Study A Public Key in RSA Algorithm

Taleb A. S. Obaid

***Abstract*—To transmit sensitive information over the unsafe communication network like the internet network, the security is precarious tasks to protect this information. Always, we have much doubt that there are more chances to uncover the information that is being sent through network terminals or the internet by professional/amateur parasitical persons. To protect our information, we may need a secure way to safeguard our transferred information. So, encryption/decryption, stenographic and vital cryptography may be adapted to care for the required important information. In system cryptography, the information transferred between both sides sender/receiver in the network must be scrambled using the encryption algorithm. The second side (receiver) should be outlook the original data using the decryption algorithms. Some encryption techniques applied the only one key in the cooperation of encryption and decryption algorithms. When the similar key used in both proceeds is called symmetric algorithm. Other techniques may use two different keys in encryption/decryption in transferring information which is known as the asymmetric key. In general, the algorithms that implicated asymmetric keys are much more secure than others using one key. RSA algorithm used asymmetric keys; one of them for encryption the message, and is known as a public key and another used to decrypt the encrypted message and is called a private key. The main disadvantage of the RSA algorithm is that extra time is taken to perform the encryption process. In this study, the MATLAB library functions are implemented to achieve the work. The software helps us to hold very big prime numbers to generate the required keys which enhanced the security of transmitted information and we expected to be difficult for a hacker to interfere with the private information. The algorithms are implemented successfully on different sizes of messages files.**

***Index Terms*—Cryptography, Ciphertext, Data Security, RSA Algorithm, Key Generation.**

I. INTRODUCTION

Several researchers emphasize cryptography techniques to transferred vital information through unsecured channels. They have confirmed that the greatest technique to get secrecy and reliability of data. However, the data transferred through network channels facing real challenges by different sides that interest to uncover the secret information. Developing of information technologies is raising the level of threats and vulnerabilities of the forward the data in unsecured canals. To encounter the problem, the cryptography researchers have stressed their talents in discovers an unconventional alternative to improve transmitted information protection by ensuring information accessibility. At present dissimilar algorithms have been stimulated to provide much more security. Of course, such sophisticated algorithms generate a more expensive and consumption much computational resources, Meneses et al. [1].

As it's known the cryptography is the procedure too is used to protected important data through transfers it over a normal network channel, which is not necessary to stay secure, and the other side receives the message as it that. Nowadays, the subject of data confidence becomes a very crucial feature of information computing discipline. Easy admission of the Internet today and all the data all over the world led to the importance of the topic of security data. Although, this will be created new dangers for those users who want to remain their data safer. As we expected, hackers and penetrates are using a diversity of techniques to penetrate and break out into an information transferred channel and steal information or alteration of the original data of any organization [2]-[5].

At present, cryptography algorithms afford a high level of confidentiality by covering private data of any individuals or groups. Cryptography is implemented to provide access to data in a constrained way, data reliability, and validation. At present, many of the research's effort is going on to find out the new cryptographic algorithms more efficient based on security and complexity [2].

Generated a one secrete-key (private) of the cryptography algorithm uses for both approaches i.e., is known as an asymmetric key. This technique proved that has lesser computational efforts but unfortunately has many drawbacks like discovering and infer the key, the obligation of a shared secret key, validation [3],[4].

Asymmetric cryptography algorithm, use a public-key to achieve an encryption pattern and then, used a private key to decrypt the cipher information. However, asymmetric cryptography implements two different mathematically approaches, like a public key and the other a private key. Dissimilar symmetric algorithms applied only one key to both the encryption/ decryption approach performance, [6], [7]. Moreover, the public key is speared openly and can be used to encrypt data by anyone. On the other hand, the private key is kept secret and implemented by the recipe side to decrypt the received encrypted data.

Rivest, Shamir, and Adleman (RSA), in (1977) were the first described the algorithm that implemented public key, [2]. The RSA technique is succeeded to solve the asymmetric cryptography problems. RSA algorithm applied different keys as public/private keys but are related to a large scale of applications. As a result, reliable secured results and better security transfer data were big prime integer numbers chosen for both the public / private keys [6], [7]. RSA applied extensively for encryption/decryption problems leading a protected transmission of the data. RSA comes to be more enhanced protection when the value of the key is big enough and it becomes much more difficult to figure out its common factors of the key number. An

Published on April 2, 2020.
T. A. S. Obaid is with University of Basrah, Iraq.

asymmetric key means that it works on two different keys as a public key and a private key. The public key shoul be known by everyone but the private key is not and kept privately to receiver only. The objective of RSA founded on the fact that it is hard to factorize a key because a large prime integer is chosen. Usually, the public key generated by two prime numbers.

II. Symmetric vs. Asymmetric Cryptography

Cryptographic techniques had been used since ancient times before inventing computers system, and the techniques have evolved since those times.

Cryptography algorithms are regularly separated into two categories and identified as symmetric/asymmetric cryptography. The essential difference between these two categories of encryption/decryption depends on the fact that symmetric cryptography uses a single key that needs to be common among the second side who need to receive the message that sent by the first side. While asymmetrical cryptographs contain a public key to encrypt data only. The private/public keys are unlike, but they are related. However, the public key is offered to everybody who desires to use this method and send the messages, but in other hands, the private key is set hidden at a secured place, One of drawback is asymmetric encryption takes much more time than symmetric encryption [7]-[9].

Of course, both types of cryptographic have benefits and drawbacks relative to one another. Symmetric encryption algorithms are much quicker, require less computational power, and simpler, but their main weakness is that a key may be discovered by hackers. Because in the symmetric technique is only one key is applied to both encryption and decryption of data, so, this key must keep safe. though this key handover to a trusted person who needs it to access the data, so, the key does not open up for the public to keep it secured, [10],[11].

On the other hand, asymmetric encryption resolves the problem of key spreading for using public keys for encryption technique and private keys for decryption. The compromise, however, is that asymmetric encryption technique is very slow by comparison to symmetric technique and require much more computation power as a result of their massively longer key lengths.

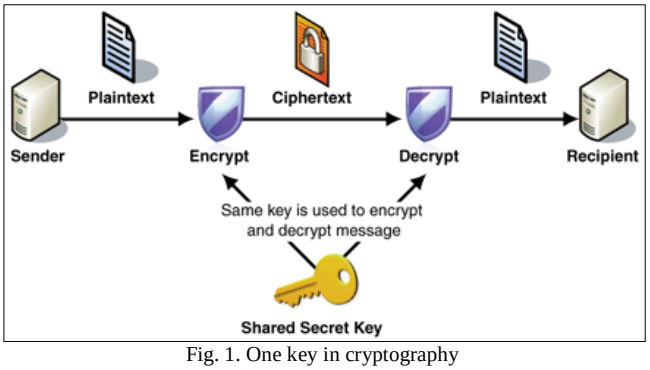

Fig. 1. One key in cryptography

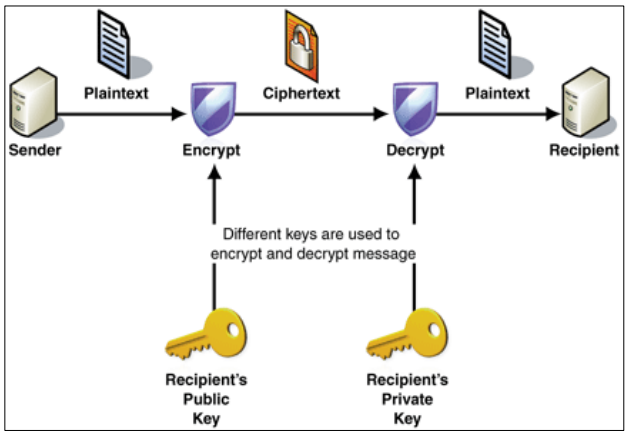

Fig. 2. Two keys in cryptography

III. RSA Algorithm [11] - [16]

To implement the RSA technique smoothly, we need to trail the following three steps:

A. Key generation

- RSA algorithm involves generating two different keys, like a public key beside a private key. As a familiar, the public key should be distributed for anyone who is intending to implement this technique to encrypt a piece of transmitted information. The messages are encrypted via public key but it may be decrypted by one who had a privet key in a sensible amount of time so that it is mean, the private key should be delivered by receipt side. The keys of the RSA algorithm are Select two big prime integer numbers **N** and **M**. Since we intend to satisfy safekeeping the message, the integer's **N** and **M** should be chosen as big prime integers.
- Compute a number **n** = **N***M. where n is computed as the modulo for both the public and private keys.
- The Euler's function phi() should be computed as, phi **(n) = (N − 1)*(M − 1)**, where phi function is the integer number.
- Let generated as the following: [17], [18]:
- an integer e in the range $1 \leq e \leq \text{phi}(n)$ and the GCD (e, phi (n)) = 1, so that e and phi(n) are coprime.

B. Encryption key

Select the index integer e so that e is greater than 1 and less than phi **(n)**, and the greatest common divisor GCD **(e,** phi **(n)) = 1**. The integer, **e,** and phi**(n)** are should be a co-prime. The **e** is unconstrained as the public key exponent.

C. Decryption Key

Let d is a decryption key and is computed **d** as:

$$\mathbf{d = e^{-1} \bmod} (\text{phi } \mathbf{(n)});$$

where d is computed as the multiplicative inverse of e (modulo phi (n)). To be more clarified d solved as:

$$\mathbf{d*e \equiv 1 \ (mod} \text{ phi } \mathbf{(n)).}$$

The public key involves the modulo of **n** and the index **e**. While the private key involves of the modulus **n** and the private key **d**, which must be kept the secret, at the same time the **N**, **M**, and phi **(n)** must also be kept the secret to prevent the interveners applied these parameters to calculate **d**, [19]-[22].

IV. A WORKED EXAMPLE

In the following, we offer an applied example of RSA encryption/decryption. The parameters used here are small to clarify the procedure.

Enter the prime integer for N = 59
Enter the prime integer for M = 41
Compute n = N*M = 59 *41=2419.
Compute the function
phi ((N-1)* (M-1))
= ((59-1) * (41-1)
= 2320.

Compute the public key for exponent **e** such that **1 < e < phi(n)** and so that greatest common divisor
GCD (e, phi(n)) = 1;
$\Rightarrow$ **e = 1381**.
Compute the private key **d** as
d*e ≡ 1 (mod phi(n)) ;
d * 1381= 1 (mod 2320)
$\Rightarrow$ **d=1181.**
To prove that a public and private keys whether to satisfy the above relation:
e*d mod (phi()) =
(1381 * 1181) mod 2320
= 1630961 mod 2320
= 1
So,
Puplish the public key is (1381, 2419)
Puplish the private key is (1181, 2419)

We are ready to send the public key to the second side (receipts) to write a required text message and encrypted it using a public key, i.e., converted to ciphertext and the second side sends the cipher message to the first side (sender) to decrypt the received a cipher message using a private message.

e.g., Let us applied a numerical example:
suppose the second side enter the following message: "**Computer Science"**
The ASCII equivalent of the message is:
67 111 109 112 117 116 101 114 32 83 99 105 101 110 99 101

The encrypted message is

1955	937	1643	2236	235	2240
750	173	91	83	1633	400
750	1821	1633	750		

The decrypted cipher message in ASCII is

67	111	109	112	117	116
101	114	32	83	99	105
101	110	99	101		

The decrypted message is: **Computer Science**

V. CONCLUSION

The most widely-uses asymmetric key is the RSA algorithm. RSA algorithm is effectively proved to be resisted the spam attempts to penetrate the data had been sent through the network and tampering these data. The more security is based on the difficulty of the factorization of the large prime integers chosen to generate the key. To prevent an intruder discovery of the ciphertext we should select a big prime number in the RSA algorithm. The encrypted plaintext by the RSA algorithm is often used in mixture with other encryption schemes to safely transfer the data. To make RSA more efficient things more efficient, a plaintext will generally be encrypted first with a symmetric algorithm, and once again use the RSA algorithm to encrypt the ciphertext using the asymmetric key. A final use of the symmetric key in the decryption of the ciphertext and recover the original plaintext.

REFERENCES

[1] Meneses F., Fuertes W., José Sancho, Salvador S., Flores D., Aules H., Castro F. Torres J., Miranda A., Nuela D., (2016), "RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8.
[2] Jamgekar R. S., Joshi G.S., (2013), "File Encryption and Decryption Using Secure RSA," International Journal of Emerging Science and Engineering (IJESE), ISSN: 2319–6378, Volume-1, Issue-4,
[3] Obaid T. A. S. Khami M. Shehab L. G. (2017), "Hiding Secured key in digital media", Int. Jo. Eng. Res. App., ISSN: 2248-9622, Vol. 7, Issue 9, pp.58-63, www.ijera.com
[4] Nisha S., and Farik M., (2017), " RSA Public Key Cryptography Algorithm – A Review", International Journal of Scientific & Technology Research Volume 6, Issue 07, ISSN 2277-8616.
[5] Khyoon, A. I. (2005) "Modification on the Algorithm of RSA Cryptography System," Al-Fatih Journal, ISSN: 87521996, Volume: 1 Issue: 24 Pages: 80-89.
[6] Al-Lehiebe A., (2015), " Ciphered Text Hiding in an Image using RSA algorithm", J. Of College of Education for Women vol. 26 (3).
[7] Cid C., (2019), " Cryptanalysis of RSA: A Survey", SANS Institute.Bonde S. Y.; Bhadade U.S., (2017) International Conference on Computing, Communication, Control and Automation (ICCUBEA)", DOI: 10.1109/ICCUBEA .8463720, Publisher: IEEE.
[8] Patel S. R., Shah K., Patel G. R., (2013), "Study on Improvements in RSA Algorithm," IJEDR, ISSN: 2321-9939.
[9] Milanov E., (2009), "The RSA Algorithm" https://sites.math. washington. edu/~morrow/336_09/ papers/Yevgeny.pdf.
[10] Kumar Y., Munjal R., Sharma H, (2011), "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," Int. J. Comp. Sci. and Management Studies, Vol. 11, Issue 03, ISSN: 2231-5268, www.ijcsms.com.
[11] Choudhary V., Praveen N. "Enhanced Rsa Cryptosystem Based On Three Prime Numbers," Int. J. Innov. Sc., Eng. & Tech., Vol. 1, Issue 10, 2014. www.ijiset.com.
[12] Intila C. Gerardo B. Medina R., (2019) "A study of public key 'e' in RSA algorithm," The International Conference on Information Technology and Digital Applications, IOP Conf. Series: Materials Science and Engineering 482 012016, IOP Publishing, DOI:10.1088/1757-899X/482/1/012016.
[13] Kumar M. (2018), "Advanced RSA Cryptographic Algorithm for Improving Data Security" https://www.researchgate. net/publication/324812723, DOI: 10.1007/978-981-10-8536-9_2.
[14] Thaku P., Rana A., (2016), "A Symmetrical Key Cryptography Analysis using Blowfish Algorithm", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 5 Issue 07.
[15] Choudhary V. and. Praveen N., (2014), "Enhanced RSA Cryptosystem Based On Three Prime Numbers", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, www.ijiset.com.
[16] Abdeldaym R. S., Abd Elkader H. M., Hussein R., (2019), " Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem", I.J. of Electronics and Information Engineering, Vol.10, No.1, PP.51-64, (DOI: 10.6636/IJEIE.201903 10(1).06) 51.
[17] Ch. J. L. Padmaja Ch. J. L., Bhagavan V. S., and Srinivas B., (2016), " RSA Encryption Using Three Mersenne Primes", Int. J. Chem. Sci.: 14(4), 2273-2278, ISSN 0972-768X, www.sad gurupublications.com.
[18] Nisha S., and Farik M., (2017), " RSA Public Key Cryptography Algorithm – A Review", International Journal of Scientific & Technology Research Volume 6, Issue 07, ISSN 2277-8616.

[19] Meneses F., Fuertes W, José S., Santiago Salvador, Daniela Flores, (2016), " RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.8, 55.

[20] Thangav M., Varalakshmi P., Murral M., Nithya K., (2015), " An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)", Journal of Information Security and Applications, Volume 20, Pages 3-10.

[21] Intila C., Gerardo B., Medina R., (2019), " A study of public key 'e' in RSA algorithm", The International Conference on Information Technology and Digital Applications, IOP Conf. Series: Materials Science and Engineering 482. 012016, IOP Publishing, DOI:10.1088/1757-899X/482/1/012016.

[22] Uthman S., (2017), " An Improved RSA based on Double Even Magic Square of order 32 ", Kirkuk University Journal /Scientific Studies (KUJSS), Volume 12, Issue 4, ISSN 1992 – 0849.

Name: Dr. **Taleb A. S. Obaid**.
Date of Birth: 1-7-1952.
Marital status: Married.
Profession: Professor Dr.
e-mail: tasobaid@uobasrah.edu.iq, tasobaid@gmail.com
Department of Computer Information Systems, College of Information Technology, University of Basra, Basra, IRAQ.

Ph. D. "A Computer Simulation of the Flow of Newtonian Liquids", Department of Computer Science, University College of Wales, Swansea, U.K., 1984.

M. Sc. "Numerical analysis and programming", Department of Computer Science and Math, University of Dundee, U.K., 1980.

B.Sc. in Mathematics, University of Basra, Iraq, 1975.