

Cipher Machine

User Manual

December 9, 2014

Table of Contents

Unbreakable Ciphers	2
Encryption Levels	2
Secure Communications	2
Creating a Cipher	2
Decrypting a Cipher	5
Color Schemes	6
Morse Code Feature	7
Appendix: (International Morse Code Lexicon)	8

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. For each encryption or decryption task, 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 user selects the desired option by checking the appropriate box. The "Morse-Compatible" level uses a character set (lexicon) of 50 characters, as defined in the Appendix. Ciphers encrypted at this level can be transmitted audibly as International Morse code and successfully decrypted at the receiving end. Any character in the original plain text that is not in the 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 and both upper-case and lower-case letters.

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 (default) is checked. The Morse-code transmission rate of 20 words per minute is the default value.

To type text into the code-key box or main 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

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 then stored in the folder.

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

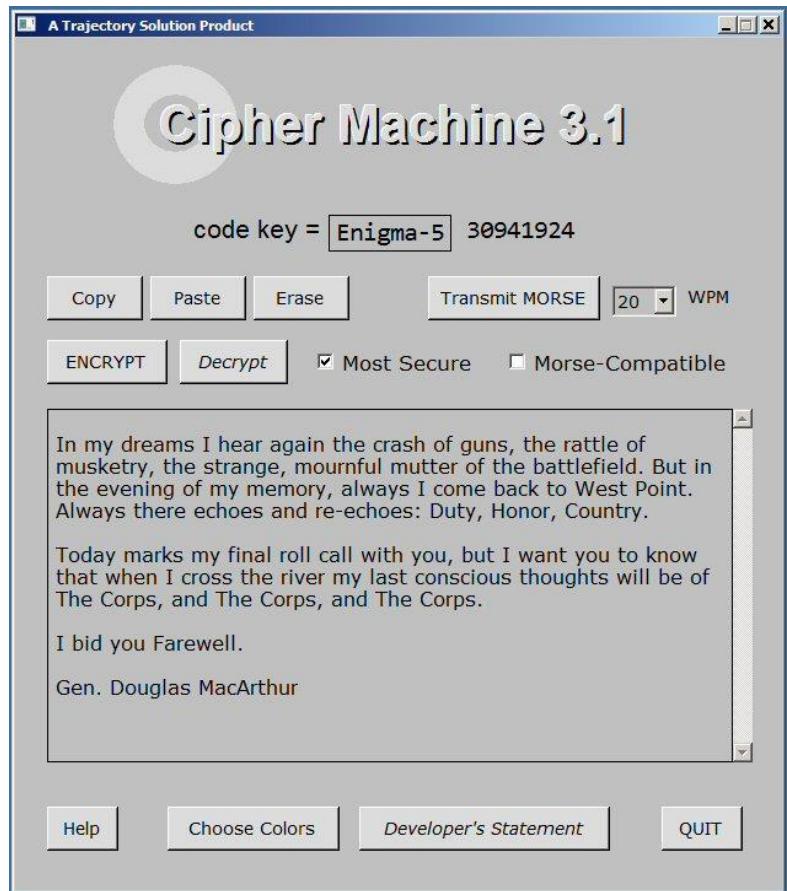
down the mouse's left key and dragging the cursor across the text.

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

The "Paste" button is used to paste whatever is in the keyboard buffer into the main 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 main text box should be cleared before clicking the "Paste" button.

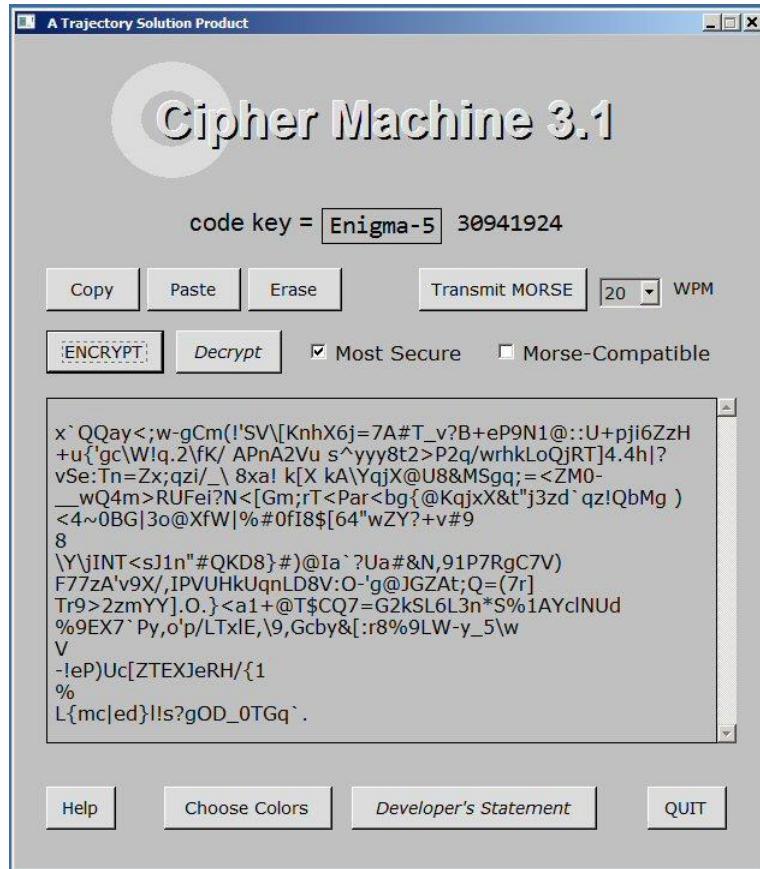
The code key can be left blank or can consist of any number of characters up to a maximum of eight. In this example, the user has typed in the code key "Enigma-5". The Cipher Machine unit's unique eight-digit serial number is displayed to the right of the code-key box. In this example, the plain text in the main 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).



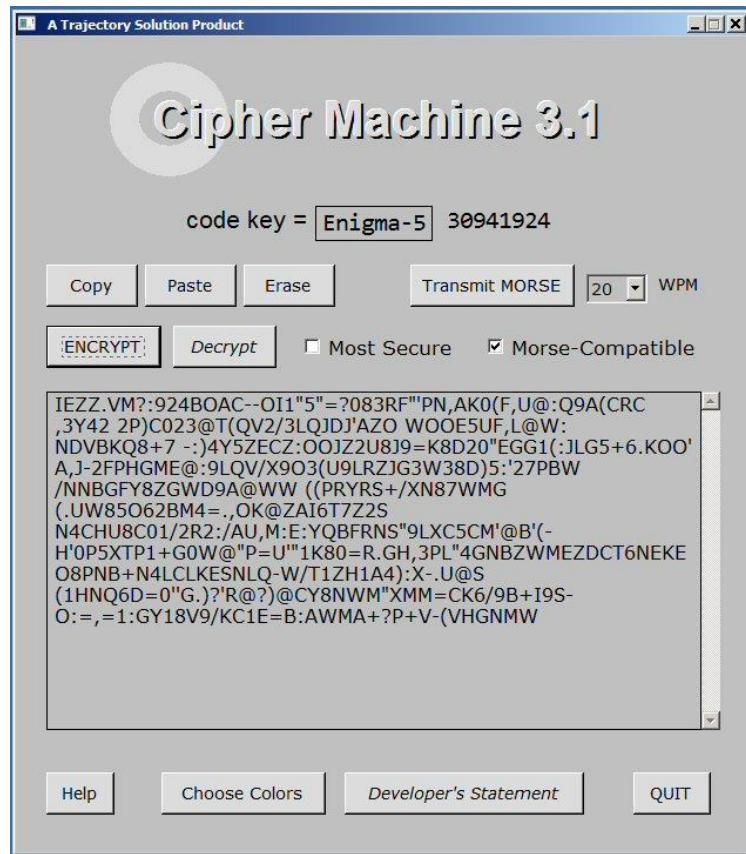
NOTE: *It is advisable to NEVER END the plain text message with a carriage return.* When the resulting cipher is copied and pasted into an email or pasted into a text file, the ending carriage return(s) may not be properly preserved. In such a case, the decryption will be gibberish.

In this example, a click of the "Encrypt" button will produce the cipher shown in the window below:



Had the "Morse-Compatible" encryption box been checked instead of the "Most Secure" box, a click of the "Encrypt" button would have produced the cipher shown in the window to 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 a Notepad attachment or to simply paste the cipher into the body of the email message. However, it is NOT recommended that a WORD document attachment be used.

A cipher can be created by an encryption sequence (clicking the "Encrypt" button a number of times). Obviously, the recipient of the cipher must know the encryption sequence in order to decrypt the cipher.

Decrypting a Cipher

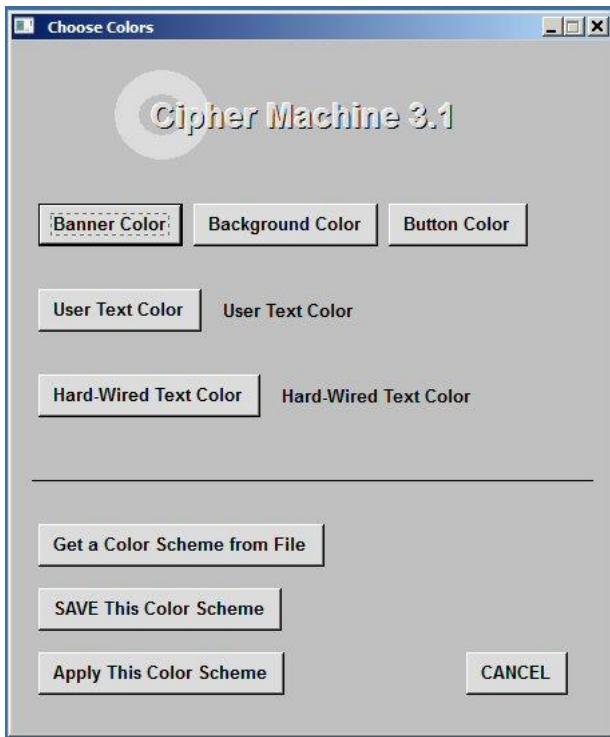
When the recipient receives the cipher, he can copy and paste it into his Cipher Machine's empty main text box (if the box is not empty, he can clear it by clicking the "Erase" button). He must also type the proper code key into the code-key box and check the proper encryption-level box. Then, when he 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.

A Cipher Machine's cipher will never end with a space. If an ending space is observed in the cipher, having perhaps been inserted by an intermediate word processor or email application, the space must be removed before the cipher can be properly deciphered. A cipher CAN begin and end with one or more carriage returns. However, care must be taken to insure that any such carriage returns are preserved during transmission of the cipher.

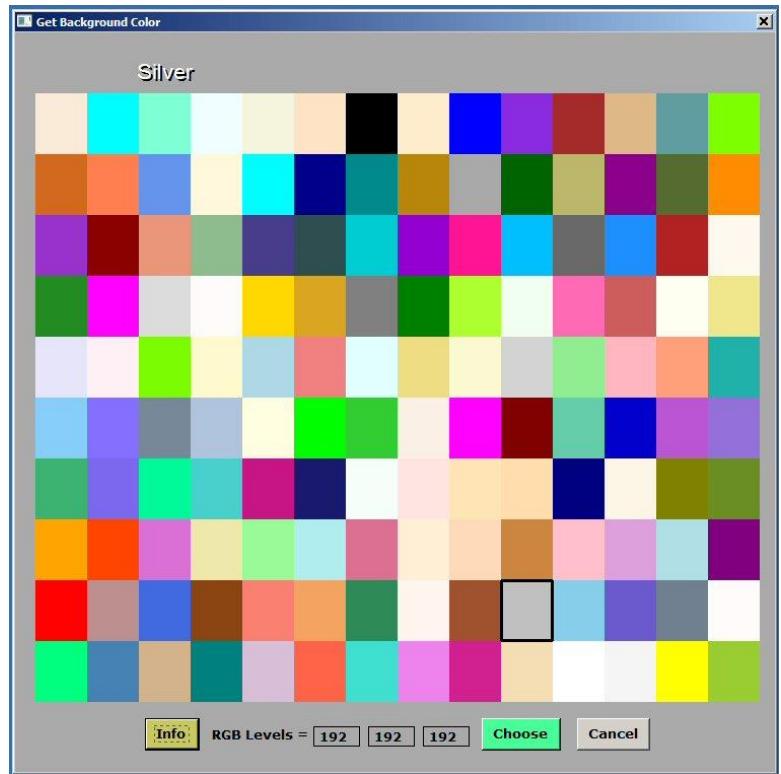
Color Schemes

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.

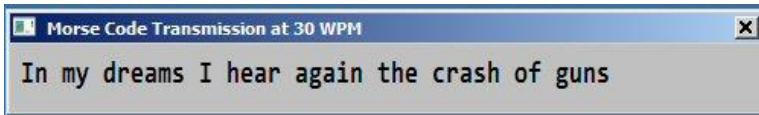
The user can choose colors individually for the "Cipher Machine" banner (logo), window background, buttons, user-supplied text, and hard-wired text by clicking the appropriate buttons in the top half of the "Choose Colors" window. When one of these buttons is clicked, the following color mosaic is displayed:



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: either 15, 20, 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.



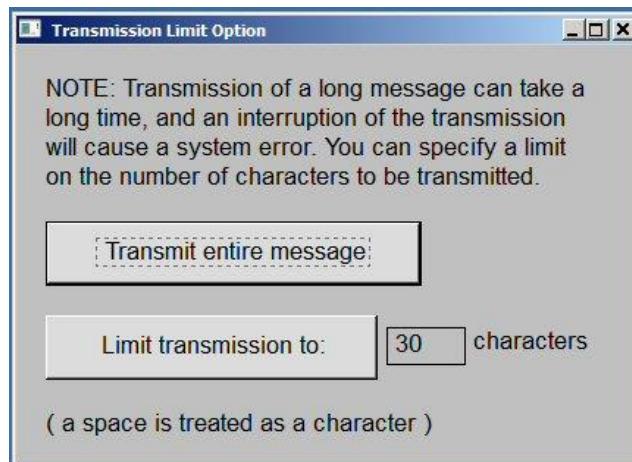
The characters are displayed in the transmission window as they appear in Cipher Machine's main text box, whether they be upper-case, lower-case, special characters, punctuation marks, etc. But, the Morse code for an upper-case letter *is the same as* for its lower-case equivalent, and any special characters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

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

⁵ A "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 may not be properly decrypted.

Appendix: International Morse Code Lexicon

Cipher Machine's International Morse code lexicon includes the following codes for the letters, numbers, and spacings:

International Morse Code

1. A dash is equal to three dots.
2. The space between parts of the same letter is equal to one dot.
3. The space between two letters is equal to three dots.
4. The space between two words is equal to seven dots.

A ● —
B — — ● ● ● .
C — — ● — ● .
D — — ● ● .
E ● .
F ● ● — — ● .
G — — — ● .
H ● ● ● ● .
I ● ● .
J ● — — — — — .
K — — ● — .
L — ● ● ● .
M — — .
N — .
O — — — .
P ● — — ● .
Q — — — ● .
R — — ● .
S ● ● ● .
T —

U ● ● — —
V ● ● ● — —
W ● — — —
X — ● ● — —
Y — ● — — —
Z — — ● ● .

1 ● — — — — —
2 ● ● — — — —
3 ● ● ● — — —
4 ● ● ● ● — —
5 ● ● ● ● ● —
6 ● — — ● ● ●
7 — — — ● ● ●
8 — — — — ● ●
9 — — — — — ●
0 — — — — — — .

The lexicon includes the following codes for punctuation marks and special characters:

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