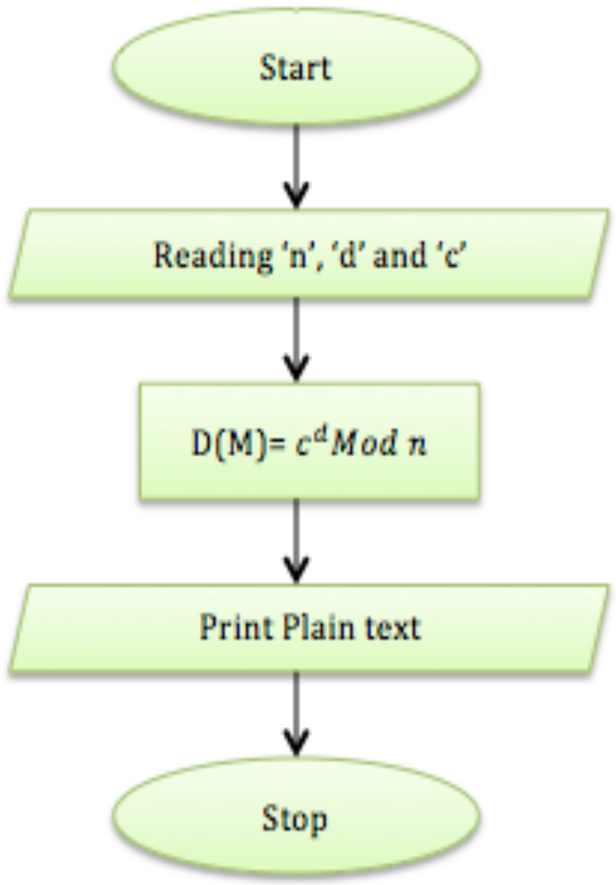
Analytical Comparison of RSA and Chinese Remainder Theorem

Electrical Engineering and Computer Science
Washkewicz College of Engineering
Cleveland State University

Students: Ankur Mantri
Hiral Makwana
Parita Parekh
Advisor: Dr. Abdul Razaque

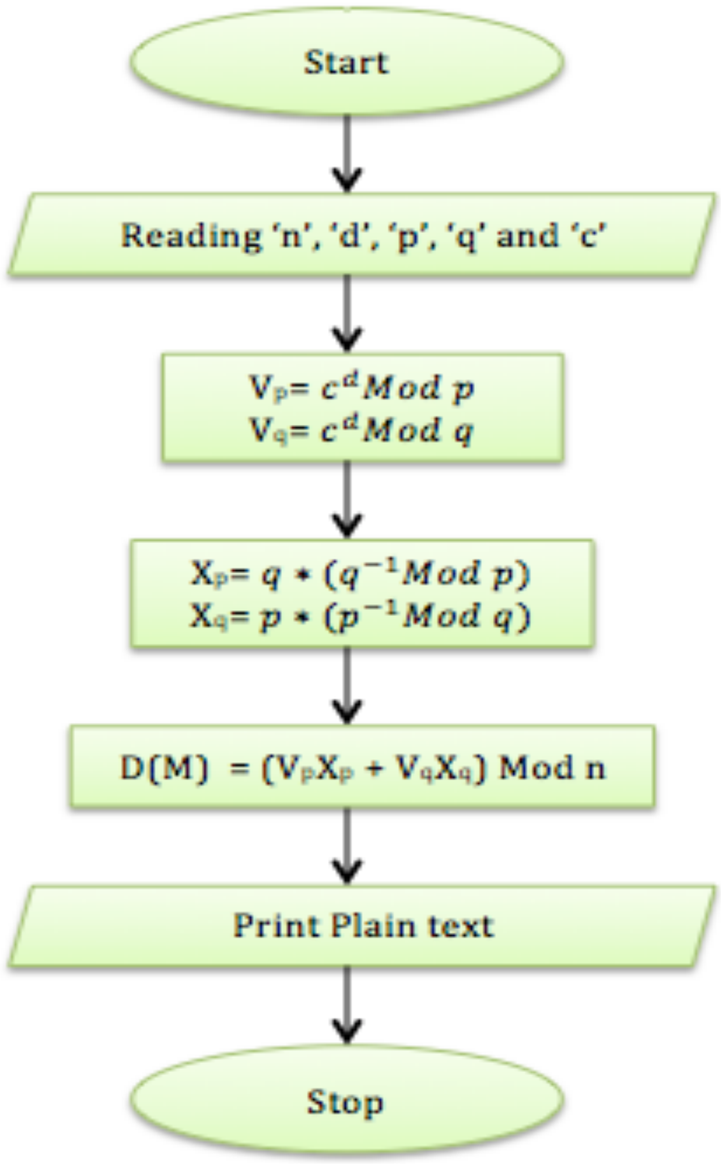
Abstract: RSA decryption is relatively slow as compared to RSA encryption. To enhance it's performance during decryption, we use an alternative approach, a mathematical theorem, called Chinese Remainder Theorem (CRT). CRT minimizes the mathematical computation to large extent, thus improving the speed. CRT is well known for improving RSA's decryption speed, but it has some drawbacks. The goal of this research paper is to address this topic in more detail by doing an analytical comparison and stating both advantages and disadvantages of CRT when used for RSA decryption.

RSA Decryption



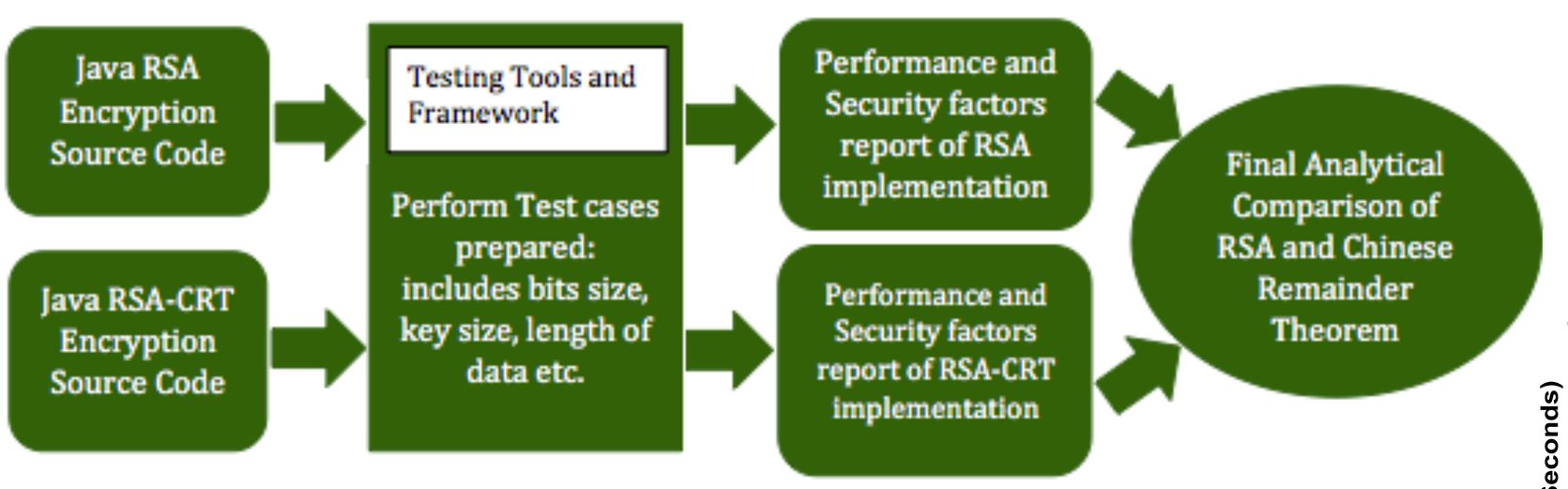
c = Cipher text
D(M) = Plain text

RSA Decryption using CRT



c = Cipher text
D(M) = Plain text
p & q are the prime factors of modulus n

Implementation:



Significance: This research paper would serve as the foundation for further research work for RSA decryption using CRT. In addition to that, it will also address situations where CRT decryption is faster and beneficial to use by stating it's advantages and disadvantages.