8. DECRYPTING A MESSAGE

To decrypt a message, the receiver set-up the start position according to the first trigram **YPX**, and typed in the second trigram on the message to obtain the message key **TMK** . Next, the receiver used the message key **TMK** as a start position to decode the actual message. If a message was divided into several parts, the operator had to insert a new start position and message key for each part of the message.

We will follow this same procedure with our practice message.

Go to "Start," "All Programs," "Enigma" icon.

1. Open Enigma cover.

2. Set-up rotors and rings per code sheet, December 16, 1944

3. Close cover.

4. Set-up plug settings per code sheet, December 16, 1944.

5. Return to Enigma top view.

6. Set the first trigram YPX as start position on the rotors.

7. Type the second trigram FZQ (the encrypted message key).

8. Set the resulting output, TMK (the decrypted message key), as the rotors' start positions.

9. Verify that a valid date was used to encrypt the message. Do this by looking for one of the four possible 3-letter Kenngruppen trigrams from the codesheet. One of these Kenngruppen trigrams plus two random letters must appear as the first five letters of the message. These five letters will confirm that a valid date was used to encrypt the message. **Do not decrypt these first five letters of the message.** Start decrypting the message at the 6th letter.

10. Type-in the encrypted message text to retrieve the original plaintext.

11. You can display the plaintext and ciphertext in a little text box at the bottom of the Enigma by clicking on the lock (18) on the wooden box. NOTE: The text will appear in 4- or 5-letter groups, depending on the type of machine.

12. When you have finished decrypting your message, move the mouse over the textbox and click on the textbox when the "Click here to Copy Output to Clipboard" message appears. Now you can see the entire message.

13. If you can read your decrypted message, congratulations on a job well done! You may have to use some mental gymnastics to figure out where one word starts and the last word ends!

14. To print a copy of the message, highlight the message and copy it from the Enigma clipboard screen. Open a word processor program such as Word or Wordpad, and paste the message. Print the document.

Now you can go back and choose a different codebook sheet, day, trigrams, and even another type of Enigma machine (If you are really brave!) to make your own messages.