RSA: Cryptography

Brandon Hohimer, Ivanna Villalba, Kristin Wohlfarth

Saint Leo University

Abstract

RSA Cryptography is used a lot in computing and modern technology. The reason it was brought up was to enforce computing laws and to ensure more advanced security. The system does this by using public keys and basically works on the system by factoring numbers to come to a conclusion. It is the first system to use the public key system and the article that we chose expands on its uses and other facts.

The article we chose explains into detail how RSA works and what are its main benefits and problems. As we read further we saw that a common problem with RSA is called the RSA problem which is when someone finds out the prime numbers of the encryption that RSA was trying to keep secret. It is highly controversial as for whether this problem is harder than to actually find prime numbers or not. The other important factor that was found when delving into this article was the idea of private keys.

The article split this idea into two parts; a and b. A showed the positive integer and b showed the private exponent. We also chose to explain the recent criticisms that RSA faced and the response they generated from the technological community. When explaining this, we will show exactly was criticized and how it affected the views that people currently have about the system. In addition to this, we will mention how secure RSA is today and the future of this cryptology system in the changing world of technology.

In conclusion, our topic that will be discussed in this paper will be the RSA cryptography and the article we chose to help us expand on it will introduce many of the important concepts that relate to understanding this complex system as well as the controversies that this system has faced.

RSA: Cryptography

Introduction

RSA Cryptography is one of the first public-key cryptosystems, which are a collection of cryptographic algorithms that are used to implement a security service. The acronym RSA stands for Rivest-Shamir-Adleman, the three computer scientist that invented this encryption in 1977. The inventors managed to create this algorithm at Massachusetts Institute of Technology, one of the world's most renown technology institutes. The main reason for this cryptosystem is to protect data; mostly highly sought after data. The RSA system protects this highly sensitive data by having key tables. In this paper, we will go on the search for the discovery of the best algorithms that are used for the cryptography system and discuss how they are used. We will then go into detail about the specific algorithms and address how the tables that are made by using prime numbers which will lead us to the discussion of how we use prime numbers to figure out the rest of the numbers.

RSA key tables are what primarily make the system function properly. The prime numbers that are used for the tables are paramount to the algorithm and, therefore, must be kept secure and hidden from anyone not authorized to access it. In a situation where someone were able to get the exact primary numbers needed for the algorithm, this could lead to a major security breach that would potentially allow the intruder to get sensitive information he or she should not have. A security breach like this would be detrimental to a company as customers would not only lose faith in the security of the system but would hold the company itself accountable for the loss of privacy and information.

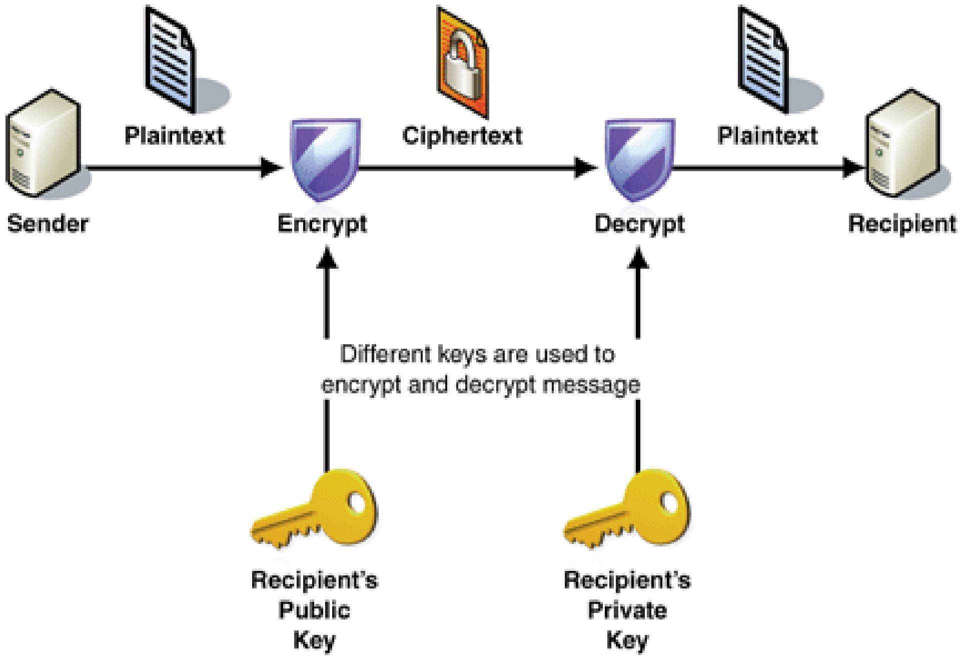
Even though the RSA is a well-designed algorithm, the system performance can be very slow. With the algorithm performance being sluggish, this leads it to have a major disadvantage because it cannot be used for certain data encryption. In this paper we will focus on the data that the algorithm can actually be used on and we will furthermore explain descriptively why the RSA system is so slow.

As with most algorithms that have been developed and implemented over the years, certain concerns can be developed over time about its resilience to withstand the changing technological environment as well as how the overall structure is keeping up with security demands. In this paper, we will address these concerns to address how the RSA cryptology has withstood the dynamics of the new age of technology. This will then lead to the discussion of the recent criticisms of the RSA cryptology algorithm and how that was addressed by the cryptology and technological community. In 2012, there was a research paper released that aimed it's criticisms directly at RSA cryptology which called the algorithm "flawed" and began to address how a user of the algorithm would experience it's lack of functionality. Further analysis of this finding will be discussed in depth as well as the response that the RSA had to this concern about the algorithm.

History of RSA

RSA not only has a great reputation for its Asymmetric key algorithm, but also has a very rich unique history. RSA was developed in 1970. It had a few problems when it first came out but were later resolved with multiple solutions. RSA Cryptography was worked on by a lot of great minds who later went on to work on other great computation problems. There was one main function that was used and other ideas worked around it. Multiple people with diverse backgrounds all worked on this together to come up with one unique very essential tool to later be known as a great breakthrough in cryptography.

RSA Cryptography is an Asymmetric key algorithm. This basically means that that there are two keys for the cryptography. This was one of the first for its time. A man named Diffie, who was a student at MIT was one of the first to recognize both the problems in RSA Crytopgray and how to solve them. He also was one of the first to realize the potential of the APRANet before it later turned into the internet. "Whitfield Diffie, a former mathematics student of MIT, was the one to come up with the revolutionary idea for this scheme. Early in the 1970s Diffie had realized the potential of the so-called APRANet, which later was to develop into the Internet, as well as the need for keeping information secret, for example in money transactions, in such a net" (Jankavist p.4)



"One of the oldest problems in cryptography is that of distributing the private encryption and decryption key between two parties. A solution was finally found in 1975 by a small group of cryptographers at Stanford University. Actually they solved the problem in two different ways, first by coming up with a safe way to generate a common integer, that is, the key, between two parties; and second, by proposing a totally new system of cryptography, public-key cryptography, which we shall deal with here”(Jankvist p.3). Here the author explains how RSA originally had a problem and later was solved in multiple ways. A safe way and a regular way. This was a huge breakthrough for RSA cryptogram because it gave the algorithm a lot more independence and confidence.

There were many implications with the history of RSA. Different dates in time yielded many steps in the algorithm’s history: “As an interesting twist to the history of public-key cryptography it was made public in 1997 that the British Government Communication Headquarters (GCHQ) Volume 23 (2008) 159 already knew of the system back in 1969—see Singh (1999, 279–292). During the 1960s the British military had been playing with the idea of equipping soldiers with radios in order for them to be constantly in contact with their superiors”(Jankvist p.6 160) Here the author explains how this system was worked on ven earlier than most people thought. He also explains how it was used for military movement and how secret it was tried to kept for that reason.

Overall RSA cryptography is a very unique algorithm with many implications with an even ore diverse history. The algorithm came a long way from 1970 to what it is today. The algorithm works on a prime number degree which makes it a tedious computation to deal with but the benefits of this system most certainly outweigh the cons throughout computer and human history.

How it Works

To understand RSA Cryptography, you need to first understand what and algorithm is. An algorithm is a set of instructions that a computer uses to complete a task. RSA is a set of two algorithms, key generation and RSA function Evaluation. Since RSA is asymmetric it has two keys, one that is public and one that is private. These two keys are what makes RSA so great, because you need one key to unlock another as mentioned in the introduction part of this paper.

The key generation algorithm is used to create a public and private key. There is a five-step process to create both keys. The first step is to generate two large prime numbers. The second step is to find the modulus of both numbers. The third step is to calculate the totient. The fourth step is to create the public key. The fifth step is to create the private key. Both private and public keys will be created after key generation does all these steps.

When generating a prime number, it is paramount to the security of the algorithm that both numbers be very large and be far apart from one another. Best practice is to make it around 1024 digits long. So, the algorithm picks a number and test to see if it is prime, if the number is prime it then picks another prime number, if it is not prime it adds one and test to see if it is prime again; it keeps doing this until it has two prime numbers. To test if the number is prime it can use an algorithm called the Rabin-Miller primality tester. This tester is optimal because it is extremely fast and will tell the RSA algorithm if the number is prime or not.

$P = 53 \qquad Q = 59$

Once key generation is done there should be two prime numbers. RSA uses a composite number that is called n this is the modulus of the two prime numbers. Modulus is calculated when multiplying both prime numbers together. Once the modulus is calculated RSA moves to the third step: calculating the totient. Totient is the count of the number of elements that have their greatest common divisor (gcd) with the modulus equal to one. The symbol for totient is ϕ(n). So, to find the totient you just do (p – 1) * (q -1), whereas p is prime number one and q is prime number two.

$$\phi(n): (53 - 1) * (59 - 1) = 3016$$

The public key has two variables n and e. The n variable is the compound number that was made when taking the totient of the two prime numbers. The e is a small prime number exponent that you need to make the public key. The exponent you chose must follow these three rules: must be an integer, cannot be a factor of n, and e needs to be greater than one and less than the totient of n, the equation is $1 < e < \phi(n)$. When it comes to choosing e, it is recommended to choose smaller numbers, so that it is more efficient when encrypting. The higher the number the less efficient it will be.

$$n = 3016 \qquad e = 3$$

Now that the public key has been generated, there needs to be a private key to complete RSA cryptography. As with the public key the private key is made up of two variables d and n. The d variable is the private key where n is the compound number chosen before. Public key uses a gcd of 1 with respect to the modulus, whereas the private key uses the multiplicative inverse of the public key. So, this means that d can be found by multiplying 2 by the totient of n and adding 1, then dividing by e, the equation is $(2(\phi(n)) + 1)/e$. Once this equation is completed the private key (d) will be generated.

$$d = \frac{2*(3016) + 1}{3}$$

$$d = 2011$$

The last thing that needs to be done is the RSA function evaluation. This is when plaintext is converted into cipher text, or when cipher text is reverted to plaintext. Down below I will show a sample encryption (which will be represented by the variable c) and decryption with the numbers from the previous diagrams. In this example, I will encrypt the word be then decrypt it. The letter b is number 2 and the letter e is 5, so both equal 25.

$$c = 25^{e} \bmod n$$

$$3117 = 25^{3} \bmod 3127$$

$$= c^{d} \bmod n$$

$$25 = 3117^{2011} \bmod 3127$$

Criticisms of RSA

In February of 2012, the technology community was in an uproar as a new research paper that was released had now addressed concerns about the RSA encryption algorithm and slammed the algorithm entirely. The major concern that the research paper brought up was how the algorithm would fail when it had to generate random numbers for the encryption keys. It's important to note that the paper had proclaimed that this meant the algorithm was "fundamentally flawed" and that the system should not be used any longer as it could result in an enormous amount of errors or the event of the protocol completely falling apart and causing a major security breach. This paper, titled "Ron was wrong, Whit was right", slammed the RSA inventors for not acknowledging the potential for a security breach in their algorithm where the system didn't even manage to give security to "12, 720 different RSA moduli" (Messmer 2012).

The creators of the paper did not hold back on their opinion and research about the RSA system and made it so that the errors that were found wouldn't be ignored any longer as they posed a serious risk to the users of the system. What baffled most of the technological community was that this problem was something the industry had noticed before and they had even acknowledged its existence in the algorithm numerous times. In fact, the problem of the number generation in this algorithm was not recognized as a problem at all since another major tech company (Intel) was planning on emphasizing the random number generation factor to form more secure keys through in the development of a new chip for their computers. The fact remains that there was a problem not acknowledged seriously by the technical community within the RSA cryptology system and the research paper that brought it into the forefront of the community.

After the release of the paper, a statement had come from RSA which did not undermine the issue that was brought up but it also stated how the RSA supported “security tied to millions of public X.509 certificates that they collected across the web” (Messmer 2012). They went on to say that this information is important because throughout all the securities they had collected, the RSA algorithm system managed to provide 99.8% security. However, the RSA was kind enough to also mention that they welcomed the new information and insight that the researcher who created the paper had shown but they still felt that the algorithm had been misunderstood. For example, they never took into consideration the capability of the algorithm and how it has withstood the quickly changing world of technology today. RSA mentioned how the system had been providing a secure enough environment for many of their users and has stayed strong when other concerns were brought about the system throughout the years.

On the contrary, RSA also said in their statement that they know how important this aspect of the algorithm is and they ensured that in order to make the RSA system is properly functioning on their standards, the cryptographer must take care when implementing the algorithm into a device. The response to the statement that RSA released was mostly positive and met with support from the community. There are even some who completely reject the released paper itself as they believe that it should not had be acknowledged by the community in the first place. Some, however, just believe that the paper addressed something that should have been addressed but readers should not believe the thesis of the paper. It’s safe to say that RSA won’t be going anywhere any time soon but it’s also important to note that there are flaws in the system and, like any other system, it is not the completely perfect but is a well-designed cryptography system.

In conclusion RSA cryptography has come a long way. There are many benefits with it and have had many implications since it first came out. The algorithm that is used is highly ambiguous and uses a prime number key system. There is a lot of rich history with the algorithm and had been worked on by a lot of great minds. Without this algorithm computing would not be what it is today.

References

Messmer, E. (2012, February 16). RSA brushes off crypto research findings that RSA algorithm is flawed; Plus, researcher Dan Kaminsky expresses skepticism about study conclusions. Network World. Retrieved from https://www.networkworld.com/article/2185971/security/rsa-brushes-off-crypto-research-findings-that-rsa-algorithm-is-flawed.html

PKCS #1: RSA Cryptography Specifications Version 2.2. (n.d.). Retrieved from https://tools.ietf.org/html/rfc8017

Rouse, M. (2014, November). What is RSA algorithm (Rivest-Shamir-Adleman) - Definition from WhatIs.com. Retrieved from http://searchsecurity.techtarget.com/definition/RSA

Thomas Jankvist, U. (2008). A teaching module on the history of public-key cryptography and RSA. BSHM Bulletin: Journal Of The British Society For The History Of Mathematics, 23(3), 157-168. doi:10.1080/17498430802304032

Walter, C. (1993). Systolic Modular Multiplication. IEEE Transactions on Computers, 42(3), 376-378. doi:10.18411/d-2016-154