A Practical Cryptosystem with Provable Security: Three New Innovations in Cryptography

Howe, Wyatt (School: Hershey High School)

The purpose of this project is to develop a cipher (encryption algorithm) and cryptosystem that is both practical and provably secure. First, I investigate the relationship between continued fractions and irrational numbers and how they can be applied in cryptography as the basis of a fast, new stream cipher and key derivation function. Next, I investigate how to implement a key exchange using vector products (a new approach) and developed a viable model. Finally, I designed a new structure that can be used to create an entire family of secure block ciphers from any pseudorandom function. I have written a computer program to run each algorithm I design and collect data (e.g. number of bits flipped, digits of accuracy, distribution of ciphertext bytes) that I analyze using differential cryptanalysis. The result is a set of original building blocks that form a new cryptosystem that processes data faster than the most used secure ciphers currently available. The components are also useful individually for other cryptographic purposes and include additional advantages, such as encryption and decryption use the same functions which makes it easier to implement in software and cheaper in hardware, and the key exchange can be done very efficiently because the new approach isn't dependent on expensive operations such as exponentiation.

Awards Won:

Mu Alpha Theta, National High School and Two-Year College Mathematics Honor Society: Second Award of $1,000

Air Force Research Laboratory on behalf of the United States Air Force: First Award of $750 in each Intel ISEF Category