

Cipher Machine Instructions

Release Date: 16 Aug 2023

Table of Contents

Unbreakable Ciphers	1
Encryption Levels	1
Secure Communications	1
Creating a Cipher	1
Decrypting a Cipher	4
Color Schemes	5
Morse Code Feature	6
Appendix: International Morse Code	7

Unbreakable Ciphers

Each unit of Cipher Machine creates its own unique 8-digit serial number the first time it is executed. No two units of Cipher Machine will have the same serial number. Cipher Machine's 16-character encryption key is formed from the unit's unique serial number and an 8-character code key supplied by the user. The code key can include any of the 95 characters on a typical keyboard. The way in which the serial number and code key are combined to form the encryption key, and the algorithm that employs the encryption key to encrypt and decrypt text, are proprietary. These safeguards insure that a Cipher Machine cipher is virtually¹ unbreakable.

Encryption Levels

There are two optional encryption levels: "MORSE COMPATIBLE" and "MOST SECURE" (the default level). The user selects the desired level with the [Change to ...] button. The "MORSE COMPATIBLE" level uses a lexicon of 50 characters (including the space), as defined in the Appendix. Ciphers encrypted at this level can be transmitted audibly, as International Morse code, with the [Transmit MORSE] button. Any character in the original plain text that is not in the Morse Code lexicon is replaced by a space before encryption. Any lower-case letter in the original plain text is replaced by its upper-case equivalent before encryption.

The "MOST SECURE" encryption level uses a lexicon of 95 characters², including the space, upper-case and lower-case letters, punctuation marks, and special characters.

¹ The word "virtually" has been used in deference to the common notion that, in theory, no cipher is unbreakable.

Secure Communications

The owner of a Cipher Machine unit can provide copies of his *Cipher Machine Folder*³ to those with whom he wants to establish a secure communication network. These copies will have the same serial number, a requirement for successful encrypted communication.

Creating a Cipher

The Cipher Machine window is illustrated on the next page (with one of the available color schemes). An example plain-text message has been entered in the text box, a code key (Enigma-5) has been entered in the code-key box, and the "MOST SECURE" encryption level has been chosen.

To type text into the code-key box or text box, place the mouse cursor in the box and start typing. The keyboard accelerators CNTRL+C (copy), CNTRL+V (paste), CNTRL+X (cut), and CNTRL+Z (undo) can also be used to manipulate text in the boxes. Portions of text can be selected by holding down the mouse's left key and dragging the cursor across the text.

² Essentially all of the characters on the modern keyboard.

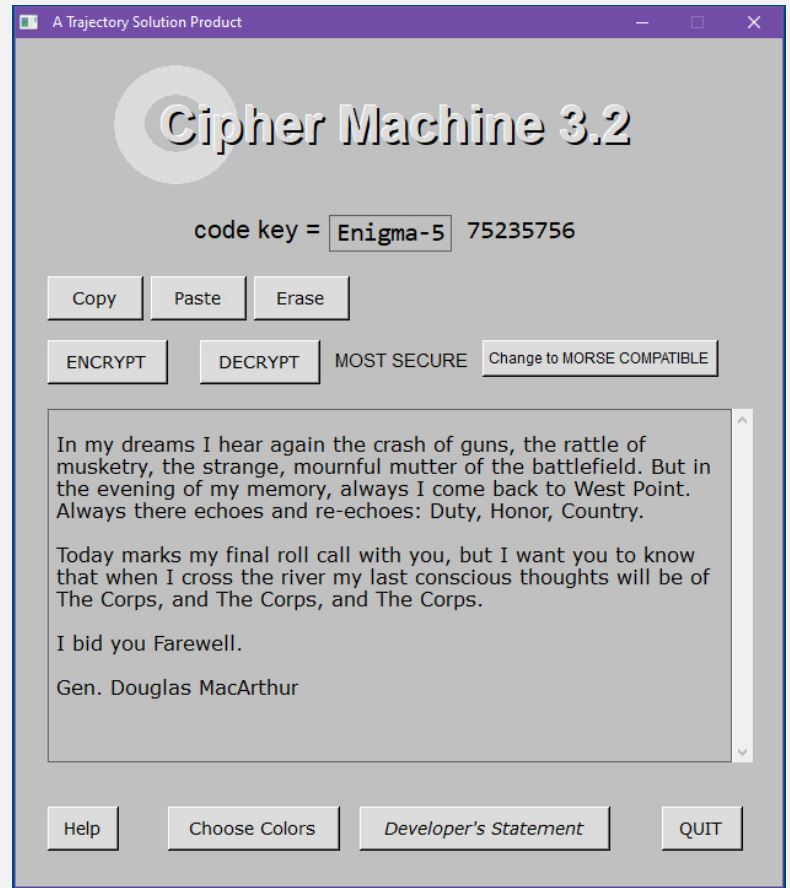
³ Before distributing copies of the *Cipher Machine Folder* to establish a network, the program must be executed to create the unique serial number, which is automatically encrypted and stored as file "encSN.txt" in the folder.

The [Copy] or [Erase] button is used to copy or erase *all of the text* in the text box without having to select it with the mouse cursor. When the [Copy] button is clicked, all text in the text box is copied into the keyboard buffer. When the [Erase] button is clicked, the text box is cleared.

The [Paste] button is used to paste whatever is in the keyboard buffer into the text box. The pasting starts at the top-left corner of the box and overwrites any text that may already be in the box. Therefore, the text box should be erased before clicking the [Paste] button.

The code key can be left blank or can consist of any number of characters up to a maximum of eight. In the example shown at the right, the user has typed in the code key "Enigma-5". The Cipher Machine unit's unique eight-digit serial number is displayed to the right of the code-key box. In this example, the plain text in the text box is not long enough to activate the scroll bar on the right side of the window. When a longer text exceeds the vertical dimension of the box, the scroll tab will appear in the scroll bar.

The maximum number of characters in the text should not exceed 30,000, and if a text with more than 30,000 characters is pasted into the text box, all except the first 30,000 characters will be deleted automatically and will not be displayed (it is prudent to limit the plain text to no more than 29,000 characters).



NOTE: When the [ENCRYPT] button is clicked, any carriage returns or spaces at the beginning or end of the plain text message will be automatically deleted before the plain text is encrypted.

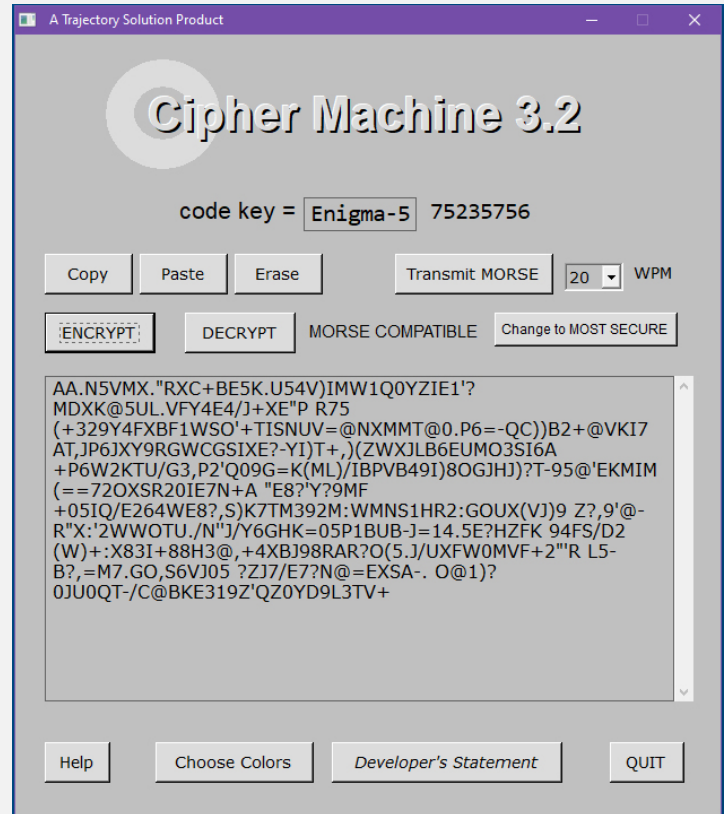
For the plain-text example on the previous page, a click of the [ENCRYPT] button will produce the cipher shown in the following window:



Had the "MORSE COMPATIBLE" encryption level been chosen instead of the "MOST SECURE" level, a click of the [ENCRYPT] button would have produced the cipher shown in the window at the right.

Cipher Machine's encryption and decryption algorithms operate on the entire text as a whole. If any part of a cipher is altered during transmission, the decryption operation will produce gibberish. It is

normally OK to transmit a cipher via email in an attached text document or to simply paste the cipher into the body of the email message.



A cipher can be created by an encryption *sequence* (clicking the [ENCRYPT] button a number of times in succession). If desired, a different code key can be used for each encryption in the sequence.

Decrypting a Cipher

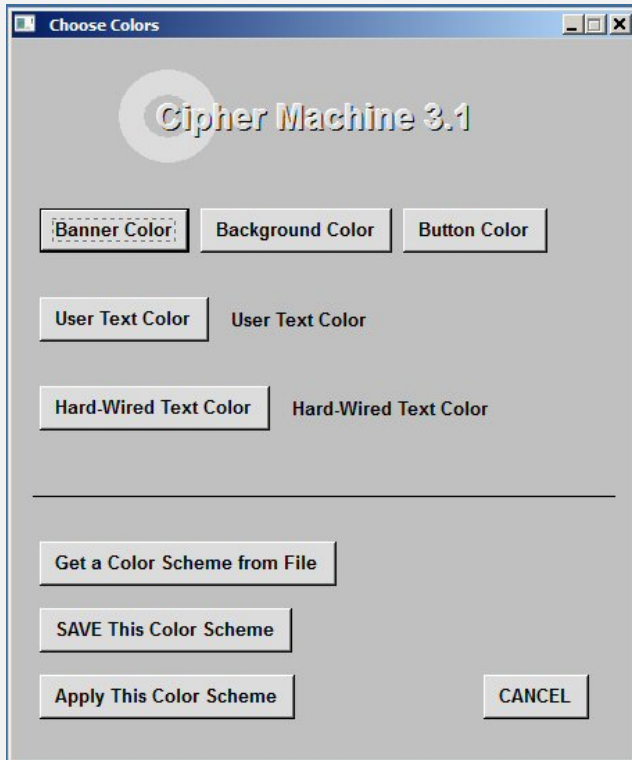
When the recipient receives the cipher, he can copy and paste it into his Cipher Machine's empty text box (if the box is not empty, he can clear it by clicking the [Erase] button). He must also type the proper code key into the code-key box and choose the correct encryption level. Then, when he clicks the [DECRYPT] button, the plain text will replace the cipher in the box (unless an encryption sequence was used to create the cipher).

A cipher that was created with an encryption sequence will be properly decrypted when the recipient clicks the [DECRYPT] button the proper number of times, using the correct code key. If the encryption sequence included a code-key sequence, the decryption code-key sequence must be the reverse of that used in the encryption sequence.

A Cipher Machine's cipher will never begin or end with a space or carriage return. If a beginning or ending space or carriage return is observed in the cipher, having perhaps been inserted by an intermediate word processor or email application, these must be removed before the cipher can be properly deciphered.

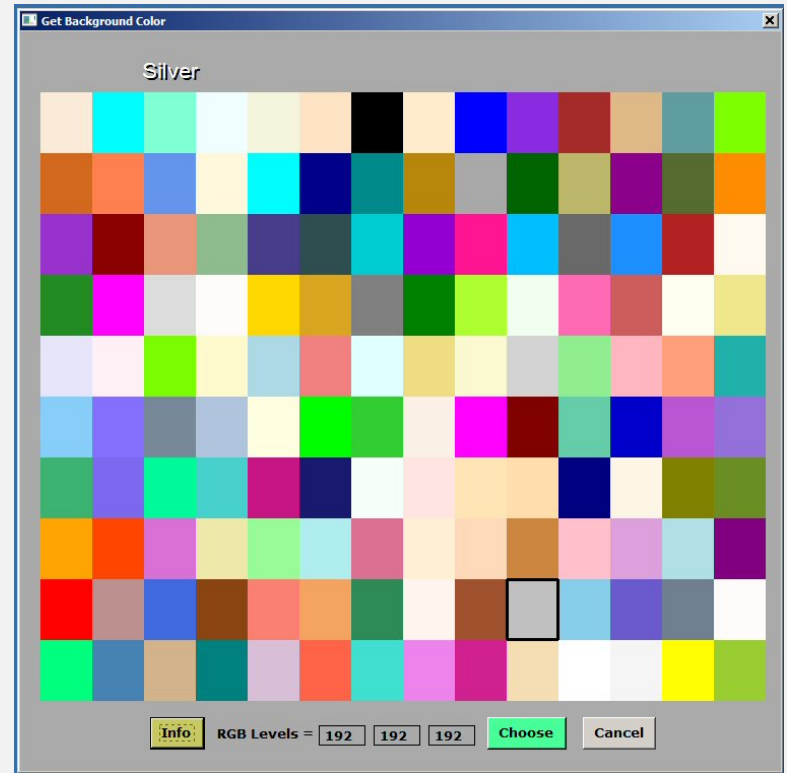
Color Schemes

The user can change the colors of the Cipher Machine Window's components by clicking the [Choose Colors] button to display the following window:



When the [Get a Color Scheme from File] button is clicked, a list of existing color schemes is displayed, from which the user can select. The user can name and save a color scheme he's developed by clicking the [SAVE This Color Scheme] button. When the [Apply This Color Scheme] button is clicked, the chosen colors will be applied.

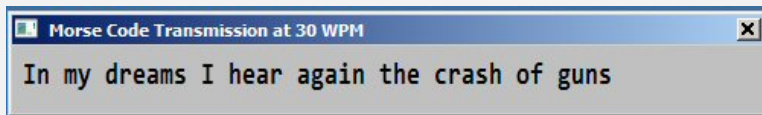
The user can choose colors individually for the "Cipher Machine" banner (logo), window background, buttons, user-supplied text, and hard-wired text by clicking the appropriate buttons in the top half of the "Choose Colors" window. When one of these buttons is clicked, the following color mosaic is displayed:



The user can either click on a color square or enter a color's RGB values (0 to 255) in the boxes provided. Then when the [Choose] button is clicked, the selected color will be applied appropriately (in this example, to the window background).

Morse Code Feature

An audible Morse-code⁴ transmission of the text (plain or cipher) in the text box can be heard by clicking the [Transmit MORSE] button. Before doing this, the desired transmission rate, in words per minute (WPM) can be selected: 15, 20 (default), or 30 WPM. These transmission rates are only approximations which depend on the average word length and the computer's CPU speed. When the [Transmit MORSE] button is clicked, a small window like the following appears, where the characters are displayed as their Morse-code equivalents are sounded.



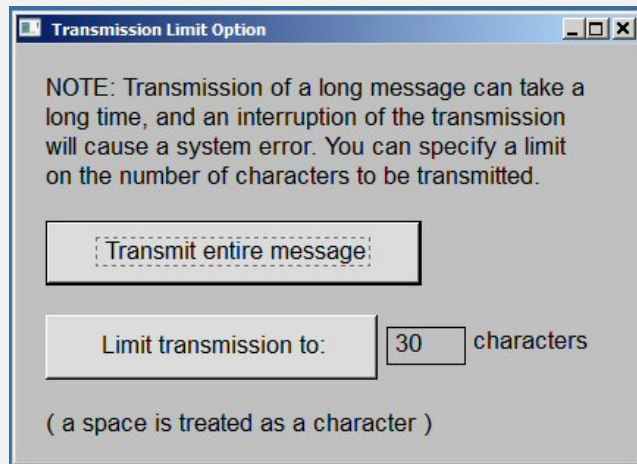
The characters are displayed in the transmission window as they appear in Cipher Machine's text box, whether they be upper-case, lower-case, special characters, punctuation marks, etc. But, the Morse code for an upper-case letter *is the same* as for its lower-case equivalent, and any special characters that are not in the Morse code lexicon are NOT sounded⁵. When the transmission is

⁴ i.e., the *International* Morse Code

⁵A "Morse" cipher will contain only characters in the Morse code lexicon. Before the plain text is encrypted, any plain-text character not in the lexicon will be replaced by a space, and all lower-case letters will be replaced by their upper-case equivalents.

completed, there is a short pause before the transmission window closes.

If the text in the text box consists of more than 30 characters, the following window will appear when the [Transmit MORSE] button is clicked.



The user has the option of transmitting the entire message or specifying a limit on the number of characters transmitted (default value is 30).

A cipher to be audibly transmitted in Morse code should be created using the "MORSE COMPATIBLE" encryption option. An audibly-transmitted cipher, that was created with the "MOST SECURE" encryption option, cannot, in general, be properly decrypted.

Appendix: International Morse Code

The International Morse Code lexicon includes the following codes for the letters, numbers, punctuation marks, and special characters:

International Morse Code

1. A dash lasts as long as three dots.
2. Intervals between a letter's dashes and dots last as long as one dot.
3. Intervals between a word's letters last as long as three dots.
4. Intervals between words last as long as seven dots.

<p>A ● ■■</p> <p>B ■■ ● ● ●</p> <p>C ■■ ● ■■ ●</p> <p>D ■■ ● ●</p> <p>E ●</p> <p>F ● ● ■■ ●</p> <p>G ■■ ■■ ●</p> <p>H ● ● ● ●</p> <p>I ● ●</p> <p>J ● ■■ ■■ ■■</p> <p>K ■■ ● ■■</p> <p>L ● ■■ ● ●</p> <p>M ■■ ■■</p> <p>N ■■ ●</p> <p>O ■■ ■■ ■■</p> <p>P ● ■■ ■■ ●</p> <p>Q ■■ ■■ ● ■■</p> <p>R ● ■■ ●</p> <p>S ● ● ●</p> <p>T ■■</p>	<p>U ● ● ■■</p> <p>V ● ● ● ■■</p> <p>W ● ■■ ■■</p> <p>X ■■ ● ● ■■</p> <p>Y ■■ ● ■■ ■■</p> <p>Z ■■ ■■ ● ●</p>
<p>1 ● ■■ ■■ ■■ ■■</p> <p>2 ● ● ■■ ■■ ■■</p> <p>3 ● ● ● ■■ ■■</p> <p>4 ● ● ● ● ■■</p> <p>5 ● ● ● ● ●</p> <p>6 ■■ ● ● ● ●</p> <p>7 ■■ ■■ ● ● ●</p> <p>8 ■■ ■■ ■■ ● ●</p> <p>9 ■■ ■■ ■■ ■■ ●</p> <p>0 ■■ ■■ ■■ ■■ ■■</p>	

Punctuation / Special Character	International Morse Code
.	· _ · _ · _
,	_ _ · · _ _
?	· · _ _ · ·
'	· _ _ _ _ ·
"	· _ · · _ ·
-	_ · · · · _
(_ · _ _ ·
)	_ · _ _ · _
:	_ _ _ · · ·
=	_ · · · _
+	· _ · _ ·
@	· _ _ · _ ·
/	_ · · _ ·