THE IMPLEMENTATION OF RSA ALGORITHM IN TEXT MESSAGES ENCRYPTION AND DECRYPTION

Shovan Mondal, Aji Primajaya*
Universitas Singaperbangsa Karawang
Jl. H.S. Ronggowaluyo, East Karawang 41361
aji.primajaya@staff.unsik.ac.id

ABSTRACT

In terms of texting, especially in such an ultramodern period of time, precisely 4.0 Industry, one of its topmost challenge or problems faced is related to security. Thousands, if not, hundred thousands of crime are committed through text message hacking because text communication could contain plenitude of particular personal informations, similar as passwords, ID number, phone number, etc. Cryptography from the Discrete Mathematics field is one of the best option to cover the data contained in text messages, hence, as time passed by, it is developed into RSA Algorithm; encryption and decryption key. Anyone who possess the wrong key will still be able to get the message, but the encrypted version would be far different from the real one.. The conversation covers basic topics such the decryption process—which reverses this process using a private key—and the encryption process—which converts plaintext into ciphertext by means of a public key. using means of prime numbers in key generation using RSA, data confidentiality is facilitated, therefore allowing only those with the suitable private key to decode the messages. Different cases show how well RSA protects personal data sent across networks, therefore stressing its importance in enhancing safe digital communication. Using a public key, the encryption process transforms plaintext into ciphertext therefore only those with the corresponding private key can decode the message. RSA creates safe, asymmetric key pairs by means of a mathematical approach involving prime numbers, therefore impeding attackers' access into the system. Emphasizing RSA's relevance in maintaining communications safe in email, mobile, and online apps, practical examples show how effectively the algorithm performs for encrypting and decryption of text messages. The paper then discusses how difficult RSA computation is and emphasizes how much security is truly enhanced by employing big prime values. This paper emphasizes the need of RSA for safeguarding digital communications and establishing a safe environment for data flow in modern digital systems.

Keywords: *encryption, decryption, key, RSA algorithm, cryptography*

1. INTRODUCTION

In quite an advanced era, 4.0 Industry, where people substantially use internet connections and digital technologies to complete all sorts of their activities, there are plenty implementation of Discrete Mathematics, especially in the field of Information Technology. Discrete Mathematics help programmers or engineers to make, develop, and perfected their programs so they would have effective and safe performance for users world wide.RSA activities may be categorized into three primary steps: key creation, encryption, and decryption. RSA possesses several design problems, rendering it unsuitable for commercial usage[1].

Most things are easily exposed these days because of those technologies, especially informations contained within certain online interactions. Of course, some words exchanged among the people is not always to be exposed. Some messages are meant to be private or kept only between the related persons. That is why people try to find a secret way to give certain code to their acquintance so none but them would know, like Caesar Cipher for example. When opening a text messaging application, some of them briefly mentioned encryption which makes us wonder how is exactly does it work. It is part of Discrete Mathematics study without which our text messages might not be secure or not free from spies. So we will see how exactly is it doing its job.

2. LITERATURE REVIEW

The RSA algorithm, developed by Rivest, Shamir, and Adleman, utilises asymmetric key encryption for secure data transport. It employs a dual-key system: a public key for encryption and a private key for decryption. Goshwe [2] emphasises its efficacy in a network setting, especially for data encryption and decryption. The algorithm's efficacy is rooted in the mathematical challenge of factoring big prime numbers, rendering it a reliable option for secure communications.

The application of RSA in text messaging has attracted interest owing to the growing demand for secure communication routes. Bodur and Kara [3] devised a safe SMS encryption technique employing the RSA algorithm in an Android messaging application, demonstrating the practical utility of RSA in daily communication. This study demonstrates the capability of RSA to protect critical information conveyed by SMS.

Recent studies have investigated novel methods to improve the usefulness of the RSA algorithm.[4] introduced a novel approach for the encryption and decryption of textual messages utilising ASCII representations, positing that algorithmic adaptation

can enhance both efficiency and security. This adaptability is especially pertinent for text messaging, where data quantity and processing speed are critical aspects.

In a comparative analysis of encryption algorithms,[5] assessed RSA in conjunction with other approaches like DES, 3DES, and AES, highlighting RSA's distinct benefits regarding security and implementation simplicity. This comparative research underscores the algorithm's significance in modern cryptographic methods, especially for applications necessitating strong security, such as text messaging.

The feasibility of executing RSA has been further proved in numerous study settings[6]documented the deployment of the RSA algorithm for email encryption and decryption, which similarly demonstrates its efficacy in safeguarding data integrity and confidentiality in text messaging.[7] elucidated the mathematical underpinnings of RSA, hence affirming the algorithm's dependability in cryptographic contexts. RSA is predicated on factorizing and factoring big numbers. First, you have to pick two big prime numbers for the key pair—hard to factor[8]. Therefore, the prime numbers have to be chosen at random with a significant variance among them. Think of the two selected prime numbers, for instance, as p and q. The technique then computes their product, indicated by n = p * q. While n, used as the modulus for public and private keys, must be made public, the values of p and q should be kept secret. After that, the totient function of the carmecheals is computed with p and q; the integer e, whose value serves as the public exponent, is chosen then. The value of d, which serves as the private exponent, is then next calculated.

3. RESEARCH METHOD

3.1. Cryptography

Cryptography is a discipline that examines the security of communication methods, ensuring that only the sender and the designated receiver may access the actual content of the message. The phrase is derived from the Greek word kryptos, meaning concealed. In cryptography, the word encryption is firmly established. It involves converting plain text into ciphertext and subsequently reverting it upon receipt[1]. Cryptography plays a significant role in data protection, particularly for software and applications operating inside a network context.

Nevertheless, despite the existence of protected communication for millennia, the major operational issue prevented its widespread use. The advancement of public-key cryptography has facilitated secure communication among a vast number of network users, even in instances when they have not previously interacted[2]. We are analyzing the Public Key encryption method utilizing the RSA algorithm, which transforms information into an unintelligible format for potential intruders. Therefore, preventing unauthorized users from accessing the information, even if they manage to infiltrate the system.

3.2. Public Key Encryption Algorithm

The Public Key Encryption[3] Algorithm is classified as an asymmetric algorithm, meaning that the sender and receiver use different keys for encryption and decryption—specifically, a pair of keys: a Public Key and a Private Key.

Public key encryption is utilized for the encryption process, while the private key is employed for decryption. The designated public key was inadequate for the decryption process. The two keys are interconnected; however, the private key cannot be obtained from the public key. The public key is accessible in the open environment, whereas the private key remains confidential and is known solely to its owner. This indicates that any individual can transmit a message to the user utilizing the user's public key; however, only the user possesses the capability to decrypt the message with their private key.

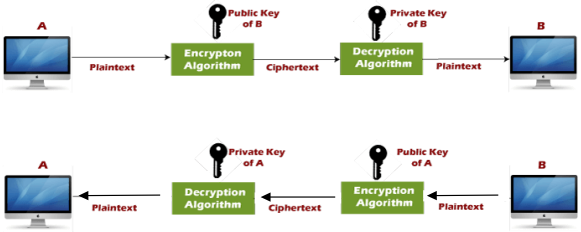

Figure 1. Encryption/Decryption Using Public/Private Keys

Here is the procedure of Public Key Algorithm:

a. The data that was going to be transferred is encrypted by sender A using the public key of the intended receiver.
b. B decrypts the entered ciphertext using its private key, which is known only to B. B replies to A by encrypting its message using A's public key.
c. A decrypts the entered ciphertext using its private key, which is known only to him.

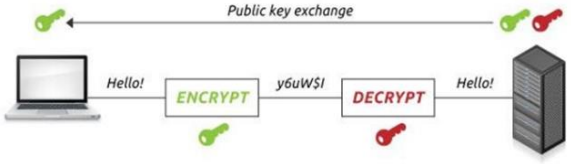

Figure 2. Public Key Exchange Illustration

3.3. RSA Algorithm

The RSA Algorithm[4] is a widely recognized implementation of Public-Key Cryptography, introduced by Rivest, Shamir, and Adelman in 1978, which is reflected in the name 'RSA' in the RSA Algorithm. This algorithm employs two separate keys: a public key, which is generally accessible to all, and a private key, which is kept secure and is not permitted to be exchanged between the sender and receiver. The following procedure is employed by this algorithm to generate public and private keys:

a. Choose two distinct large random prime numbers; p and q (secret).
b. Calculate n = p × q, where n is called the modulus for encryption and decryption (not secret).
c. Calculate Euler's function of n, which is m = (p−1)·(q−1)
d. Choose one integer as e which value is less than n, and keep in mind that n is relatively prime to m. It means that e and m have no common factor except 1. Choose 'e' such that 1<e<m, e is prime to m.gcd$(e, d(n))$ = 1 (1)
e. If n = p × q, then the public key is number pair <e, n>. To find ciphertext from plain text, compute d such that e.d = 1(mod m) or for encrypting a message M with the public key, the equation $C = Me \ mod \ n$ (2)
f. Can also be used. With M represented by blocks of numbers where every value of block must be less than n. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
g. To determine the private key, we use the following formula to calculate it:
d=$(1 + k - m)/e$ (3)
h. A ciphertext message C is decrypted using private key <d, n>. To calculate plain text M from ciphertext C, we can use the equation
$M = C^d mod \ n$ (4)

Note that M is divided into blocks as form: (M_1|M_2|… …. M_i| …) and C will be as form: (C_1|C_2|… … C_i| …).

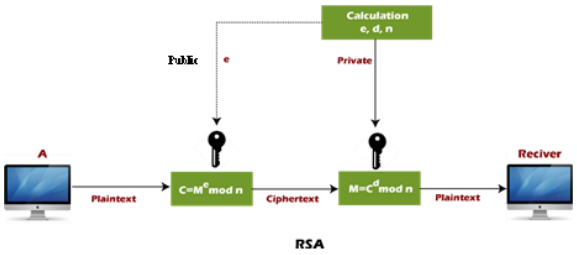

Figure 3. RSA Algorithm Illustration

3.3.1 Prime Numbers

RSA encryption, as mentioned, is based on a special property of prime numbers[6]. The prime numbers 2, 3, 4, 5,… are natural numbers higher than 1 that cannot be stated as the product of smaller natural numbers. As a result, a prime number is a natural number bigger than 1 whose sole positive elements are itself and 1.

Each natural number greater than 1 can be factorized as a product of powers of primes. Moreover, if we ignore the order of the prime powers, then there is only one way to do this. For example, we can write

$$60 = 2^2 \times 3 \times 5 \quad (5)$$

There amount of prime numbers are infinite. It is quite easy to find lots of huge prime numbers using a computer. In practice, finding the prime factorization of a really big integer is quite difficult. This is what makes RSA encryption so difficult to break. As a result, the larger the number, the more difficult it is to break and the more secure it may be. The RSA algorithm, attributed to its creators Rivest, Shamir, and Adleman, stands as the most widely utilized public key cryptographic method, playing a crucial role in securing data communication [10]. The foundation is fundamentally rooted in two primary cryptographic processes. Initially, a public key is employed to transform an input data referred to as plaintext into an unintelligible encrypted output known as ciphertext (encryption process). This transformation ensures that recovering the original plaintext without the encryption password is infeasible within a reasonable timeframe. Secondly, the RSA algorithm employs a private key to transform the encrypted data back into its original format, a process known as decryption [10]. Currently, it finds application in web browsers, email applications, mobile devices, virtual private networks, and secure shell environments.

3.4. ASCII System

ASCII, or American Standard Code For Information Interchange, serves as a standardized data-transmission code utilized by smaller and less-powerful computers. It encodes textual data, including letters, numbers, and punctuation marks, along with commands for non-input devices, known as control characters. The process involves converting data into standardized digital formats, enabling computers to communicate with each other and manage data more effectively[7].

The traditional ASCII code utilizes seven-digit binary numbers formed by various combinations of 0's and 1's. Given that there are 128 unique combinations of seven 0's and 1's, this code can signify 128 different characters. The binary sequence 1010000 denotes a capital 'P', while the sequence 1110000 signifies a lowercase 'p'. The characters can subsequently be transformed into either a decimal or hexadecimal representation.

Table 1. ASCII Table (Partial)

ASCII	Decimal	Hexadecimal	Octal	Binary
space	32	20	40	100000
!	33	21	41	100001
"	34	22	42	100010
#	35	23	43	100011
$	36	24	44	100100
%	37	25	45	100101
&	38	26	46	100110
'	39	27	47	100111
(	40	28	50	101000
)	41	29	51	101001
*	42	2A	52	101010
+	43	2B	53	101011
,	44	2C	54	101100
-	45	2D	55	101101
.	46	2E	56	101110

ASCII	Decimal	Hexadecimal	Octal	Binary
/	47	2F	57	101111
0	48	30	60	110000
1	49	31	61	110001
2	50	32	62	110010
3	51	33	63	110011
4	52	34	64	110100
5	53	35	65	110101
6	54	36	66	110110
7	55	37	67	110111
8	56	38	70	111000
9	57	39	71	111001
:	58	3A	72	111010
;	59	3B	73	111011
<	60	3C	74	111100
=	61	3D	75	111101
>	62	3E	76	111110
?	63	3F	77	111111
@	64	40	100	1000000
A	65	41	101	1000001
B	66	42	102	1000010
C	67	43	103	1000011
D	68	44	104	1000100
E	69	45	105	1000101
F	70	46	106	1000110
G	71	47	107	1000111
H	72	48	110	1001000
I	73	49	111	1001001
J	74	4A	112	1001010
K	75	4B	113	1001011
L	76	4C	114	1001100
M	77	4D	115	1001101
N	78	4E	116	1001110
O	79	4F	117	1001111
P	80	50	120	1010000
Q	81	51	121	1010001
R	82	52	122	1010010
S	83	53	123	1010011
T	84	54	124	1010100
U	85	55	125	1010101
V	86	56	126	1010110
W	87	57	127	1010111
X	88	58	130	1011000
Y	89	59	131	1011001
Z	90	5A	132	1011010

4. RESULTS AND DISCUSSION

From the previous explanation, it would be suitable to perform and see the implementation of RSA Algorithm itself into decryption and encryption, starting from the basic to a small real case.

4.1. Example 1

Encrypt plaintext 9 using RSA public-key encryption algorithm with n = 7×11 to generate the public and private keys.

Example:

1. $p = 7$ & $q = 11$ (6)
2. $n = p \times q = 7 \times 11 = 77$ (7)
3. $m = (p-1) \times (q-1) = (7-1) \times (11-1) = 60$
   The public key is <e, n> = (7, 77) (8)
4. From (2) we can get
   $C = 9^7 mod\ 77 = 37$ (9)
5. From (3) we can get
   $d = \frac{1+k \cdot 60}{7}$ (10)
   $d = \frac{1+5 \cdot 60}{7} = 43$ (11)
6. From (4) we can get
   $M = 37^{43} mod\ 77$ (12)
   $M = 9$ (13)

So the solution to this problem is plain text = 9 and the ciphertext = 37

4.2. Example 2

Lucy woke up in the morning and remembered that her class will have a test today. She wanted to remind her friend, Lola, just in case. Her message says

MATH TEST, 1PM

With n = 53×67 and e=25, write down the ciphertext output and explain how to decrypt it back to plaintext.

Explanation:

1. First, we must convert the plain text above into ASCII decimal using table 1. And we will get 77658472328469838444324980 77
2. Form blocks which each consists of three digits. Which leads to 776 584 723 284 698 384 443 249 807 7
3. $p = 53$ & $q = 67$ (14)
4. $n = p \times q = 53 \times 67 = 3551$ (15)
5. $m = (p-1) \times (q-1) = (53-1) \times (67-1) = 3432$ (16)
   The public key is <e, n> = (25, 3551)
6. From (2) we can get
   $C_1 = 776^{25} mod\ 3551 = 3300$ (17)
   $C2 = 584^{25} mod\ 3551 = 2492$ (18)
   $C3 = 723^{25} mod\ 3551 = 3353$ (19)
   $C4 = 284^{25} mod\ 3551 = 2477$ (20)
   $C5 = 698^{25} mod\ 3551 = 854$ (21)
   $C6 = 384^{25} mod\ 3551 = 1162$ (22)
   $C7 = 443^{25} mod\ 3551 = 1841$ (23)
   $C8 = 249^{25} mod\ 3551 = 2693$ (24)
   $C9 = 807^{25} mod\ 3551 = 764$ (25)
   $C10 = 7^{25} mod\ 3551 = 1840$ (26)
7. Thus, the encrypted message is 3300249233532477854116218412693764 1840
8. From (3) we can get
   $d = \frac{1+k \cdot 3432}{7}$ (27)
   $d = \frac{1+7 \cdot 3432}{7} = 961$ (28)
9. From (4) we can get
   $M_1 = 3300^{961} mod\ 3551 = 776$
   $M2 = 2492961 mod\ 3551 = 584$ (30)
   $M3 = 3353961 mod\ 3551 = 723$ (31)
   $M4 = 2477961 mod\ 3551 = 284$ (32)
   $M5 = 854961 mod\ 3551 = 698$ (33)
   $M6 = 1162961 mod\ 3551 = 384$ (34)
   $M7 = 1841961 mod\ 3551 = 443$ (35)

$M8 = 2693961 mod\ 3551 = 249$ (36)
$M9 = 764961 mod\ 3551 = 807$ (37)
$M10 = 1840961 mod\ 3551 = 7$ (38)

And those are the steps on how the encryption and decryption calculation works. Reference [2] showed that there's a certain software that was tested on University of Agriculture to perform calculation similar to this one for the internet. Reference[8] stated that an application has been developed on the Java platform in order to use the RSA encryption algorithm on Android-based mobile devices in the process of sending messages via SMS. Thus, people could feel secure about their data from fear of being stolen by unwanted third party.

The security of RSA Algorithm[5] lies within the difficulties to factorized a non- prime number to its prime number, which, in this case, is n = p×q. Once n is successfully discovered, then m=(p-1)(q-1) can also be found, and so are the rest of the calculation.

The founders of RSA algorithm suggested that the value of p and q is longer than at least 100 digits. Thus, the multiplication result of p and q (n) would have at least 200 digits. According to Rivest and his friends, the effort of finding the factor of 200 digits needed about 4 billion years of computation time (with the assumption that the factorization is done using the fastest algorithm right now with a computer that has the speed of 1 milisecond.

Fortunately, an algorithm so powerful to factorized enormous amount of numbers has yet to be found so the RSA algorithm could still be used up until today. As long as nobody found that great algorithm to factorized the integers into its prime factors, then RSA algorithm is still recommended to be used to cipher a text. Though large companies for text messaging technologies rarely use RSA algorithm because they need faster and more secure algorithm for users world wide and also involved symmetric algorithm.

5. CONCLUSION

Previous research and explanations have proven that cryptography helps people to study advanced secure communication that would be very useful in this era, where almost everything is digitalized and stored important datas, be it governor's or citizens'.

RSA Algorithm is one of the most common of Public-Key Cryptography used for data security and is usually used on text messaging, where it would convert a plain text into cipher text using a recipient's public key that said person would open using his private key.

RSA Algorithm would be more secure if the value of both p and q are bigger, or as suggested, more than 100 digits, so that the value of n is about 200 digits which made it difficult to be factorized or hacked by a third party.If a third party who tries to break into the message, they will get a meaningless message instead since they don't have the private key to receive the right message.

BIBLIOGRAPHY

[1] Kaspersky, "Cryptography Definition," *www.kaspersky.com*, Jan. 13, 2021. https://www.kaspersky.com/resource-center/definitions/what-is-cryptography (accessed Dec. 24, 2021).

[2] "ASCII | communications | Britannica," *Encyclopædia Britannica*. 2021, Accessed: Dec. 25, 2021. . https://www.britannica.com/topic/ASCII.

[3] A. Steef, M. N. Shamma and A. Alkhatib, "RSA Algorithm With A New Approach Encryption And Decryption Message Text By ASCII," *International Journal on Cryptography and Information Security (IJCIS)*, vol. 5, 2015. DOI:10.5121/ijcis.2015.5403.

[4] N. Goshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment," *IJCSNS International Journal of Computer Science and Network Security*, vol. 14, no. 5, p. 82, 2014, Accessed: Dec. 24, 2021. [Online]. Available: http://cloud.politala.ac.id/politala/1.%20Jurusan/Teknik%20Informatika/19.%20 e-journal/Jurnal%20Internasional%20TI/IJCSNS/2014%20Vol.%2014%20No.%2005/20140515_Data%20Encryption%20and%20Decryption%20Using%20RSA%20Algorithm%20in%20a%20Network%20Environment.pdf.

[5] Singh, G. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. In International Journal of Computer Applications (Vol. 67, Issue 19).

[6] A. Ginting, R. R. Isnanto and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," *Jurnal Teknologi dan Sistem Komputer*, vol. 3 No 2, April 2015.

[7] M. Evans, Math delivers! RSA Encryption, J. Pitkethly, Ed., Melbourne: the Creative Commons, 2013.

[8] "RSA Encryption Algorithm - Javatpoint," *www.javatpoint.com*, 2011. https://www.javatpoint.com/rsa-encryption-algorithm (accessed Dec. 25, 2021).

[9] H. Bodur and R. Kara, Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application, Valencia: Duzce University, 2015.

[10] Mijanur Rahman Jatiya Kabi Kazi Nazrul et al. (2012)