The Enigma Machine

Overview of Project #4  
The Enigma Machine

Cryptography—Bletchley Park

I’ve twice had the opportunity to teach cryptography at Stanford in Oxford, which made it possible to visit Bletchley Park—the home of the Government Code and Cipher School (GCCS), where the Enigma code was broken.

In our field trips to Bletchley Park, our tour was led by Jean Valentine, who worked with the Bombe decryption machine shown in these pictures.
The Enigma Rotors

Operation of the Enigma Machine

- Whenever the operator types a letter key on the Enigma, the following things happen:
  1. The force of the key press advances the fast rotor one position. If the indicator on the fast rotor wraps around from Z to A, that action “carries” to the medium rotor, just like the digits on an odometer. Similarly, if the medium rotor passes Z, the slow rotor advances one position.
  2. An electrical signal is fed into the wire corresponding to the key, which then flows through seven letter-substitution steps:
     - Through the fast rotor from right to left.
     - Through the medium rotor from right to left.
     - Through the slow rotor from right to left.
     - Through the reflector, which turns the signal around.
     - Through the slow rotor from left to right.
     - Through the medium rotor from left to right.
     - Through the fast rotor from left to right and on to the lamp.

Encoding the Letter “A”

The Next “A” Is Different

Milestones for Project #4

- Like the ImageShop application you created for Project #3, the Enigma project is divided into a series of milestones that allow you to write and test your code in pieces:
  Milestone 1: Create the keyboard.
  Milestone 2: Respond to mouse events in the keys.
  Milestone 3: Create the lamp panel.
  Milestone 4: Connect the keyboard and the lamp panel.
  Milestone 5: Add the rotors in their original position.
  Milestone 6: Implement click actions for the rotors.
  Milestone 7: Implement one stage in the encryption.
  Milestone 8: Implement the full encryption path.
  Milestone 9: Make the rotors advance on pressing a key.
- The web site for the assignment includes animations for each of the milestones so you can more easily check you progress.

What Made Enigma Vulnerable?

- Early in the war, mathematicians working for the Polish Resistance were able to smuggle Enigma machines to France and England along with a strategy for breaking the code.
- The British government established a top-secret cryptography center at Bletchley Park and staffed it with the top British mathematicians.
- The decryption team at Bletchley was able to exploit the following facts about the Enigma machine:
  - The encoding is symmetrical.
  - The Enigma machine can never map a character into itself.
- The codebreakers were helped by the fact that the Germans were careless and overconfident. In believing they had an unbreakable encoding machine, they failed to take adequate measures to safeguard the integrity of their communications.
Breaking the Enigma Code

- The most common technique used at Bletchley Park was the known-plaintext attack, in which the codebreakers guess that a particular sequence of characters exists somewhere in the decoded message. A sequence of characters that you guess is part of the plaintext is called a crib.
- *The Imitation Game* gives the mistaken impression that Alan Turing came up with the idea of a crib during the war. The value of a crib has been known since antiquity.
- The 2001 movie *Enigma* offers a much more accurate view of why cribs are important and how codebreakers use them.

Jean Valentine on Bletchley Park