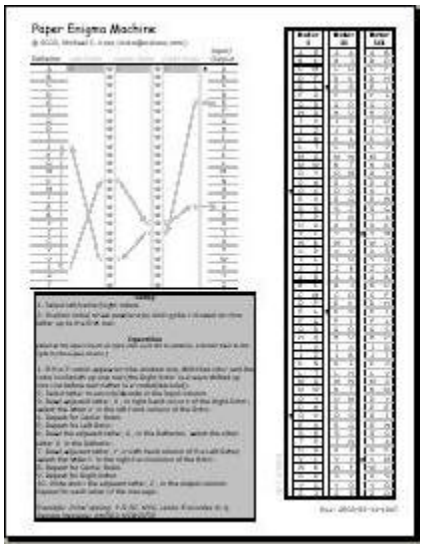
The Paper Enigma Machine

http://mckoss.com/crypto/enigma.htm

Mike Koss
mike04@mckoss.com

Wednesday, April 28, 2004

Introduction



Having been fascinated with codes and secret writing since I was young, I had a special fascination for the mechanical cryptographic machines I read about in Martin Gardner's *Codes, Ciphers, and Secret Writing,* and in David Kahn's *The Code Breakers*. While there are several museums where you can see some of these devices they are usually placed behind a glass case where you cannot see for yourself how they work.

With the advent of the Internet, it became possible for people with obscure hobbies like collecting cryptographic machines to find others with similar interests and a market was born on sites like eBay. I first realized that I could own an Enigma of my own via a Bletchley Park email mailing list. A collector in Washington D.C. emailed the list indicating he had an Enigma to sell. We agreed on a price and I flew to Washington (from Seattle) to inspect the machine. We also took it to the National Cryptological Museum (http://www.nsa.gov/museum/) to check it for authenticity.

Satisfied, I returned home to Seattle with my first historical cryptographic machine. I found replacement bulbs and wired up a battery so I could put the machine though its paces. Over the years, I've enjoyed demonstrating the workings of the Enigma to friends, and I have taken it to local area schools to lecture on the workings and historical significance of the Enigma.

In 2003, I had the pleasure of lecturing to the MIT Alumni Club of Puget Sound. Knowing my audience would be very technical, I wanted to do more than have a simple show and tell. These folks would want to get their hands "dirty" and actually learn the inner workings of the machine. There are several Enigma simulators available on the Web, but I wanted to be able to create a tangible "kit" that each participant could build and use on their own. Thus was born, The Paper Enigma.

The Paper Enigma requires only a pair of scissors to assemble a working replica of the German Enigma machine; messages encoded on one can be decoded on the other! The Paper Enigma is simplified in two respects. First, it lacks a plug board (*stecker*) which adds an additional layer of a single transposition cipher to the Enigma. While this innovation, added to the military version of the Enigma, added

an extra layer of complexity to the original Enigma, it does not change the fundamental operation of the machine.

Second, there are no "ring settings". These merely allow the inner wiring of each rotor to be rotated with respect to the outer indicator settings. The only cryptographic effect is that the rotors will "roll-over" at a different position. I've left this off for simplicity as it does not change the basic workings of the machine.

The fundamental operation of the Enigma is quite simple. When a keyboard letter is pressed, an electrical contact is made on one of 26 wires entering on the right hand side of the rotor system. That signal is then carried through the three rotors from right to left. The internal wiring of a rotor simply permutes each of the 26 input contacts on the right to one of the 26 output contacts on the left.

After traveling from right to left through all three rotors, the signal is then "reflected" by a fixed permutation (via a "reflecting rotor") and then travels in reverse through all three wheels again (this time from left to right). The 26 contacts are connected to light bulbs so that the ultimate code letter is illuminated on a lamp for as long as the keyboard key is held down.

The right hand rotor rotates to the next letter position when each key is pressed, thus changing the final alphabet permutation for every letter of the message. The other rotors can also rotate as explained below.

An excellent technical description of the workings of the Enigma can be found at Tony Sale's web site: http://www.codesandciphers.org.uk/enigma/.

How to use the Paper Enigma

Each part of the Enigma machine is modeled by a corresponding component of the Paper Enigma:

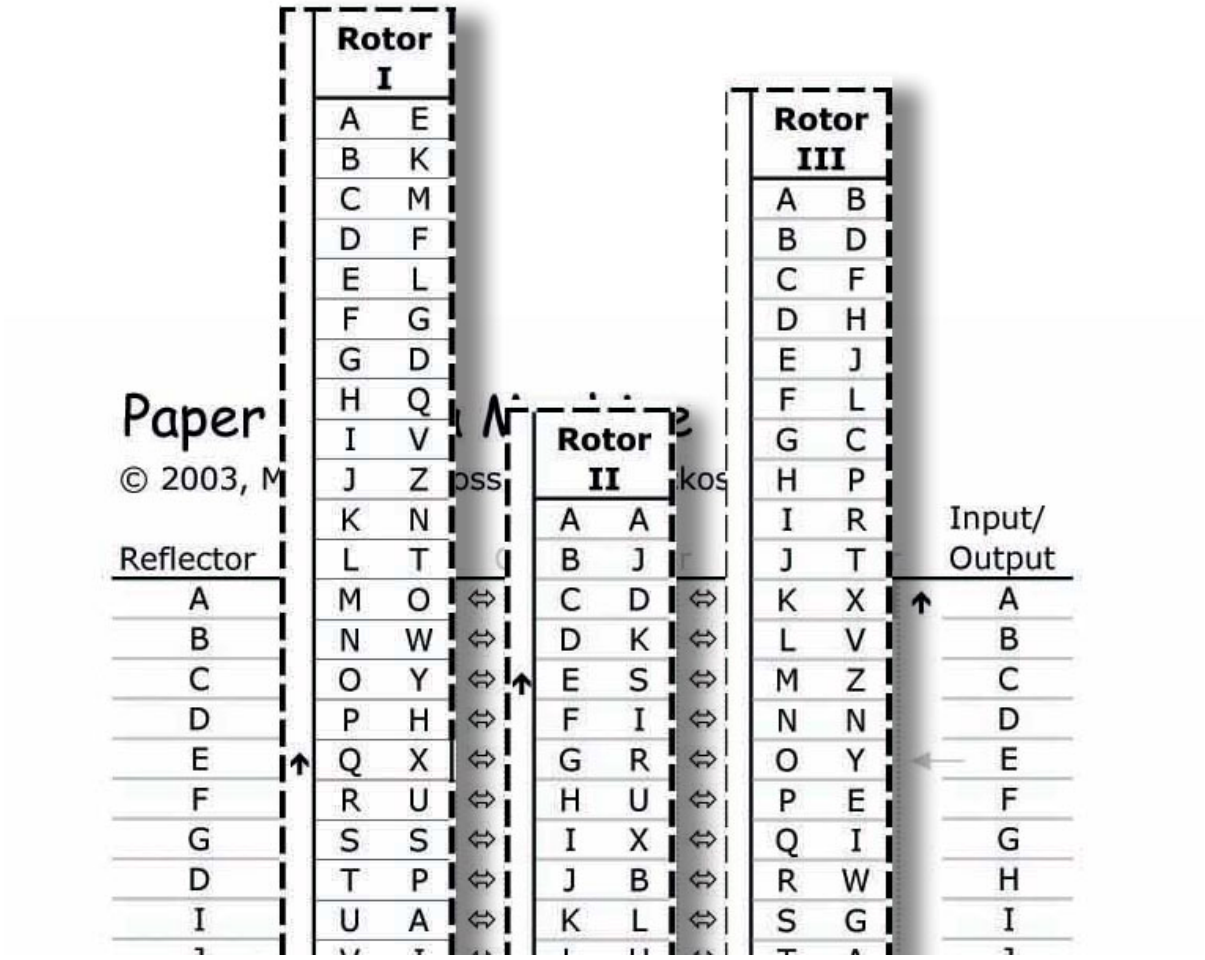
Real Enigma	Paper Enigma
Electrical Rotor	Paper Strip: Each connection made in a physical rotor is indicated by matching letters in the left and right hand column of a rotor strip. *Note that each paper rotor has two copies of the alphabet printed on it. The reason being that we can always position the strip so that a particular letter can be at the top row of the machine and we still have 25 letters below it to line up with all the input/output rows.*
Reflecting Rotor	Connections of the reflector are indicated by matching letters in the left hand column (marked "Reflector").
Rotor position indicator (windows)	The top row (printed with gray background) aligns with the left-hand column letters of each rotor to indicate rotor positions.
Keyboard and Lamps	Right hand column of letters (marked "Input/Output").

To assemble the Paper Enigma, simply cut out the three rotor strips and place each one over the columns marked "Left Rotor", "Center Rotor", and "Right Rotor".

Operation

To use the Paper Enigma, one need know only how to emulate the motion of the rotors after each letter, and be able to trace the path of the letter permutations through the rotor strips. It's probably easiest to follow a specific example (this example is printed on the Paper Enigma in light gray).

1. First position the rotors into their selected columns and starting positions. In our example, we'll use rotors I, II, and III in order, and start at positions "M", "C", and "K". In a real Enigma, the rotor wheels would be inserted into the machine, and then rotated until "M", "C" and "K" were visible on the indicator windows above each rotor. In the paper Enigma, we position the strips so that the indicated left-hand letter of each rotor is over the first row (next to input/output letter "A").



2. The first step of encoding any letter is to *Advance the Rotors*. This is done before encoding each letter – even the first one. The right-most rotor is always shifted up one letter. So, in our example, rotor III is shifted up to the "L" position.

   The rotors on the Enigma move something like an odometer – but not quite! In an odometer, we would expect the sequence 189 -> 190 -> 191. On an Enigma, we would have the corresponding sequence 189 -> 190 -> 201(!) The reason being that an Enigma machine does not contain a true "carry" mechanism. Rather, each rotor has a notch on its left hand side. When the notch rotates into the "roll-over" position, both the notched wheel AND the wheel to the left are moved one letter ahead.

   In the Paper Enigma, the notches are indicated with small upward pointing arrows along the left edge. When the starting position for a letter has an arrow in the first row, move that rotor and the one to its left up one position. Note that in no circumstance should any rotor advance more than one position between two successive letter encodings; either the right wheel will move by itself, or the right wheel and the middle wheel will move together, or all three wheels will advance one letter.

3. Now it is a simple matter to trace the path of the permutations through the machine. Starting at the input letter on the right (in this case, "E"), note the letter on the right-most rotor III (another "E"). Find the matching "E" in the left hand column of rotor III.

4. That "E" lines up with the letter "Y" on the right hand column of the center rotor II. Find "Y" in the left hand column.

5. "Y" lines up with "V" in left-most rotor I. Locate "V" in the left hand column.

6. "V" lines up with "J" in the reflector. Find the other letter "J" in the reflector.

7. Now we trace the signal path back through the rotors form left to right. "J" in the reflector lines up with a "J" in rotor I.

8. "J" lines up with "P" in rotor II.

9. "P" lines up with "D" in rotor III.

10. Finally "D" lines up with "Q" in the Input/Output column. Our output letter is "Q".

To encode (or decode) a whole message, repeat the above steps for each letter. Note that the Enigma can be used to decode any message by simply starting the machine in the same configuration as the encoding. Enigma encodings are symmetrical; if "A" encodes to "X", then "X" will encode to "A" by following the reverse path through the rotors.

Starting from the position above (rotors I-II-III starting at positions M-C-K) try decoding this sample message: QMJIDO MZWZJFJR.

Availability

The Paper Enigma is available as a free download from http://mckoss.com/crypto/enigma.htm. All you need are a pair of scissors and you too can have a working model of the famous World War II German Enigma machine.

Biographical Sketch

Mike Koss is a software engineer living in the Seattle area. He received his MS in computer science from MIT in 1983, including a study of cryptology under Professor Ron Rivest. Besides feeding his eBay addiction with antique cryptographic machines, Mr. Koss's interests include programming instruction and web-based application development. He is currently president of the MIT Alumni Club of Puget Sound.