Under What Circumstance Can the Enigma Cipher Machine Be Decrypted?

Ribler, Diem-Mi (School: Central Virginia Governor's School for Science and Technology)

The Enigma was an encryption device the Nazis used during World War II. The purpose of this study was to determine the circumstances under which intercepted Enigma messages could be decrypted without knowledge of the machine settings. A computer simulation of the Enigma was programmed and used to encrypt and decrypt messages. This simulator was also used as the basis for algorithms designed to crack the code. The machine itself employed a polyalphabetic cipher implemented through the use of three interchangeable rotors, a reflector, and a plugboard. Alan Turing and the code breakers at Bletchley Park were able to crack Enigma messages when they contained some known plaintext using a plugboard deduction algorithm based on assumption and contradiction. This elimination algorithm was able to dramatically reduce the number of machine settings that needed to be evaluated. Turing's elimination algorithm was implemented in the Bombe machine used during the war. A computer program was written to simulate this process. The program was able to determine all rotor settings and the plugboard configuration in an average of one minute. When the known plaintext contained all the letters in the alphabet, it was found that the elimination method was always successful in determining all settings. When known strings contained fewer characters, the program could still decrypt these messages in some cases. Encrypted messages were tried with the same plaintext using various settings of the machine, and in some cases, the program was able to break the code while in others it was not. A sample of settings were tested to determine an estimate of the probability of cracking a message that contained a particular plaintext string.

Awards Won: