1106-C1-1413 **Edmund A. Lamagna*** (eal@cs.uri.edu), Department of Computer Science and Statistics, University of Rhode Island, Kingston, RI 02881. *Decrypting Cryptography.*

Cryptography is an important, contemporary real-world application of mathematics. The subject can be taught at different levels to diverse populations from freshman non-majors to upper level math and computer science students. To assist in teaching such courses, the presenter has created a website with tools for encrypting and decrypting using a representative variety of classical and contemporary techniques. The methods include substitution and transposition ciphers, the Enigma machine, simplified versions of modern block codes (DES, AES), and public key techniques such as Diffie-Hellman and RSA. The site provides both pedagogic tools to trace step-by-step how the methods operate, and computational tools to perform cryptanalytic attacks on classical ciphers. Students use the site to work on problem sets and the tools to crack cryptographic challenges. The website eliminates the need for students to write programs to perform these computational tasks.

The tools are demonstrated by mounting an automated attack on the Vigenère cipher, a polyalphabetic substitution studied in virtually every cryptography course. The statistical and linguistic ideas behind the attack are presented, and then the tools are used to demonstrate these concepts visually. (Received September 12, 2014)