

1035-G1-674 **Kristen A. Meyer*** (kristi.meyer@wlc.edu), 8800 W. Bluemound Rd., Milwaukee, WI 53226.
Are You Talking to Me? An Introduction to Identity Based Encryption.

Public-key cryptography is a standard topic in almost every introductory cryptology course. However, RSA is generally the only example given of a working public-key system. Another example of a functional public-key cryptosystem is Identity Based Encryption, or IBE. IBE has properties which work particularly well in encrypting e-mail, making it a timely and relevant topic for students. Although IBE requires a minimal knowledge of cyclic groups, the necessary group theory can be taught in a self-contained manner if necessary. This allows for an application of basic abstract algebra concepts to cryptography, even in a class where the students have not yet studied abstract algebra. In this talk, I will discuss the basics of IBE and present ideas on how this topic can be integrated into a cryptology course. (Received September 13, 2007)