Name(s)	**Project Number**
Rachana Madhukara	**J1418**

Project Title

Devising a Secure and Efficient Hybrid Cryptosystem

Abstract

Objectives/Goals
The objective of this project is to devise a cryptosystem that is both efficient and secure.

Methods/Materials
Paper, pencils and a computer for initial research. Wolfram Mathematica software was used to validate final mathematical operations. After researching, determined that combining an asymmetric cryptosystem with a key exchange is beneficial. This was mathematically verified later.

Results
The combination suggested was more secure and efficient since the mathematical equations proved that the system is less susceptible to attacks.

Conclusions/Discussion
Combining the two systems did produce a stronger, more secure cryptosystem in the end. The cryptosystem is stronger and efficient as it can withstand more attacks while also optimizing computations. My cryptosystem is also able to eliminate most problems from both RSA and the Diffie-Hellman Key Exchange methods. Hence I conclude that my method produced a strong cryptographic system to encode messages.

Summary Statement

I devised a more efficient and secure hybrid cryptosystem to better encode messages.

Help Received

None. I designed and performed the project by myself. Then Dr. Nagabhushan reviewed my results.