An application of Number Theory to RSA Cryptosystem

Sabina Hajimuradova
Department of Computer Science
French-Azerbaijani University
Baku, Azerbaijan
sabina.hajimuradova@ufaz.az

ABSTRACT

RSA (Rivest-Shamir-Adleman) is a public key encryption technique used by modern computers and is considered as the most secure way of encryption. In this work, I explored the RSA Encryption method. I explained each concept related to RSA algorithm and gave an illustration of how the RSA algorithm works using much smaller prime numbers. Then, I verified that RSA works for short messages. This provides a better understanding of the encryption method. To completely understand RSA encryption method, I studied the mathematical theory behind RSA method. To do so, I proved RSA encryption method using number theory and presented these proofs in the report. Based on the mathematical knowledge, I developed a Java program to demonstrate how RSA encryption and decryption works.

KEYWORDS

Cryptography, Encryption , Decryption, Symmetric Key, Asymmetric Key, Number Theory, Java

INTRODUCTION

Data packets sent on the Internet pass through public networks, which makes it possible for us to access these packets. While highly confidential information is transferred on the Internet, security of personal data has become a major concern for people across the globe. It is not safe to do business or communicate on the Internet without protecting such information. The data transferred over public networks is extremely sensitive for the client and therefore must be protected in an approtiate way. Information security can be provided with the action of eliminating threats such as eavesdropping, identity theft, information extortion, and the main tool used for this purpose is called Cryptography.

Modern Cryptography is about using computers and mathematical functions to provide a more safe and secure representation of the data. In other words, it is based on complex mathematics and offers several important information security services such as authentication, confidentiality, integrity and non-repudiation. Modern cryptography relies on cryptographic keys, which is a piece of information used in combination with an algorithm for transforming plaintext into ciphertext (encryption) and vice versa (decryption). Based on the type of keys used, cryptography divides in two main branches: symmetric cryptography and asymmetric cryptography. [1]

The most important and famous assymetric key cryptographic algorithm is RSA, which have accepted and wisely used at present time. In this study, I aim to answer the following research questions.

I. **How does the RSA Algorithm works?** This part is going to include different concepts you will have to get your head around before I can explain how it all fits together. I will be simplifying separate processes involved in computing the public and private keys used in the encryption and decryption processes. A complete example will be presented, but I'm going to work with small prime numbers so it'll be easy to follow arithmetic. However, we have to keep in mind that in a real RSA encryption system prime numbers are extremely huge.

II. **How the RSA Algorithm works correctly?** To prove the correctness of RSA, one simply has to state that ciphertext produced from message must be equal to original message when decrypted. I use the Fermat's Little Theorem [2] to prove that RSA works correctly and accurately. Mathematically I show that applying the encryption function and the decryption function successively produces the identity function.

After the explanation of the terms and processes that are used in RSA Cryptosystem, I provide a Java program to implement RSA algorithm. This Java program allows me to successfully encrypt and decrypt any messages.

FUTURE WORK

In the future, I would like to study different approaches used to attack the RSA algorithm. Futhermore, evaluate some common attacks on RSA and its variants and provide some necessary precautions to safeguard against such attacks.

REFERENCES

[1] J. Katz and Y. Lindell, Introduction to Modern Cryptography, Chapman & Hall/CRC Press, 2007.
[2] J. Stillwell, Numbers and Geometry, Springer, 1997.