Rick Klima* (klimare@appstate.edu), Appalachian State University, Department of Mathematical Sciences, Boone, NC 28608, and Neil Sigmon. Estimating Success When Combining RSA and the Diffie-Hellman Key Exchange. Preliminary report.

In the RSA system, a plaintext $m$, with $0 \leq m \leq n - 1$, is transformed into the ciphertext $m^e \mod n$, where $n$ is the product of two primes and $\gcd(e, \varphi(n)) = 1$. Since the RSA system is public-key, users can make $e$ public knowledge without compromising security. To break the system, an eavesdropper would have to factor $n$, a seemingly intractable problem if the prime factors of $n$ were both extremely large. However, being unable to factor $n$ is the only thing preventing an eavesdropper from breaking the system. A method through which it might be possible to keep the system secure even if $n$ were factored is to hold the key $e$ secret, by, for example, using the Diffie-Hellman key exchange. But there is no guarantee that the Diffie-Hellman key exchange with a non-prime modulus $n$ would result in a value of $e$ that satisfies $\gcd(e, \varphi(n)) = 1$. In this talk, we will discuss and present the result of a large number of simulations estimating the probability that the Diffie-Hellman key exchange with a non-prime modulus $n$ will result in a value of $e$ that satisfies $\gcd(e, \varphi(n)) = 1$. (Received August 26, 2012)