# **An Analysis on Advanced Cryptography Standard RSA Algorithm for Information Security**

Tanvir Hossain; ID- 20103131

Md. Mahidur Rahman; ID-20103104

A Thesis in the Partial Fulfillment of the Requirements

for the Award of Bachelor of Computer Science and Engineering (BCSE)



Department of Computer Science and Engineering

College of Engineering and Technology

IUBAT – International University of Business Agriculture and Technology

Fall 2023

**An Analysis on Advanced Cryptography Standard RSA Algorithm for Information Security**

Tanvir Hossain; ID- 20103131

Md. Mahidur Rahman; ID-20103104

A Thesis in the Partial Fulfillment of the Requirements for the Award of Bachelor of Computer Science and Engineering (BCSE)

The thesis has been examined and approved,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Prof Dr. Utpal Kanti Das**Chairman & Professor   
Dept. of Computer Science and Engineering  
IUBAT – International University of Business Agriculture and Technology

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**[Rashedul Islam](http://cse.iubat.edu/rashedul-islam/)  
Assistant Professor & Coordinator**  
Dept. of Computer Science and Engineering  
IUBAT – International University of Business Agriculture and Technology

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mahmudul Hasan

Supervisor and Lecturer  
Dept. of Computer Science and Engineering  
IUBAT – International University of Business Agriculture and Technology

## **LETTER OF TRANSMITTAL**

15th January, 2022

The Chairman

Thesis Defense Committee

College of Engineering and Technology - CEAT

IUBAT- International University of Business Agriculture and Technology 4

Embankment Drive Road, Sector- 10, Uttara Model Town

Dhaka-1230, Bangladesh

**Subject:** Letter of Transmittal.

Sir,

With due respect, We would like to inform you that it is a great pleasure and a great pleasure for us to submit this report entitled **“An Analysis on Advanced Cryptography Standard RSA Algorithm for Information Security”** to complete my thesis course.

It was a great opportunity for us to work on this research to make our theoretical knowledge more realistic. We now look forward to your kind commentary on this performance report.

We will always be very grateful to you if you kindly go through this report and check our performance.

Your sincerely,

\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Tanvir Hossain Md. Mahidur Rahman

20103131 20103104

## **STUDENT’S DECLARATION**

We hereby declare that the thesis project entitled **“An Analysis on Advanced Cryptography Standard RSA Algorithm for Information Security ”** submitted to the International Universityof Business Agriculture and Technology, is a record of an original work done by us under the guidance of **Mahmudul Hasan,** Lecturer, Dept. of Computer Science and Engineering, International University of Business Agriculture and Technology, and this project work is submitted in the partial fulfillment of the requirements for the award of the degree of BCSE in CSE. Any reference to work done by any other person or institution or any material obtained from other sources have been duly cited and referenced. This report contains no plagiarism or falsification of any data.

Thanking you,

\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

Tanvir Hossain Md. Mahidur Rahman

20103131 20103104

## **Supervisor’s Certification**

I am **Mahmudul Hasan,** Lecturer, Dept. of Computer Science and Engineering, International University of Business Agriculture and Technology State that Tanvir Hossain -20103131 and MD Mahidur Rahman-20103104 has performed their undergraduate thesis work under my supervision. They carried out the research of the project “**An Analysis on Advanced Cryptography Standard RSA Algorithm for Information Security”** from semester FALL’2022 to Fall’2023.

The work submitted by them is genuine and original work to the best of my knowledge.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Mahmudul Hasan**

Lecturer

Department of Computer Science and Engineering

IUBAT–International University of Business Agriculture and Technology

## **Abstract**

Cryptography is a key tool for safeguarding the authenticity, confidentiality, and integrity of sensitive data in the current digital environment. Cryptography is essential because it prevents unauthorized access to and theft of sensitive data like passwords, credit card numbers, and other personal information. The difficulty of using cryptography depends on many factors, including the chosen encryption method, the size of the key, and the computer power of the attacker. In 1977, Ron Rivest, Adi Shamir, and Leonard Adleman developed the public-key cryptosystem RSA (Rivest- Shamir-Adleman). RSA has had a significant impact on digital communication and security because of its capacity to transmit sensitive data securely over open networks. RSA enabled the development of several other cryptographic protocols and systems that are still in use today. Despite being the victim of a number of theoretical attacks, RSA remains one of the most used and trustworthy cryptographic techniques. Someone unearths a modified algorithm. But there are also other things lacking. Although RSA is a trustworthy and widely used cryptographic method, it is not without limitations and weaknesses. Here are a few examples of potential RSA drawbacks. the following: Quantum computing, Key management, Key length, Computational complexity, Vulnerabilities. Basically, our main worry is the key length. The key length has a significant impact on the RSA encryption scheme's security.

The key length affects both the strength of the encryption and, therefore, the security of the encrypted data. The encryption and decryption keys were also generated using the CRT approach using the n primary integers. The Chinese Remainder Theorem (CRT) is a method for reducing the quantity of modular multiplications needed, which quickens the RSA decryption computation. The number of primary numbers (i.e., two) is necessary for generating the encryption and decryption key using the CRT approach in order to allow the Chinese Remainder Theorem to be employed to speed up the RSA decryption process. In addition, because we may create any number of encryption keys, the decoding process will be speedier than in earlier tests.

## **Acknowledgments**

## First, we would like to thank our Supervisor Mahmudul Hasan, Lecturer Dept of Computer Science and Engineering, International University of Business Agriculture and Technology without his guidance we couldn’t come this far. He guided us, helped us, and motivated us which helped us to continue our journey through this whole thesis project. Then we would like to thank Computer Science and Engineering department of international university of Business Agriculture and Technology for giving us the opportunity to conduct the thesis work. Also, we would like to thank ART203 course instructor Ms. Moumitu Tasnim, Lecturer, Dept. of Computer Science and Engineering, International University of Business Agriculture and Technology for giving us guidance on writing the report in support of our thesis. Finally, we would like to thank all our friends, family members and faculties who supported us and helped us whenever and wherever we needed them.

**TABLE OF CONTENTS**

**LETTER OF TRANSMITTAL** i

**STUDENT’S DECLARATION** ii

**Supervisor’s Certification** iii

**Acknowledgments** iv

**Abstract** v

**LIST OF FIGURES** v

**LIST OF TABLES** vi

**Chapter-1** 1

**Introduction** 1

**1.1 Background** 1

**1.1.1** **Symmetric key Cryptography:** 2

**1.1.2** **Asymmetric key Cryptography:** 3

1.1.3 **RSA Algorithm:** 4

**1.1.3** **CRT:** 4

**1.2** **Motivation:** 5

**1.3 Problem Statement:** 6

**1.4 Objective** 6

**Chapter-2** 7

**Literature Review** 7

**Chapter-3** 12

**Research Methodology** 12

**3.1 Research Question:** 12

**3.2 Description of research methodology:** 12

**3.3 Work Flow:** 13

**3.4 Existing Techniques** 14

**3.4.1 RSA Algorithm** 14

**3.4.2 Proposed Formulation of RSA with CRT:** 15

**Chapter-4** 17

**Result and Discussion** 17

**4.1** **Key Generation Comparison:** 17

**4.2 Decryption Time Comparison:** 20

**Chapter-5** 22

**Conclusion** 22

**Reference:** 24

## **LIST OF FIGURES**

**Fig 1.1** Symmetric Cryptography 2

**Fig1.2.** Asymmetric Key Cryptography 3

Fig 3.1: Work Flow of Research Methodology 13

Fig 4.1 : Key Generation 19

Fig 4.2 : Key Decryption 21

## **LIST OF TABLES**

Table 4.1 Key Generation Time …………………………………………….......................... 2

Table 4.2 Decryption time …………………………………………........................................ 6

## 

## **Chapter-1**

## **Introduction**

#### **1.1 Background**

By turning plaintext—unencrypted information—into cipher text—encrypted information—using mathematical algorithms and protocols—cryptography is the discipline of protecting communication and information. In order to prevent unwanted access, manipulation, or theft, cryptography aims to guarantee that only authorized parties may access and understand the data.

Keys, protocols, keys, and decryption algorithms are only a few of the elements that make up cryptography. Using a key, encryption algorithms convert plaintext into cipher text, while decryption algorithms carry out the opposite operation, turning cipher text back into plaintext using the same or a different key. To prevent unwanted access, keys are employed to manage the encryption and decryption process and are kept secret.

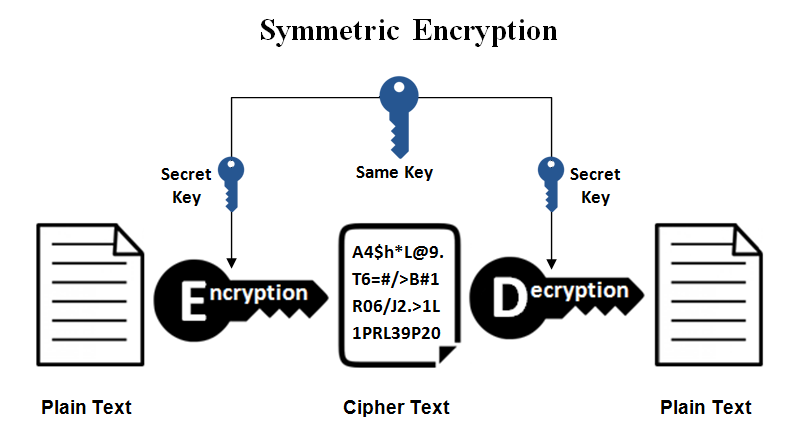
Many facets of contemporary life, such as e-commerce, online banking, secure texting, and information storage, depend heavily on cryptography. Additionally, it is used to safeguard private data as well as business and state secrets. With constant research into novel algorithms and protocols to guarantee the security of information in the face of growing threats, cryptography is a topic that is continually developing.

When information is converted from plaintext (information that has not been encrypted) to cipher text (information that has been encrypted), a mathematical process known as a cryptographic algorithm is utilized. Particularly in the current digital era, cryptographic algorithms are crucial for safe communication and data storage.

The Caesar cipher was historically the oldest known cryptographic technique. Julius Caesar used it to send his generals covert communications. The Caesar cipher generates the cipher text by moving each letter of the alphabet a predetermined number of times.

Symmetric key cryptography and asymmetric key cryptography are the two primary divisions of contemporary cryptographic algorithms.

* + 1. **Symmetric key Cryptography:**

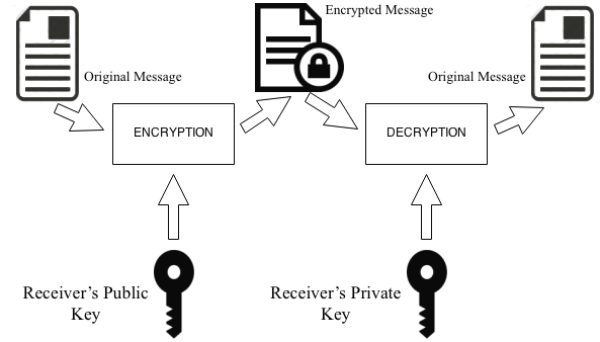
****Same key is used for both encryption and decryption. Data Encryption Standard (DES), Advanced Encryption Standard (AES), and 3 Data Encryption Standard (3DES) all are symmetric cryptography

**Fig 1.1** Symmetric Cryptography

Both sender and receiver side has one key that’s why attacker easily attack the system.

* + 1. **Asymmetric key Cryptography:**

Asymmetric key cryptography is also known as public key cryptography. Two different keys are used in asymmetric encryption. It's commonly used for secure communication, digital signatures, and key exchange. RSA is an asymmetric key.

****

**Fig1.2.** Asymmetric Key Cryptography

Public key is used for encryption the data and private key used for decryption the data. It is more secure because it has a two different key that’s why RSA algorithm famous for worldwide because RSA is a public key algorithm.

1.1.3 **RSA Algorithm:**

Rivest-Shamir-Adleman developed by this RSA algorithm in 1977. Secure email, online banking, and SSL/TLS encryption for secure web browsing are just a few of the applications that employ RSA to protect communications, digital signatures, and key exchanges. RSA work as a public key cryptography when sender send a plaintext that time both sender and receiver has public key. Receiver send his public key for encryption the plaintext after complete encryption sender send a cipher text to receiver. Cipher text means when we do encryption the plaintext that plaintext convert any other language, code, symbol, etc. If third party see the cipher the cipher text they cannot understand what are plaintext. Receiver receive the cipher text then receiver has won private key and this private key use for decryption the cipher text receiver see the original plaintext.

One issue has RSA algorithm In contrast to RSA encryption, RSA decryption typically takes a long time. Experts and academics suggest using the Chinese Remainder Theorem (CRT), a modulo-based mathematical theorem, to boost decryption efficiency. CRT greatly reduces the amount of numerical computation required, increasing speed.

* + 1. **CRT:**

The Chinese Remainder Theorem, often known as CRT, is a mathematical concept and method used to number theory and computer technology. It has several uses, including in the realm of cryptography, and is especially helpful for accelerating modular arithmetic computations. The CRT offers a means to divide a modular arithmetic issue into smaller, easier-to-manage sub problems.

**Application of CRT:** The Chinese reminder theorem has several application in various field. Some common applications of CRT are-

1. **Cryptography:** The RSA cryptosystem uses CRT to accelerate the decoding process. In RSA, exponentiation modulo two large prime numbers is required for the private key procedure. By conducting exponentiation modulo each prime individually and then merging the results using the CRT, CRT enables faster computing.
2. **Error Detection and Correction:** Error-correcting codes like Reed-Solomon codes require CRT. These codes are used in data storage systems, such as CDs, DVDs, and QR codes, to identify and correct errors that could happen when data is being transmitted or stored.
3. **Computer Graphics:** Colors in computer graphics are represented by CRT. Colors are commonly represented in the RGB color model as mixtures of the three fundamental colors (red, green, and blue), each with its own modulus. Combining these color elements to get the final color is made easier by CRT.
4. **Number Theory:** When using modular arithmetic to solve problems, CRT is a helpful tool in number theory.

CRT is a strong mathematical tool with applications in many areas, especially when modular algebra is involved, and it can greatly increase computer efficiency.

* 1. **Motivation:**

There are several motivations for cryptographic research, including:

* **Security:** The primary motivation for cryptographic research is to provide secure communication and data protection, which is critical in today's digital age. Cryptographic techniques are designed to prevent unauthorized access, manipulation, or theft of information, which is essential in ensuring privacy, integrity, and confidentiality.
* **Cryptographic attacks:** Cryptographic research is necessary to develop new algorithms and protocols that can resist or mitigate attacks, such as brute-force attacks, side-channel attacks, and quantum attacks. Cryptographic attacks are continually evolving, and researchers must stay ahead of these attacks to ensure the security of information.
* **Performance:** Cryptographic research is also motivated by the need to improve the performance of cryptographic algorithms and protocols. Efficient and fast cryptographic techniques are necessary for secure communication and data protection while maintaining the required level of security.
* **Regulations and Standards:** Cryptographic research is also necessary to ensure that cryptographic systems meet regulatory and industry standards. Standards such as FIPS (Federal Information Processing Standards) and ISO (International Organization for Standardization) ensure that cryptographic algorithms and protocols meet specific security requirements.
* **Emerging technologies:** As new technologies emerge, such as the Internet of Things (IoT) and cloud computing, there is a need for cryptographic research to provide secure communication and data protection in these new contexts.

Overall, cryptographic research is necessary to ensure the security, privacy, and confidentiality of information in today's digital age, as well as to stay ahead of emerging threats and technological advancements.

#### **1.3 Problem Statement:**

* Using a smaller number of prime number encryption can be break by the hacker.
* Weak encryption is that it poses a significant risk to the security of sensitive information, and efforts must be made to identify and mitigate it to ensure the safety of individuals and organizations.
* Get more time to decrypt a massage.
* Lack of using CRT method.

#### **1.4 Objective**

* To identify the lack of RSA problem.
* To identify the mathematical error for RSA algorithm
* Find out the reason for breaking the encryption key.
* To try to build a modified RSA algorithm where encryption will be more secure from the previous RSA algorithm

.

## **Chapter-2**

## **Literature Review**

Engr. Shaheen Saad Al-Kaabi at al. 2019 find out the following document gives a brief overview of various suggestions for improving the RSA algorithm and boosting its security. Some of these improvements include integrating the RSA algorithm with the Diffie-Hellman or ElGamal algorithms, changing the RSA method to include three or four prime numbers, storing generated keys offline, creating a secured RSA algorithm where the message can be encrypted using two encryption keys, etc.

To solve some of the significant security concerns found in the RSA method, Gupta and Sharma proposed a new hybrid encryption algorithm based on RSA and Diffie-Hellman. Whitfield Diffie and Martin Hellman created the Diffie-Helaman algorithm (DH) in 1976. The algorithm used on the internet to protect various communication methods is remarkable and vast. SSL, IPsec, and SSH are a few examples of such protocols. In order for two parties to safely exchange a shared secret over a public network, each participant has to have access to both their public and private keys. The primary goal of this proposal's combination of these two algorithms is to create a better and more secure cryptosystem by using the speed and security of the secret key system and the public key system, respectively.

By merging the RSA method with the ElGamal algorithm, Iswari has suggested improving the RSA algorithm once more. A well-known public key cryptography algorithm is ElGamal. It was first exclusively used for digital signing. It was later improved and changed to be used for both encryption and decryption. The ElGamal algorithm's security strength is dependent on how difficult it is to compute the discrete logarithm.

In the Author's suggestion, 256-bit prime numbers rather than the 1024-bit prime numbers utilized in the original RSA technique were employed to reduce the computing time needed for key production. Due to issues with factorization and discrete logarithm computation, RSA and ElGamal may be combined to retain security factors and complexity even when little bit prime numbers are employed. Due to issues with discrete logarithm computation and factorization, complexity is maintained even when little bit prime values are employed.

In order to enhance the performance of the conventional RSA algorithm when information is exchanged between two parties via a network, Patidar and Bhartiya additionally suggested a brand-new algorithm idea. The suggested update used a third prime integer to create a modulus n that is difficult for outsiders to break down. It also included an improved version of the RSA method. Before the procedure is started, the keys for the proposed system are stored offline. Compared to the conventional RSA, this results in an increase in the speed needed for encryption and decryption. For that purpose, two tables were created in a database engine to store the keys. The values of the first table are p, q, n1, and (n), whereas the values of the second table are e, d, r, e1, and d1. The process of getting values out of and into the database is shown in the following image. The idea of utilizing a database to store keys is still crucial since keys may be readily obtained if the system is compromised, even if this suggestion speeds up the encryption and decryption of the communication.

By removing the distribution of n, a large number whose factor, if determined, weakens the RSA method, Minni et al. have presented another safe approach.

Jaju and Chowhan updated the RSA method to include three prime numbers instead of two prime random numbers for calculating n and passing value of X instead of n in the public key and private key in an effort to speed up and strengthen the security of the procedure. Due to the following factors, the suggested method is thought to be safer than the original RSA from a security perspective: (1) The only way to get the common modulus n is to factor the three prime integers p, q, and r, which is a time-consuming and more challenging task for intrusion attempts. (2) When a factorization attack is made, it will be challenging to determine the concealed value of n since the value of X is sent in the public key rather than n. Compared to the RSA technique, the improved approach takes longer to encrypt and decode text, while addressing the security and key generation performance issues.

A modified and improved method based on the RSA public-key cryptosystem and employing four prime integers was also suggested by Thangavel et al. The values of E and D are determined by the value of N, a product of the four prime integers. Additionally, the calculation of E is indirect, necessitating the acquisition of the values of e1 and e2 in order to ascertain the value of E1. This contributes to lengthening the assault window. Only the value of n is maintained as a public and private component, which prevents an attacker with knowledge of n from discovering all the primes that serve as the foundation for calculating the value of N, and consequently, D, according to The system's complexity may be increased by using the parameter E1.

Using a method from the Java Big Integer Library, the improved RSA was developed. By employing random functions, the user may utilize this approach to define the prime numbers to be used or to decide the length of the bit to be used. The Big Integer Library "provides the operations for modular arithmetic, GCD calculation, primary testing, prime generation, bit manipulation, and a few other ad hoc operations". The creation of the key for the upgraded technique takes a little longer than the other RSA-based algorithms examined in this work, adding to the additional complexity needed to eavesdrop on a communication channel. Due to the usage of four prime numbers, this holds true for both the encryption and decryption processes. The degree of security in the improved system rises as the processing time grows. According to a security examination of the system, the upgraded system would take far longer to brute-force attack than conventional RSA schemes. This is because just the value of 'n' is known to the attack, but identifying E and D is required to determine the value of 'N,' making it difficult to defeat the system.

Thangavel et al.'s research has shown the suggested system's top-notch security and enhanced complexity for attackers. Because of this, it is more secure than the conventional RSA.

A novel hybrid security technique for RSA is proposed by Panda and Chattopadhyay in a different paper, where the calculation of the public key P and the private key Q relies on the value of N, where N is 64. The result of four reduced-size prime numbers is the International Journal of Network Security & Its Applications (IJNSA), Vol. 11, No. 3 (May 2019) [5]. This makes factorizing the variable N more difficult and hence boosts security Similar to what is suggested in the calculation of P is not straightforward, requiring that the values of p1 and p2 be ascertained in order to establish the value of P1. Additionally, when a factorization attack is performed, the value of M is masked by the distribution of the value of w rather than M in the public key.

An improvement to the conventional RSA technique is presented by Mathur et al. in their updated approach to RSA. The K-NN method, the use of prime numbers and exponential powers, the use of multiple public keys, and other techniques were all included in this improvement. The improved technique offers the functionality of verification on the sender and recipient sides as well. The suggested method's drawback is that it takes more time to encrypt and decode data than the original RSA

Islam et al. presented a modified RSA (MRSA) method in an effort to overcome various computation-related weaknesses in the RSA algorithm The improved approach used 'n' unique prime numbers for key creation. There are three distinct components to the private and public as defined in the MRSA. One of these parts is N, which is the product of the four huge prime integers w, x, y, and z that were chosen at random. The public key is made up of three parts on its own: e, f, and N. Components e and f are chosen at random from the group of three. The key generation function of the chime becomes more sophisticated as a result of this and the factoring of "N." Only the value of N is present in both the private and public keys out of all these values. This implies that the attacker cannot compromise the system with the number N alone, as 66He or she must figure out the values of all four more huge prime numbers International Journal of Network Security & Its Applications (IJNSA) Vol. 11, No. 3, May 2019. As a result, the attacker is unable to calculate the values of e and f. The private key, however, is made up of three distinct parts: d, g, and N.

Goel, (2017) suggested a unique RSA-based algorithm capable of repelling assaults that are frequent in RSA in an effort to overcome the vulnerability discovered in the RSA algorithm. This algorithm's major components are a double mod operation-based encryption using two private keys, a double mod operation-based decryption using two public keys, and the generation of the modulus value using more than two huge prime integers. The three aforementioned elements work to strengthen the message's security by lengthening the times for key creation, encryption, and decryption. It is more difficult to factorize the two huge public and private keys utilized in the dual modulus technique in order to obtain the private key.

Dharitri Talukdar1 at al. suggested the research focuses on the use of dynamic keys for data security while keeping in mind the significance of dynamic keys for safe data transfer. This involves the use of five prime integers in the RSA algorithm's upgraded variant to create an n-modulus that is difficult for attackers to break down. Using MATLAB12a, simulations of the findings have been accomplished.

## **Chapter-3**

## **Research Methodology**

#### **3.1 Research Question:**

* + - * How does the size of the RSA key impact the security of the encryption, and what key lengths are currently considered to be secure?
      * How does the RSA encryption algorithm work, and what are its strengths and weaknesses?
* How does the Chinese Remainder Theorem (CRT) impact the security and efficiency of RSA encryption, and what are its limitations?
* What are some future directions for research in RSA encryption, and how can the technique be improved or adapted to meet evolving security needs?

#### **3.2 Description of research methodology:**

This section discusses in detail the proposed RSA-CRT method, which is the modified version of the RSA algorithm. The motivation of RSA-CRT development is that it will run on the hardware or system with limited resources. RSA Cryptosystem implementation in a long key that is longer than 2048 bits to reach minimal security requirements hugely influences windows 10, ram-8gb. Based on the four main problems above, we conducted research method in Figure to develop an RSA-CRT algorithm model.

The current recommended key lengths for RSA encryption are:

* 2048 bits for general-purpose use
* 3072 bits for high-security use
* 4096 bits for extreme-security use

Our Method will be able to generate 4096 bits for extreme-security. These key lengths are based on current knowledge of the best-known attack methods and the computational power required to break the encryption.

It is important to note that the key size is only one factor in determining the security of RSA encryption. Other factors, such as the quality of the random number generator used to generate the key, the security of the implementation, and the potential vulnerabilities in the encryption algorithm itself, must also be considered. CRT method will help the decrease the decryption time.

#### **3.3 Work Flow:**

**Problem identification:**

\*Secure RSA Standard

\* Weak Encryption (Using small prime number)

**Literature Studies:**

\*Identifies relevant previous researches

\* Analysis the gap

Modified Standard RSA Algorithm based on CRT Method

Standard RSA Algorithm based on 2 prime number

**Proposed Algorithm:**

**\*Modified Standard RSA Algorithm**

**RSA-CRT Algorithm**

**Analysis RSA VS RSA-CRT algorithm**

Fig 3.1: Work Flow of Research Methodology

#### **3.4 Existing Techniques**

#### **3.4.1 RSA Algorithm**

R. Rivest, A. Shamir, and L. Adleman developed the RSA cryptosystem, which is the most used public key cryptosystem today. The first encryption and decryption algorithm was the RSA technique, which utilized modular multiplication and exponentiation. Both the plaintext and the cipher text for some n in the cipher block of the RSA method are integers between 0 and n-1. The use of prime numbers makes this technique one of the best asymmetric key cryptosystems for digital signatures, exchange keys, and data encryption blocks.

Asymmetric cryptography, sometimes referred to as public key cryptography, uses two different keys to encrypt and decode data. Keys are utilized, both public and private. The keys are created by applying a mathematical operation to two very large prime numbers. The public key should be shared among all participants in the system, but the RSA private key must be kept private. How hard it is to factor enormous prime numbers determines how secure the RSA cryptosystem is. Using just the information from the public key, which comprises the prime number n (multiplication of prime integers), the attacker cannot get the prime factor of n and, therefore, the private key. And as a result, the RSA algorithm is more secure.

**RSA Key Generation:**

1) Obtain two large numbers prime p and q of relatively same size such that their product n = pq is required bit length for example 1024.

2) Compute n = pq and φ(n) = (p − 1)(q − 1).

3) Choose a random integer encryption such that gcd[e, φ(n)] = 1 and 1 < e < φ(n).

4) Compute the exponent secret d in the range 1 < d < φ such that: ed = 1 mod φ(n).

5) The public key is (e, n) and the private key is (d, n).

The secret values are d, p, q and φ.

1) n is known as the multiplication or modulus of the prime numbers.

2) e is known as the exponent public or exponent encryption or just the exponent.

3) d is known as the exponent private or exponent decryption.

**RSA Encryption:** Sender does the following operations:

1) Determine the public key.

2) The plaintext message represented as a message positive as an integer positive.

3) Calculates the cipher text: C = Me mod (n).

4) Send to the receiver the cipher text.

**RSA Decryption:** The receiver does the following:

1) Use the private key (n, d) to compute plaintext: M = C d mod (n).

2) Extract the plaintext from the message representative M

#### **3.4.2 Proposed Formulation of RSA with CRT:**

As was previously said, RSA encryption is faster than decryption. This may be improved by creating a new algorithm that is comparable to the current one or by providing an alternative to it. CRT is an alternative method to RSA decryption that accelerates decryption. In RSA-CRT, two modular exponentiations are used instead of the one used in RSA decryption. Additionally, each replacement modulus and exponent in CRT is eight times larger than it was before. As a result, the speed of RSA decryption may be enhanced by up to four times using CRT.

**Algorithm:**

Consider two prime numbers ‘p’ and ‘q’ that is used in basic RSA decryption. This ‘p’ and ‘q’ is used in conjunction with ‘n’ and ‘d’, where ‘n’ and ‘d’ is also calculated like RSA decryption. Cipher text ‘c’ is obtained from RSA encryption. Then CRT is applied.

dp = d mod (p-1)

dq = d mod (q-1)

Qinv = q-1 mod p

Now,

M1 = cdp mod p

M2= cdq mod q

h = Qinv (M1 - M2) mod p

Decrypt cipher text M, which is a plain text, by using following equation.

M = M2 + hq

## **Chapter-4**

## **Result and Discussion**

This section presents and discusses the computational (running time) and security performance of our proposed RSA-CRT method.

**Running Time Comparison**

Computational performances of the proposed method, which includes running time of random key generation, encryption, and decryption processes, are discussed here. Based on the duration of a key pair generation process for all of its bits size, respectively, the processing time is shown in Fig. 3 and Fig. 4. It can be compared more rigid, increasing speed up on the process based on the utilization of n-prime numbers for the same key size. Generally, it can be seen that for increasing the longer size of keys or system modulus (n), the time processing to get the RSA key pair will also increase exponentially for all of the methods.

|  |  |  |
| --- | --- | --- |
| **Size in bits** | **Key generation time of RSA (MS)** | **Key generation of RSA-CRT(MS)** |
| 512 | 2159 | 1679 |
| 1024 | 2511 | 1692 |
| 2048 | 2675 | 2847 |
| 3072 | 2587 | 3249 |
| 4096 | 4210 | 5934 |

#### **Key Generation Comparison:**

Table 4.1: Key Generation Time

The table I provide lists the key generation timings for RSA (Rivest-Shamir-Adleman) and RSA-CRT (Chinese Remainder Theorem) for various key sizes in milliseconds (MS). Let's examine what each of these characteristics signifies in more detail:

**Size in bits**: The RSA encryption keys' bit size is shown in this column. One of the most important elements in evaluating how secure the encryption is the RSA key size. Longer key sizes often provide more security, but they also need more processing power.

**Key creation time of RSA (MS):** This column shows how long it takes to produce an RSA key pair of the given size when the standard RSA algorithm is used. The time is measured in milliseconds. Two prime integers are chosen, some mathematical operations are carried out, and then the public and private keys are generated using the RSA algorithm.

**The RSA-CRT (MS) key generation time was:** This column displays, in milliseconds, how long it takes to use the RSA-CRT technique to produce an RSA key pair of the given size. An optimization method called RSA-CRT (Chinese Remainder Theorem) divides some RSA processes, including private key decryption, into smaller, more manageable components.

**Let's now examine the information in the table:**

A normal RSA key pair of this size takes 2159 milliseconds to produce, while RSA-CRT requires 1679 milliseconds. In this instance, RSA-CRT is quicker since it streamlines the key creation procedure.

* **1024 bits:** RSA-CRT takes 1692 milliseconds whereas the conventional RSA key creation process takes 2511 milliseconds. Once again, at this key size, RSA-CRT is quicker.
* **2048 bits:** At 2048 bits, the production of an RSA key takes 2675 milliseconds, but the development of an RSA-CRT key takes 2847 milliseconds. In this instance, the typical RSA key creation is a little bit quicker.
* **3072 bits:** RSA key creation for keys of this size (3072 bits) takes 2587 milliseconds, whereas RSA-CRT requires 3249 milliseconds. In this instance, standard RSA is quicker.
* **4096 bits:** RSA-CRT requires 5934 milliseconds and conventional RSA requires 4210 milliseconds to generate RSA keys with 4096 bits. For this big key size, standard RSA is a lot quicker.

In conclusion, the key size and the particular implementation determine whether to use normal RSA or RSA-CRT for key creation. Standard RSA may be more effective for bigger key sizes, whereas RSA-CRT may be quicker for lower key sizes. The hardware and software used for key generation might also have an impact on the real performance. When selecting key sizes, it's also crucial to take security needs into account since longer keys tend to be more secure but also use more computing resources.

Fig 4.1: Key Generation

#### **4.2 Decryption Time Comparison:**

|  |  |  |
| --- | --- | --- |
| **Size in bits** | **Decryption time of RSA (MS)** | **Decryption time of RSA-CRT(MS)** |
| 512 | 7 | 3 |
| 1024 | 5 | 3 |
| 2048 | 16 | 2 |
| 3072 | 20 | 5 |
| 4096 | 49 | 21 |

Table 4.2 decryption time

The decryption timings for RSA (Rivest-Shamir-Adleman) and RSA-CRT (Chinese Remainder Theorem) for various key sizes are shown in the table you supplied in milliseconds (MS). Let's examine what each of these characteristics signifies in more detail:

**1. Size in bits:** The size of the RSA encryption keys is shown in this column in bits. This value corresponds to the key size utilized for both encryption and decryption operations.

**2. RSA decryption time (MS):** This column displays the amount of time, in milliseconds, required to conduct RSA decryption using the chosen key size.

**3. RSA-CRT decryption time (MS):** This column displays the amount of time, in milliseconds, required to conduct RSA-CRT decryption with the same key size. An optimization method called RSA-CRT may make certain RSA decryption procedures faster.

Let's now examine the information in the table:

* **512 bits:** RSA-CRT decrypts in about 3 milliseconds compared to 7 milliseconds for a regular 512-bit RSA key. In this situation, RSA-CRT decryption is much quicker.
* **1024 bits:** RSA-CRT decryption requires 3 milliseconds whereas standard RSA decryption takes 5 milliseconds. Once again, with this key size, RSA-CRT is quicker.
* **2048 bits:** While RSA-CRT decrypts in under 2 milliseconds, normal RSA keys of 2048 bits take 16 milliseconds to decrypt. At this key size, RSA-CRT decrypts data much more quickly.
* **3072 bits**: RSA-CRT decryption takes 5 milliseconds, whereas standard RSA decryption requires 20 milliseconds. The difference between the two algorithms is less pronounced than for lower key sizes, although RSA-CRT is still quicker.
* **4096 bits**: Standard RSA decryption for RSA keys of 4096 bits requires 49 milliseconds, whereas RSA-CRT requires 21 milliseconds. RSA-CRT is quicker, although with lower key sizes, the difference in decryption times between the two approaches is less noticeable.

In conclusion, the key size and the particular implementation determine whether to use normal RSA or RSA-CRT for decryption. For decryption procedures with different key sizes, RSA-CRT is often quicker, particularly for smaller keys. As the key size grows, the performance benefit might, however, decline. It is crucial to remember that RSA-CRT optimization is very helpful for accelerating private key decryption processes in RSA. When choosing the right RSA key size and optimization technique, it's important to take performance and security needs into account. Actual decryption durations may also vary depending on hardware and software implementations.

Fig 4.2 : Key Decryption

## **Chapter-****5**

## **Conclusion**

The addition of the Chinese Remainder Theorem (CRT) to our project's encryption system has shown out to be a crucial improvement, greatly enhancing the speed of decryption and system performance as a whole. The following vital benefits are provided by this key optimization, which has brought about a new era of effectiveness and responsiveness in our cryptography implementation:

Decryption procedure Speed Improvement: Our system's decryption procedure has been significantly accelerated by CRT. The modular exponentiation was broken down into smaller, independent computations by CRT, which lightened the computing burden and sped up the extraction of plaintext from cipher text. This improvement in decryption performance is especially beneficial for real-time applications where prompt data access is crucial.

Resource Efficiency: The CRT improvement reduces the amount of CPU resources needed for decryption while simultaneously enhancing speed. This results in decreased hardware and energy requirements, which makes our system more cost- and environmentally-efficient to run, especially in regions with limited resources.

Enhanced Scalability: Data decryption skills are becoming more important as data quantities continue to increase dramatically. Our system scales smoothly because to CRT's efficiency, keeping up its responsiveness and dependability even while dealing with massive amounts of encrypted data.

Improved User Experience: When engaging with our system, users will gain from a more smooth and responsive experience. Improved user satisfaction, particularly in applications needing real-time access to sensitive information, might result from faster decryption times since they result in less delay in data retrieval.

Competitive Advantage: In a market that is competitive, our product may stand out from competing cryptographic solutions due to its capacity to deliver quicker decryption. For companies and people looking for the most efficient and effective encryption technology, this competitive advantage may be a key consideration.

In conclusion, a new age of cryptographic performance has begun with the incorporation of the Chinese Remainder Theorem (CRT) into our encryption system. Our product is positioned as a reliable and effective solution for secure data transfer and storage because to the major increase in decryption speed, resource efficiency, and scalability. The effect of CRT on user experience and competitive advantage emphasizes how crucial this optimization is to fulfilling the requirements of contemporary information security. We can state with confidence that CRT has improved not just our project but has also opened the door for quicker, more effective cryptographic solutions in a constantly changing digital environment.

## **Reference:**

Nanang Triagung Edi Hermawan a, Edi Winarko b,\*, Ahmad Ashari b, Indonesia, (IJASEIT), “Eight Prime Numbers of Modified RSA Algorithm Method for More Secure Single Board Computer Implementation.’’ ISSN: 2088-5334, 31 December, 2021

Engr. Shaheen Saad Al-Kaabi and Dr. Samir Brahim Belhaouari “METHODS TOWARD ENHANCING RSA ALGORITHM : A SURVEY’’ (IJNSA) Vol. 11, No.3, May 2019

Dharitri Talukdar, Lakshmi Prasad Saikia “Simulation and Analysis of Modified RSA Cryptographic Algorithm using Five Prime Numbers” ISSN: 2321-8169 224 – 228

Nitin Jain, Surendra Singh Chauhan, Alok Raj, India, (IJEAT) , “Security Enhancement of RSA Algorithm using Increased Prime Number Set . ISSN: 2249 – 8958, Volume-9 Issue-3, February 2020

METHODS TOWARD ENHANCING RSA ALGORITHM: A SURVEY. Engr. Shaheen Saad Al-Kaabi and Dr. Samir Brahim Belhaouari, Qatar, (IJNSA) Vol. 11, No.3, May 2019

K. El Makkaoui, A. Beni-Hssane, A. Ezzati, and A. El-Ansari, “Fast Cloud-RSA Cloud-RSA Scheme for Promoting Promoting Data Data Confidentiality in the the Cloud Computing,” in Procedia Computer Science, 2017, vol. 113, pp. 33–40, doi: 10.1016/j.procs.2017.08.282.

S. Nalajala, P. Ch, A. Meghana, and P. M. B, “Data Security Using Multi Prime RSA in Cloud,” Internatinal J. Recent Technol. Eng., vol. 7, no. 6S4, pp. 110–115, 2019.

P. Matta, M. Arora, and D. Sharma, “A comparative survey on data encryption Techniques: Big data perspective,” Mater. Today Proc., no. xxxx, 2021, doi: 10.1016/j.matpr.2021.02.153.

W. Susilo, J. Tonien, and G. Yang, “A generalised bound for the Wiener attack on RSA,” J. Inf. Secur. Appl., vol. 53, p. 102531, 2020, doi: 10.1016/j.jisa.2020.102531.