Najalia Singh

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

Category: Mathematics

Rationale

Technology is widely impacting how society shares information. Even though technology has provided a faster and efficient way to exchange information between others, it makes information vulnerable to hackers. Therefore, applying mathematics to cryptography will preserve exchanged information through technology. Cryptography requires the sender and recipient to apply their mathematical knowledge to create schemes and formulas to allow communication through coding. This will secure information from hackers without a specific key. Early encryptions are the Caesar shift cipher and the Substitution cipher which are private-key systems. The Caesar shift and the Substitution ciphers can be readily broken. In 1977, the RSA public-key cryptosystem was invented by Ronald Rivest, Adi Shamir and Leonard Adleman. RSA is used to encrypt and decrypt numerical messages. To send text in English, one can assign the letters A to Z the numbers 00 to 25. As an example, the word ENCRYPT will be mapped to the string of numbers 04130217241519. In RSA I must be able to pick the keys and learn how to encrypt and decrypt messages. The important aspect of RSA is that it is secure once we make prudent choices for the keys. In this system we use Diophantine linear equations to encrypt messages and provide an effective way for anyone to communicate information secretly with their intended receiver in a public key system. An important technique that is used in our calculations to solve Diophantine equations is Blankenship's method which involves row reducing matrices and extracting solutions. This technique gives us the ability to compute the private key and other parameters. This is an efficient method that is readily accessible.

Hypothesis

It is easier to find the decryption code using Blankenship's Method with large prime pairs in RSA's code. In RSA we have a hash function that allows us to encrypt data easily but proves difficult to decrypt (the inverse process) within a reasonable time.

Research Question

1. How will RSA encrypt and decrypt messages for various prime pairs p and q using the Blankenship Method to decide on the best choices by simulating various examples?

Expected Outcomes

Establish bounds on the primes p and q that make RSA effective and secure using Blankenship's Method.

Methods

Simulate message encryption and decryption for different prime pairs and use techniques from linear algebra such as Blankenship's method to compute the keys. The software that will be used for the RSA cryptosystem and the Blankinship Method is Maple.

Safety Precautions

This project will have no safety risks or precautions.

Data Analysis

Compare the ease with which codes can be broken for various prime pairs (p, q) for small and large pairs to gauge how secure RSA can be.

Bibliography

1. Menezes, A J, Oorschot P. C. Van, and Scott A. Vanstone. (1997) *Handbook of Applied Cryptography*. CRC Press

2. Trappe, W, Washington, C. W (2002) *Introduction to Cryptography with Coding Theory, 2nd Ed*. Pearson

3. Erickson, M, Vazzana A (2008), *Introduction to Number Theory*, CRC Press

4. Rosen, K H (2011) *Elementary Number Theory and its applications*, *6th Ed*. NJ, Pearson,

5. https://simple.wikipedia.org/wiki/RSA_algorithm

No Addendums Exist