1125-B1-245 **N. Paul Schembari*** (schembariesu@gmail.com), Mathematics Department, 200 Prospect Street, East Stroudsburg, PA 18301. *The Simulation and Cryptanalysis of Rotor Ciphers.*

Ciphers based on rotor machines were the state-of-the-art in the mid-1900s, with arguably the most famous being the German Enigma. We have found that students have great interest in the Enigma and its cryptanalysis, so we created our own rotor cipher which is simulated with shifting tables and can be cryptanalyzed. Ours and the historic rotor ciphers are based on rotating wheels which change the encryption with each character encrypted. Our cipher is easily programmed or can be simulated in Excel for students with less experience, and its cryptanalysis leads to the re-creation of the rotor wheels. The cryptanalysis of our cipher is executed on simulated machines with one or two wheels and is based on a known-plaintext attack.

Our classroom experiences include discussion of Enigma encryption and the analysis of our rotor cipher. Also as part of our instruction in cryptology, a National Security Agency historian visited campus to display an Enigma, and we display another rotor machine (US Navy CSP-1500 Six Rotor Portable Mechanical Cipher Machine) on loan from the National Cryptologic Museum, Fort Meade, MD. In this paper we discuss the simulation of our rotor cipher, its cryptanalysis, external cryptologic educational experiences, and experiences with our exercises. (Received August 18, 2016)