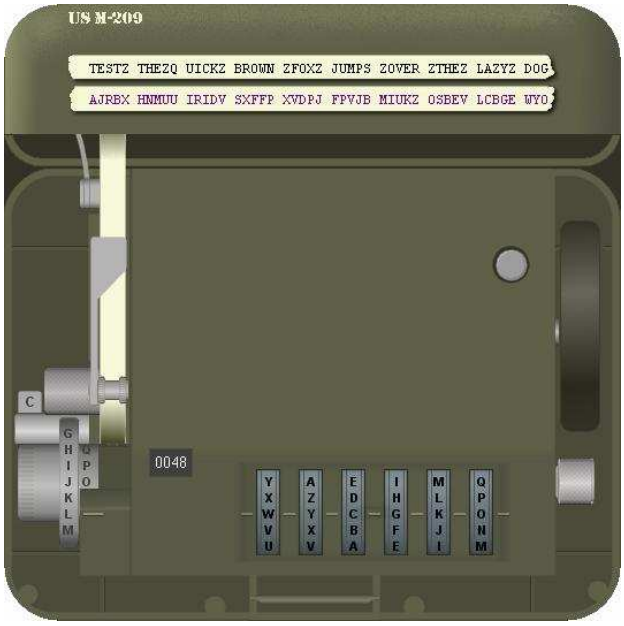
M-209 SIMULATOR 3.0 MANUAL

About the M-209 Sim



This program is an exact simulation of the M-209 Cipher Machine, used by the US Army during and after the Second World War. The M-209, an American licensed version of the Hagelin C-38, was a portable hand operated cipher machine for tactical messages. It had the size of a lunchbox and presented a brilliant mechanical design, developed by the Swedish cryptographer Boris Hagelin.

This simulator, fully compatible with the original cipher machine, has a realistic look and feel, with rotating wheels, setting of wheel pins and drum lugs, combined with authentic graphics.

In this help file, we will explain how the simulator works, how the M-209 was actually used by the US military, with the complete enciphering procedures, and give you the technical details of the machine.

Special thanks to Tom Perera from the Enigma Museum and David Hamer for the pictures in the gallery and the advice and help.

Copyright Information

dr.defcom@telenet.be
http://users.telenet.be/d.rijmenants

Disclaimer of Warranties

How to use the simulator

To prepare the M-290 for use, you need to set the wheel pins, the lugs on the drum and the message indicators. As you will notice, there's always a little hand visible when you move the mouse to places where you can select or click something. With the F1 key you can call the help file.

The Menu

The main menu of the simulator appears when the mouse is moved over the US M-209 label in the top left corner of the machine.

Setting the pins

Click on the bottom of the M-209 to open the cover and reveal the mechanism. Click on the upper or lower half of one of the six wheels to place it in the desired position. To set the A-pin on the first wheel in the active position, you turn that wheel until the letter A is aligned with the pins. Next, you click on the pin to change its position. Note that the pin is in its active position when it is located on the right side of the wheel.

The best way to set the machine is to first clear all previous pin and lug settings by using the **Zeroise** option in the main menu or by pressing **F12**. The setting of the pins can be done in two ways: you can set all the pins of one wheel, and than continue with the next wheel, or a more practical method is starting with all wheel on A-position (you can reset the wheels by pressing **Backspace**) and set all the A pins of all wheels, according to the key sheet. Next, you advance all wheels to the B-position, by clicking the lower half of the knob on the right, and continue with setting all the B pins.

Setting the lugs

The drum has 27 bars, each holding two sliding lugs. Each lug can be set in one of the six numbered positions, or one of the two neutral zero-positions. Turn the drum by clicking the upper or lower half on its right until the desired bar appears. Next, you click on one of the lugs, and click on a free position on the bar. The lug will move to the new position. Continue until all lugs on all bars are set in the proper position, as shown in the key sheet.

Setting the External Message Indicator

On the main screen you can change the External Message Indicator, that's the start position of the wheels, by clicking the upper or lower half of the wheels. The External Message Indicator can be saved temporarily by pressing **INS**, and can be retrieved later by pressing **HOME**. Instead of using the Home key, you can also turn back the wheels until the counter reaches zero. To advance or turn back all wheels you can click the upper or lower half of the wheel knob on the right of the machine.

Ciphering and Deciphering

Before starting, you must turn the **Cipher/Decipher switch** on the left of the machine to the desired position by clicking it. In Cipher mode, the output is printed in groups of five letters. Use the letter **Z** in the plain text to replace spaces between words. In Decipher mode, the output is printed continuously. If the deciphered plaintext letter is Z, a space is printed.

When all settings are finished you can start enciphering or deciphering your messages. To select the character you want to encipher or decipher, turn the **Indicator wheel** on the left of the machine by clicking the upper or lower half, until the desired character is aligned with the datum line.

You can also turn the Indicator by pressing the + or – key on the Num Pad. Next, turn (click) the power handle on the right of the machine, to cipher or decipher. You can also use the **ENTER** key to turn this handle. To speed up the process, you can also type the characters on the keyboard. In Cipher mode, you can use the spacebar of your keyboard, which will be replaced automatically by the letter Z, representing a space. If the operator ran out of paper ribbon, he was able to read which letter normally was printed by looking on the right side alphabet of the indicator.

Important note: When you use the indicator by hand to select the next letter, there is an important issue: Once a letter is encoded, the handle is locked to prevent a second turn. To release it, you must unlock it by turning the indicator. This means that when you encipher twice the same letter, you MUST turn the indicator and return to the letter. However, this is not necessary if you use the keyboard on your computer to enter the letters.

Reset the counter and text display

Click on the **round button** on the cover or press the **Backspace** key to reset the counter to zero and wheels to A position. Use the **Delete** key to clear the two text ribbons on top of the machine, without changing the current wheel positions and counter. If you didn't saved the start position on the beginning of a message, you can use the wheel knob on the right to turn back the wheels step by step, until the counter reaches zero.

The clipboard function

With the Clipboard function you can select in various ways how to format and transfer your plain or cipher text to the clipboard. Select the **Clipboard** in the main Menu or with **F5**.

Using the Auto Typing option

If you have a large amount of plain text or cipher text that needs to be typed, you can use the Auto Typing Window. Select **Auto Typing** in the main Menu or select **F6**. In this window you can type, edit or paste pieces of text, or retrieve the content of the clipboard. You can select three different speeds of typing. Select **Start** to begin processing the text. During the Auto Typing you can abort by pressing **ESC**. Make sure that all machine settings are completed and the external message indicator is in the correct position before starting the Auto Typing.

Auto Typing will only process alphabet characters and will ignore all other characters like numbers and signs. However, in Cipher mode, spaces will be replaced automatically by the letter Z, representing a space.

Exiting the simulator

You can exit the simulator in the main Menu. If you have changed the settings of the machine, you will be prompted to save these changes.

Image Gallery

Select the Gallery in the main Menu to view some images of a real M-209.

Screen settings and correcting graphics distortions

The program is designed to work with default 96 Dpi (100%) screen settings. If you use another screen setting, graphics might be distorted and text and graphics may not be aligned. Press F10 to adjust the alignment of text and graphics.

Shortcut keys overview

A-Z Set indicator (Space = Z in Cipher mode)
+ / - Change indicator by one position
ENTER Turn handle

INS Memorize current wheel setting
HOME Retrieve memorized wheel setting, and reset counter

DEL Delete text ribbons, without resetting the wheels or counter
BACKSPACE Reset all wheels to A position and reset counter

F5 Show Clipboard
F6 Show Autotype window
F10 Adjust text alignment with other screen settings
F12 Clear all current pin and lug settings

How the machine was used by the US Army

Setting the machine

To cipher and decipher a message correctly, sender and receiver need identical M-209 machine settings. To set up his machine, each operator had a key sheet. In general, these settings were changed every 24 hours. The operator's key sheet contained the lugs for the drum, the wheel pins, the 26 letter check to verify the settings, and the key list indicator to identify the key to the other operator. A letter represents an active pin, which must be set to the right side of the wheel. A dash means the pins is inactive, and it must be set to the left side of the wheel.

When all settings are completed, we use the 26 letter check to verify the settings. Set the machine in Cipher mode and turn all wheels in the A position. Next, encipher 26 A's, one after another. The result must match exactly the 26 letter check at the bottom of the key sheet.

Let us use the following example sheet, from the original M-209 TM 11-380 Manual, to set up the machine and send a sample message. On the left you see the usual key sheet and on the right another depiction of the same lug settings as on the key sheet, to visualize to lugs on the bars.

NR	LUGS	1	2	3	4	5	6
01	3-6	A	A	A	-	-	A
02	0-6	B	-	B	-	B	B
03	1-6	-	-	-	C	-	-
04	1-5	D	D	-	-	D	D
05	4-5	-	E	-	E	E	-
06	0-4	-	-	-	F	F	-
07	0-4	-	G	G	-	-	-
08	0-4	H	-	H	H	H	H
09	0-4	I	-	-	I	I	-
10	2-0	-	J	J	-	-	-
11	2-0	K	K	-	-	-	K
12	2-0	-	L	L	-	-	-
13	2-0	M	-	M	M	M	-
14	2-0	N	-	N	N	N	N
15	2-0	-	O	-	-	-	O
16	2-0	-	-	-	P	P	-
17	2-0	-	-	-	-	-	Q
18	2-0	-	R	R	-	-	
19	2-0	S	S	S	S	S	
20	2-5	T	-	T	T		
21	2-5	-	U	U	U		
22	0-5	V	-	-			
23	0-5	W	X	X			
24	0-5	-	-				
25	0-5	-	-				
26	0-5	-					
27	0-5						

BAR	1	2	3	4	5	6
01	-	-	X	-	-	X
02	-	-	-	-	-	X
03	X	-	-	-	-	X
04	X	-	-	-	X	-
05	-	-	-	X	X	-
06	-	-	-	X	-	-
07	-	-	-	X	-	-
08	-	-	-	X	-	-
09	-	-	-	X	-	-
10	-	X	-	-	-	-
11	-	X	-	-	-	-
12	-	X	-	-	-	-
13	-	X	-	-	-	-
14	-	X	-	-	-	-
15	-	X	-	-	-	-
16	-	X	-	-	-	-
17	-	X	-	-	-	-
18	-	X	-	-	-	-
19	-	X	-	-	-	-
20	-	X	-	-	X	-
21	-	X	-	-	X	-
22	-	-	-	-	X	-
23	-	-	-	-	X	-
24	-	-	-	-	X	-
25	-	-	-	-	X	-
26	-	-	-	-	X	-
27	-	-	-	-	X	-

TNJUW AUQTK CZKNU TOTBC WARMI O

KEY LIST INDICATOR: XA

About creating good keys

The pins settings on the wheels should be selected randomly, with preferably no more than three successive pins in the same state on a wheel. To create a good lug setting, we select 6 numbers between 1 and 14 whose sum is 27 and assign each of these numbers to one of the 6 lug positions. for example 7, 1, 3, 12, 1 and 2. Make sure that you are able to produce all values between 1 and 25 by combining one or more of these 6 values. Start with placing 7 lugs in position 1 at 7 executive bars. Proceed downwards with 1 lug on position 2 on the 8th bar, than on position 3 with 3 lugs on bars 9, 10 and 11 and so on. Working downwards, it is allowed to start the next series of lugs on the last bar of the previous series (one-lug overlap)

The External Message Indicator

Once the machine setup is completed, we can start enciphering a message. First, we reset the counter, on the simulator with the Backspace key, and set the Cipher-Decipher switch in Cipher position.

Next, we set six completely random letters on the six wheels. This is called the External Message Indicator. Write down these six letters for later use. For security reasons, it is important that we use a random Message Indicator only once with the machine setting that particular day. Each external Message Indicator must be unique!

Let use take DUFLJB as External Message Indicator

Next, we select a random letter, say K. Also write down this letter. We now encipher 12 times that letter K. The result is 12 random cipher letters. The operator would now remove the ribbon with these 12 letters and reset the counter to zero. On the sim, we first write down these 12, and reset wheels and counter with the Backspace key.

The result: PEQGB JGCDF UP

The Internal Message Indicator

These 12 letters are used to set the secret Internal Message Indicator. We start with the first letter, and set the extreme left-hand wheel in that position. We proceed trough the wheels from left to right. Since some letters are omitted on some wheels, it is possible that the given letter is not on the wheel. In that case, we strike-through that letter and take the next one. If these 12 letters are not enough to compose the Internal Message Indicator, due to many strike troughs, you must select another External Message Indicator and start all over. If all wheels are set, we are ready to encipher the message with this Internal Message Indicator.

Our Internal Message Indicator, obtained from the 12 letters: PEQGBJ

Enciphering the message

Now, we can encipher our message, with the Cipher/Decipher switch still in Cipher position. During enciphering, spaces between words should be replaced by the letter Z. When the receiver deciphers your message, each letter Z is replaced by a blank space. Separate letter are replaced by their phonetic words, C to CHARLIE, or E to EASY etc. Numbers are spelled, 1 as ONE, 2 as TWO etc.

The message:

OPERATION ZEBRA STARTS AT SUNSET

The cipher message:

KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HX

Once the message is enciphered completely, we have the cipher text printed in groups of five letters on the paper ribbon. If the last group has less than five letters, we complete it with letters X until a group of five is formed.

Our message: KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HXXXX

To complete the message, we need to add three indicators. The first indicator is called the System Indicator, telling the receiving operator that the message is enciphered with the M-209. This is the originally enciphered letter we wrote down, twice, that is KK. It is added before and after the message.

The second indicator is the randomly selected External Message Indicator we wrote down (<u>not</u> the secret Internal Message Indicator!). This is written just after the first System Indicator.

The third indicator is the Key List Indicator, telling the receiving operator which key sheet was used to encipher the message. The Key List Indicator is written down just after the External message Indicator and repeated at the end of the message. We now have the complete message, including indicators:

KK DUFLJB XA KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HXXXX KK

Finally, the message is rewritten in groups:

```
KKDUF LJBXA KBMUN ODDDC YWLVM RBVUS QYRHT XNZUI HXXXX KK
```

We now destroy the paper with the 12 letters and turn the wheels to a random position to break up the Internal Message Indicator.

Deciphering the message

To decipher the message, the receiving operator sets the Cipher-Decipher switch in the Cipher position (not the Decipher position!). Just like the sender did, he sets the six wheels according to the External Message indicator that was added to the message, enciphers 12 times the letter K that he found at the start and the end of the message, and thus retrieves the 12 letters to compose the Internal Message Indicator.

He resets the counter, sets the wheels according to the retrieved Internal Message Indicator, now turns the Cipher-Decipher switch to the Decipher position and deciphers the message. When deciphering, the deciphered letter Z is replaced by a space. On places where the missing Z in a word is obvious, we write down the letter Z, as in the word ZEBRA.

```
OPERATION  EBRA STARTS AT SUNSET
OPERATION ZEBRA STARTS AT SUNSET
```

You now have learned the complete procedure to send messages with the M-209 Cipher Machine!

The next message was enciphered with the same machine settings from the example key sheet. It's up to you to decipher this message. Good Luck!

```
SSCVQ IMKXA SISMR TRNLE POFCW
LWKUW AJWGL SUUAE NZANO TZARZ
VRBVN ZDKEB JGPUI WXXXX SS
```

Technical details of the M-209

The Wheels

Six key wheels each have a small movable pin aligned with each letter on the wheel. A pin may be positioned to the left or right. In the left position the pin is ineffective, while in the right position it is effective.

Each key wheel contains a different number of letters and pins. From left to right, the wheels have:

26 letters, from A to Z
25 letters, from A to Z, except W
23 letters, from A to X, except W
21 letters, from A to U
19 letters, from A to S
17 letters, from A to Q

Each key wheel is associated with a slanted metal guide arm that is activated by any pins in the "effective" position. From left to right, these pins are associated with the guide arm if all wheels are in the A position: P, O, N, M, L, K

The positions of the pins on each key wheel are the first part of the internal keying mechanism of the M-209.

The Drum

Behind the row of six key wheels is a cylindrical drum consisting of 27 horizontal bars. Each drum bar carries two movable lugs; the lugs can be aligned with any of the six key wheels, or may be placed in one of two neutral positions. An effective pin causes its guide arm to tilt forward, contacting the drum. The positioning of the lugs is the second part of the internal keying mechanism.

The ciphering process

When the power handle is turned, the cylindrical drum makes a complete revolution through all 27 bars. If a lug on one of the bars contacts the guide arm of an active key wheel, that bar is slid to the left. Lugs in neutral positions, or which do not contact a guide arm, do not affect the position of the bar. All bars that are slid to the left comprise a variable-toothed gear, which in turn shifts the letter to be encoded; the shift is equal to the number of bars protruding to the left. The resulting ciphertext letter is printed onto the paper tape. The M-209 uses a reciprocal substitution. The alphabet used in the plaintext message is mapped to the same alphabet in reverse:

ABCDEFGHIJKLMNOPQRSTUVWXYZ Plaintext alphabet:
ZYXWVUTSRQPONMLKJIHGFEDCBA Ciphertext alphabet:

If shifting is not considered, "A" becomes "Z", "B" becomes "Y", "C" becomes "X" and so on. Shifting proceeds in a reverse direction; for instance, a plaintext "P" maps to ciphertext "K"; shifting by three positions, to the left, gives ciphertext "N." The shift is circular, so when a shift steps off the left side, it continues again on the right. This approach is reciprocal, meaning that deciphering uses the same table in the same way: a ciphertext "N" is entered as if it were plaintext; this maps to "M" in the ciphertext alphabet, or "P" after shifting three positions, thus giving the original plaintext back.

At the end of the encipherment cycle, all six key wheels are advanced by one position. When started with positions AAAAAA, the key wheels will read BBBBBB after encoding one letter. Since all wheels have another number of letters, ranging from 17 to 26, this results in a co-prime nature. The wheels only align the same way once every 26×25×23×21×19×17 = 101,405,850 enciphered letters. Already after 17 cycles, the wheels advance from QQQQQ to RRRRA, and after 26 cycles, the wheels will read ABDFHJ.

Printing plain and ciphered text

To select between ciphering and deciphering, the Cipher-Decipher switch must be set in the proper position. In Cipher mode, the output is printed on the paper ribbon in groups of five letters. In Decipher mode, the output is printed with word spacing and the letter Z is replace by blank spaces (as mentioned in the user manual, in Cipher, you can replace spaces between words with the letter Z)

Interesting links on the M-209

The M-209 Sim Home Page
http://users.telenet.be/d.rijmenants

Tom Perera's Enigma Museum:
http://w1tp.com/enigma

Bob Lord's Pages on the M-209, Including an original 30-minute WW-II U.S. Army training film:
http://ilord.com/

Jerry Procs very complete Crypto Machines site:
http://www.jproc.ca/crypto/m209.html

David Hamer's Cryptology site
http://www.eclipse.net/~dhamer

Frode's simulator pages at CERN:
http://frode.home.cern.ch/frode/crypto/simula/

The M-209 on Wikipedia Encyclopedia
http://en.wikipedia.org/wiki/M-209