1035-G1-836 **Joshua Brandon Holden*** (holden@rose-hulman.edu), CM #125, Rose-Hulman Institute of Technology, 5500 Wabash Ave., Terre Haute, IN 47803. *The Pohlig-Hellman exponentiation cipher as a bridge between classical and modern cryptography.*

The Pohlig-Hellman exponentiation cipher is a symmetric-key cipher that uses some of the same mathematical operations as the better-known RSA and Diffie-Hellman public-key cryptosystems. First published in 1978, the Pohlig-Hellman cipher was never of practical importance due to its slow speed compared to ciphers such as DES and AES. The theoretical importance of the Pohlig-Hellman cipher comes from the fact that it relies on the Discrete Logarithm Problem for its resistance against known-plaintext attacks, as does RSA and several other modern cryptosystems. For this reason, the Pohlig-Hellman system can play a very important role pedagogically, since it also shares many features in common with classical ciphers such as shift ciphers and Hill ciphers. Thus, it allows the instructor to introduce the important concepts of the discrete logarithm and known-plaintext attacks separately from the more conceptually difficult idea of public-key cryptography. (Received September 16, 2007)