OFFICIAL ABSTRACT and CERTIFICATION

Applying Blankenship's Method in the RSA Cryptosystem to Test Information Security

Najalia Singh
Valley Stream Central High School, Town of Hempstead, New York State, United States of America

The RSA cryptosystem picks keys and uses large prime numbers as an essential tool to allow me to encrypt and decrypt messages. In my research I studied certain linear Diophantine equations and showed how they are used in RSA to encrypt and decrypt information. I also used a technique created by Blankenship, that is rooted in linear algebra and employs matrix row reduction techniques, to efficiently calculate encryption and decryption keys. I employed the Maple software to simulate data and illustrate RSA in action. Using an application of Blankenship's Method enabled me to calculate the decryption key. I then illustrated a way to break RSA for small primes and identified the weaknesses in RSA for larger primes.

Category
Pick one only—
mark an "X" in box
at right

Animal Sciences	☐
Behavioral & Social Sciences	☐
Biochemistry	☐
Biomedical & Health Sciences	☐
Biomedical Engineering	☐
Cellular & Molecular Biology	☐
Chemistry	☐
Computational Biology & Bioinformatics	☐
Earth & Environmental Sciences	☐
Embedded Systems	☐
Energy: Chemical	☐
Energy: Physical	☐
Engineering Mechanics	☐
Environmental Engineering	☐
Materials Science	☐
Mathematics	■
Microbiology	☐
Physics & Astronomy	☐
Plant Sciences	☐
Robotics & Intelligent Machines	☐
Systems Software	☐
Translational Medical Sciences	☐

1. As a part of this research project, the student directly handled, manipulated, or interacted with (check ALL that apply):

   ☐ human participants ☐ potentially hazardous biological agents

   ☐ vertebrate animals ☐ microorganisms ☐ rDNA ☐ tissue

2. I/we worked or used equipment in a regulated research institution or industrial setting: ☐ Yes ■ No

3. This project is a continuation of previous research. ☐ Yes ■ No

4. My display board includes non-published photographs/visual depictions of humans (other than myself): ☐ Yes ■ No

5. This abstract describes only procedures performed by me/us, reflects my/our own independent research, and represents one year's work only ■ Yes ☐ No

6. I/we hereby certify that the abstract and responses to the above statements are correct and properly reflect my/our own work. ■ Yes ☐ No

This stamp or embossed seal attests that this project is in compliance with all federal and state laws and regulations and that all appropriate reviews and approvals have been obtained including the final clearance by the Scientific Review Committee.