

Date: April 1st, 2009

Speaker: Stephen Haas, UNC Asheville

Title: *A mathematical security blanket, a.k.a. RSA cryptography*

Abstract: As technology has evolved, we have become capable of sending information over large distances to others using at first telegraphs and now email and facebook. With this ability arose a problem, we needed a way for our information to be secure. With that in mind, we will be looking at RSA cryptography, a method of using large prime numbers to keep information safe when it is being transmitted, so that only those holding the key can read it. We will discuss the methods used to generate the key, to encrypt the message, and to decrypt the message. We will also explore the research being done in an attempt to break RSA cryptography, and the counter-research being done to ensure its security. Finally, we will look at what information is encrypted using RSA cryptography.