED |
| AUTHORIZED SENT IN |) TO BE CLEAR | SIGNATURE | OF OFFICER | SIGNA | Mark (| Blair ADE OF WRITER |

| TIME FILED 1300 | MSG CEN NO. 383 | HOW SENT RADIO |
|---|---|---|
| NF6X V KE6MY | K | PRIORITY |
| MES | SAGE (SUBMIT TO MESSAGE CENTER IN DUPLICATE | CLASSIFICATION) |
| No. 42 | DATE | 1 MAY 2009 |
| TO MRCG PRES | ENTATION | |
| | | |
| OOZHS DNA | BR REKGT MIHB | Z KRKMR |
| ANMVL QNN | YA DPXRL BFCE | Q XQJGL |
| OVRIX ZVH | UJ AMSPN SXDI | KN GZCCN |
| FRKGM DWB | HO AXNNN EBZ | ZV FHKMT |
| YTNDQ MZR | JF WORGH BRO | ZQ BFNHB |
| HOSZH AVSI | X DNQTQ NSY | QS AGQFW |
| OOZHS DNA | BR | |
| | | |
| OFFICIAL D | ESIGNATION OF SENDER | 1243 TIME SIGNED |
| AUTHORIZED TO BE SENT IN CLEAR SIGNA | TURE OF OFFICER SIG | Mark J Blair GNATURE AND GRADE OF WRITER |

| IME FILED 1300 | MSG CEN NO. | 383 | HOW SENT | RADIO |
|------------------|--------------------------|---------------------|------------|---------------------|
| NF6X V KE6 | MYK | | PRIO | RITY |
| М | ESSAGE (SUBMIT TO | MESSAGE PLICATE) | (CLASSIFIC | CATION) |
| lo. 42 | DATE | 1 / | 1AY 20 | 09 |
| MRCG PR | ESENTATION | | | |
| | | | | |
| OOZHS DI | NABR REKGT N | NIHBZ | KRKMR | |
| ANMVL Q | NMYA DPXRL | BFCBQ | XQJGL | |
| OVRIX Z | HUJ AMSPN | SXDKN | GZCCN | |
| FRKGM DV | VBHO AXNNN | EBZZV | FHKM' | Γ |
| YTNDQ M | ZRJF WORGH | BROZQ | BFNH | В |
| HOSZH AV | SKX DNQTQ | NSYQS | AGQFV | V |
| OOZHS DI | NABR | | | |
| | | | | |
| OFFICI | AL DESIGNATION OF SENDER | | | 1243 TIME SIGNED |
| AUTHORIZED TO BE | | | Mark 9 | Blair |

| IME FILED 1300 | MSG CEN NO. | 383 | HOW SENT | RADIO |
|-----------------------------------|-------------------------|-------------------------|-----------|---------------------|
| NF6X V KE6 | | | PRIO | RITY |
| N | IESSAGE (SUBMIT T | O MESSAGE DUPLICATE) | (CLASSIFI | CATION) |
| o. 42 | DA1 | re 1 M | MAY 20 | 09 |
| MRCG PR | ESENTATION | | | |
| | | | | |
| OOZHS D | NABR REKGT | MIHBZ | KRKMR | |
| ANMVL Q | NMYA DPXRL | BFCBQ | XQJGL | |
| OVRIX Z | VHUJ AMSPN | SXDKN | GZCCN | <u> </u> |
| FRKGM D | WBHO AXNNN | EBZZV | FHKM' | Γ |
| YTNDQ N | ZRJF WORGH | BROZQ | BFNH | В |
| HOSZH A | VSKX DNQTQ | NSYQS | AGQF\ | V |
| OOZHS D | NABR | | | |
| | | | | |
| OFFIC | IAL DESIGNATION OF SEND | ER | | 1243 TIME SIGNED |
| AUTHORIZED TO BE SENT IN CLEAR | | | Mark 9 | Blair |





| IME FILED 1300 | MSG CEN NO. | 383 | HOW SENT | RADIO |
|-------------------------------------|--------------------------|----------------------------|-----------|---------------------|
| NF6X V KE6 | | | PRIO | RITY |
| M | ESSAGE (SUBMIT CENTER II | TO MESSAGE N DUPLICATE) | (CLASSIFI | CATION) |
| lo. 42 | DA | TE 1 | MAY 20 | 09 |
| MRCG PR | ESENTATION | | | |
| | | | | |
| OOZHS D | NABR REKGT | MIHBZ | KRKMR | |
| ANMVL Q | NMYA DPXRI | BFCBQ | XQJGL | |
| OVRIX Z | VHUJ AMSPN | SXDKN | GZCCN | I |
| FRKGM D | WBHO AXNNI | N EBZZV | FHKM' | Т |
| YTNDQ M | ZRJF WORG | H BROZG | BFNH | В |
| HOSZH A | SKX DNQTQ | NSYQS | AGQF\ | N |
| OOZHS D | NABR | | | |
| | | | | |
| OFFIC | AL DESIGNATION OF SEN | DER | | 1243 TIME SIGNED |
| AUTHORIZED TO BE SENT IN CLEAR S | | | Mark g | Blair |

| E FILED | MSG CEN NO. | HOW SENT |
|------------------|------------------------------|-----------------------|
| | MESSAGE (SUBMIT TO MES | SAGE (CLASSIFICATION) |
| | DATE | |
| | | |
| WELCOME | TO THE TWO TH | OUSAND |
| NINE WE | ST COAST MILITA | RY RADIO |
| COLLECTO | RS GROUP MEETIN | NG |
| PLEASE M | EET ME FOR DINN | IER TONIGHT |
| AT JOCKO | S STEAK HOUSE | |
| | | |
| | | |
| | | |
| OF | FICIAL DESIGNATION OF SENDER | TIME SIGNED |
| AUTHORIZED TO BE | | - 2 |

REFERENCES

- Cryptanalysis of the Hagelin Cryptograph
 ©1977 Wayne G. Barker
 Aegean Park Press
- History of the Hagelin Cipher Machines
 Dirk Rijmenants
 http://users.telenet.be/d.rijmenants/en/hagelin.htm
- http://en.wikipedia.org/wiki/Boris_Hagelin
- TM 11-380, 17 March 1944