

For Wednesday, October 17

Create an Enigma ciphertext.

Various procedures were used to do this. The procedures varied by the unit using the Enigma and the procedures evolved during the War. We will use the procedures in *Codebreakers* by Hinsley and Stripp, pages 86 and 87.

Look at <http://www.nku.edu/~christensen/071mat483001.html> for Monday, October 8, for links.

Use Tony Sale's Enigma emulator

<http://www.codesandciphers.org.uk/enigma/emachines/enigmad.htm>

Follow the instructions in *Codebreakers* by Hinsley and Stripp, pages 86 and 87. You received a copy in class on Monday, and a copy is available on the link "Setting up Enigma." See numbers 1 through 7 and (a). Recall that this emulator does not use the ring setting – ignore the ring setting (number 2).

Use the daily settings from the Enigma monthly setting sheet (you received a copy in class; there's a link on the website) for the 12th day of the month. Ignore the *Ringstellung*. Ignore the *Kenntgruppen*.

Using the procedure outlined in Hinsley and Stripp, the machine operator must select two random wheel settings -- an indicator setting that is transmitted in the clear at the beginning of the message (see page 87 (a)) and a message setting that is the actual setting for the message encryption.

Encrypt a message. Place the three-letter, randomly selected message setting in the clear at the beginning of the message. Follow that with the three-letter message setting encrypted twice using the indicator setting. Follow that with your message encrypted using the message setting.

The person who receives your message will decrypt it – not cryptanalyze it.