Journal of Engineering and Applied Sciences 14 (21): 7913-7916, 2019
ISSN: 1816-949X

New Approach of RSA Algorithm based on Three-Pass Protocol

Aqeel S. Azez
Department of Technical Computer Engineering, University Al-kafeel College, Najaf, Iraq

Abstract: RSA algorithm is one of the modern cryptography systems that based on asymmetric key encryption algorithms. In this research, we used a Three-Pass Protocol (TPP) method with the (RSA) cryptosystem by combining them, this combination allows senders and the receivers to exchange the messages securely without need to send a public key (e) for them because the proposed combination protocol has this property, so, the integration security of the RSA algorithm is improved. In addition, the implementation of this research shows that the security is improved and it's more efficient comparing with the traditional RSA cryptosystem.

Key words: Cryptography, three-pass protocol, RSA algorithm, cryptography algorithm, TPP, combination

INTRODUCTION

Now a days, the increasing requirement for internet and its applications, impose the need to increase the confidentiality. One of the security mechanisms that increase confidentiality is cryptography because it ensures that all communications are secure (Stallings and Brown, 2008).

The basic two algorithm methods used are symmetric and asymmetric algorithms (Stallings, 2006). Symmetric algorithms use the same key to encrypt and decrypt data. This is generally quite fast when compared with asymmetric algorithm. The problem with this method is in order to decrypt the data the key must be available and distributed securely. For the asymmetric algorithm, this method uses two keys public and private key. The advantage of this type of algorithm is that the security is higher than symmetric algorithm but the problem with this method is that it is slower when compared with symmetric algorithm. So, it is not always suitable for every application (Bellare *et al*., 2000).

To support the security of the asymmetric algorithm that is more secure than symmetric algorithm. In this study, we proposed a new model that combines one of the symmetric algorithms which is RSA cryptosystem with the modern cryptography protocol. This protocol is called three-pass protocol. The first three-pass protocol was developed by Adi Shamir circa in 1980 (Rubin, 2011). The framework of the protocol allows the asymmetric algorithms to send encrypted messages without distributing a public key. The advantage of this study is that we can send messages to other parties without sharing the public key. We will support the security of the RSA cryptosystem in the process of sending messages. The experimental results are discussed with the security and it proved that the approach works and it is secure.

MATERIALS AND METHODS

RSA cryptosystem: RSA is one of the public key encryption forms. In the RSA public-key crypto systems, participants createher/his public and secret key with the following procedures (Thomas *et al*., 2001).

Now a days RSA looks very secure. In the past 20 years of scrutiny, RSA has survived and used worldwide. The attacks that are mostly thought out for RSA are public key factoring. Achieving this, a message written with the public key could be decrypted.

We notice that with a large number, factoring takes illogical amounts of time. Breaking the RSA algorithm has not been confirmedas equivalent to factoring a large number (there might be other, easier methods), on the other hand, it has not been confirmed that factoring is not equivalent. There are dissimilar kinds of attacks on the RSA like: guessing private key (d), searching the message space, common modulus, cycle attack, low exponent, finally factoring and faulty encryption, the variable N that is factoring the public key and it, looks as the best way to go about cracking RSA.

Encryption algorithm relies on its power in some matters. Every algorithm possesses certain features of the mismatches depend heavily on the encryption key, that relies on the arrangements of and denounce it tries to integrate the key with the texts of certain deviations.

The algorithm of RSA dependson the variable N consists of multiplying each of the p and q which depend on finding the variable d. Variable d is the higher value of n. The variable d raises its size, the higher values of p and q the values of d raises. This means that the algorithm relies on adopting the prime numbers because they create a key d, relying on p and q are already prime numbers (Elbaz and Bar-El, 2000).

Three-pass protocol: An interesting cryptographic protocol is the three-pass protocol. The protocol is utilized in a lot of applications (Abdullah *et al*., 2015; Abdullah, 2015). The protocol announces that privacies could be achieved with no advance distributions of the secret key or public key. The protocol suggests that senders and receivers are connected by classical channels that guarantee the opponents can't break or tamper with a message but allow the opponents to read all messages that have been sent over links. The senders and receivers are pretended to have secret-keys encryption systems whose encrypting functions E_k have the commutative properties, that are for all plaintexts P and all keys k_S and k_R:

$$E_{K_S}\left(E_{K_R}(P)\right) \tag{1}$$

This means that the results of dual encryptions are the same whether senders first the key k_S the key k_R or vice versa. The step of the work of the classical three Pass Protocols illustrated as follows:

The senders and receivers randomly select their own private secret key, k_S and k_R, respectively. The sender send a secret plaintext P to receiver, the sender encrypts P with the sender key k_S and then sends the resulting to receiver:

$$C_1 = E_{K_S}(P) \tag{2}$$

Then, the receiver receives C_1, deals with C_1 as plaintext and encrypted C_1 with receiver key k_R. The receiver sends the resulting back to senders:

$$C_1 = E_{K_R}(C_1) = E_{K_R}E_{K_s}\left(E_{K_s}(P)\right) \tag{3}$$

When senders receive C_2, decrypt C_2 with the sender key k_S. Due to the the commutative properties, this remove the previous encryptions by k_S and the result is:

$$C_3 = E^{-1}_{K_s}\left(E_{K_R}\left(E_{K_s}(P)\right)\right) = E^{-1}_{K_s} \left(E_{K_S}\left(E_{K_R}(P)\right)\right) = E_{K_R}(P) \tag{4}$$

Then, the sender sends C_3 back to user receiver. When he receiver receives C_3, decrypts C_3 with the receiver key k_R to obtain the plaintext P that sender has successfully sent it.

In summary, the plaintext delivers securely in a two box to the receivers, the receivers utilizing two keys for opening the two boxes without sharing keys for opening the two boxes, all the procedures for the classical three pass protocol shown in following Fig. 1 and 2.

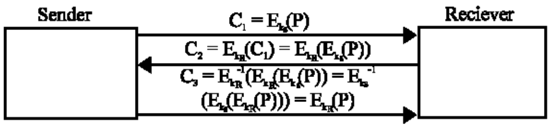
Sender
Reciever
$C_1 = E_{k_S}(P)$
$C_2 = E_{k_R}(C_1) = E_{k_R}(E_{k_S}(P))$
$C_3 = E_{k_R}^{-1}(E_{k_R}(E_{k_S}(P)) = E_{k_S}^{-1}$
$(E_{k_S}(E_{k_R}(P))) = E_{k_R}(P)$

Fig. 1: Three-pass protocol (Abdullah, 2015)

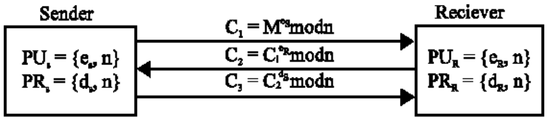

Fig. 2: Proposed algorithm work

Proposed algorithm: The main aim of the proposed algorithm is asecret message exchanges it between the sender and the receiver by using the RSA cryptosystem and they do not need to know the public key for each other. In the processes of encryptions and decryptions of the RSA cryptosystems, the encryption process done twice in a row by the sender and receiver of the message using the RSA algorithm as well as the decryption process performed twice in succession by the receiver and sender of the message. The attributes used are text messages. It is processed through the encryptions and decryptions processes. There are three stages in the process of encryption and decryption of the message. In this combination process using a RSA algorithm to perform encryption and decryption of messages to be sent while for the message delivery process using three pass algorithm protocol.

The following steps are explaining the proposed new approach RSA algorithm work. The sender and receiver agree about a big prime factor (n). The sender send a secret plaintext M to receiver, the sender encrypts M with the sender public key e_S and then sends the resulting to receiver:

$$C_1 = M_s^e \bmod n \tag{5}$$

Then, the receiver receives C_1, deals with C_1 as plaintext and encrypted C_1 with receiver public key e_R. The receiver sends the resulting back to sender:

$$C_2 = E_{e_R}(C_1) = C_1^{e_R} \bmod n \tag{6}$$

When the sender receives C_2, decrypts C_2 with the sender private key d_S and then, the sender sends C_3 back to user receiver:

$$C_3 = E_{d_s}(C_2) = C_2^{d_s} \bmod n \tag{7}$$

When he receiver receives C_3, decrypts C_3 with the receiver private key d_R to obtain the plaintext M that sender has successfully sent it. In summary, the new approach of RSA algorithm success to send the message M securely without sharing any keys and this the main point of the study and the difference with the RSA algorithm, all the procedure for the new approach of RSA algorithm as shown in following Fig. 2.

RESULTS AND DISCUSSION

The five different characters are given to the RSA algorithm and the new approach of RSA algorithm as input to check the performance. Experiments are conducted on the machine [Intel® Core™i7-3520M CPU G 630 @ 2.90 GHz, 8GB of RAM]. The operating systems and systems software utilized for this algorithmare C#2010 and Windows 10 Enterprise.

Performances measurement criterionis time taken by the algorithm for performing the encryptions and decryptions of the input texts. The encryptions computation time and decryptions computation time are the parameter which calculates the performances of an algorithm. The encryptions computation time are the time which taken by the algorithmfor producing the cipher texts from the plain texts. The encryptions time could be utilized for calculating the encryptions throughput of the algorithm. The decryptions computation time is the time taken by the algorithm for producing the plain texts from the cipher texts. The decryptions time could be utilizedfor calculating the decryptions through put of the algorithm.

Table 1 shows the five dissimilar features and corresponding encryptions and decryptions execution time taken by RSA algorithms and the new approach of RSA algorithm in the matter of seconds. By analyzing Table 1, we notice that the encryptions time and decryptions time taken by RSA is very small when compared to the new approach of RSA algorithm and this does not effect the implementation of the new approach of RSA algorithm and this is clear in Fig. 3.

The Table 2 shows the five dissimilar characters and corresponding through put taken by RSA algorithm and the new approach of RSA algorithm. The analysis of Table 2, we noticed that the throughput taken by RSA is very small when compared withthe new approach of RSA algorithm also we noticed in the Fig. 4 there is not big different in the throughput between RSA and the new approach of RSA algorithm.

The basic point of this study lies in security. We have seen the security of the proposed approach is better than RSA algorithm. The security of the new approach of RSA is based on TPP protocol. Now, we give short argument given for the security of the proposal. Given a ciphertext $C_1 = E(M^{e_s} \bmod n)$, an enemy can not drive E without information of e^s. Given a ciphertext $C_2 = E(C_1^{e_R} \bmod n)$ an enemy cannot drive E without information of e^s and e^R. Given a ciphertext $C3 = E\ (C_2^{L_s} \bmod n)$ an enemy cannot drive E without information of d^s, e^R.

Table 1: Processing time for the RSA and the new approach of RSA algorithms

No. of chars	New approach of RSA time (msec)	RSA time (msec)
500	2584	864
1000	11157	3527
1500	28251	8350
2000	52489	16093
2500	99823	31381

Table 2: Throughput for the RSA and the new approach of RSA algorithms

	Through put	
No. of chars	New approach of RSA	RSA
500	0.1697	0.5833
1000	0.0903	0.2857
1500	0.0535	0.1810
2000	0.0384	0.1252
2500	0.0251	0.0800

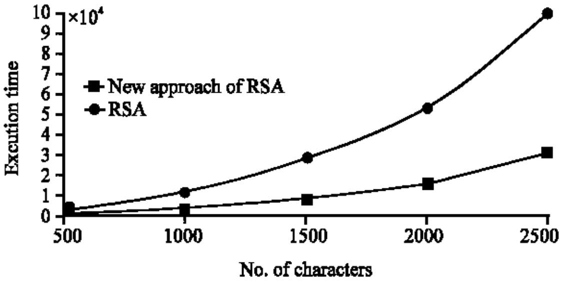

Fig. 3: Processing time for the RSA and the new approach of RSA algorithms

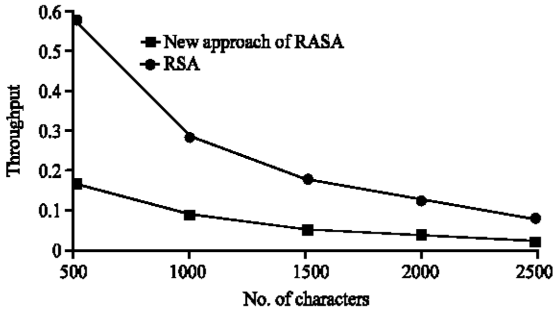

Fig. 4: Throughput for the RSA and the new approach of RSA algorithms

CONCLUSION

Two dissimilar keys are utilized in public key cryptography. One of the keys is utilized for encryptions and the other corresponding keys must be utiized for decryptions. No other keys can decrypt the messages, not even the original (i.e., the first). Key sutilized for encryptions. The good thing of this scheme is that all communicating parties need just key pairs for communicating with the values of the prime factor (n) and there is no need for sharing the public key (e) for both parties. RSA cryptosy stemsecurity depends on two mathematical issues: the first one is factoring large numbers know mathematical attack. The second one is trying all possible keys know brute force attacks. So, the new approach of RSA algorithm develops the security, it is secure when compared to RSA as it is relied on the factoring problem andsharing the public keys of both parties.

REFERENCES

Abdullah, A.A., 2015. Modified quantum three pass protocol based on hybrid cryptosystem. Ph.D Thesis, Eastern Mediterranean University, Famagusta, Northern Cyprus.

Abdullah, A.A., R. Khalaf and M. Riza, 2015. A realizable quantum three-pass protocol authentication based on hill-cipher algorithm. Math. Prob. Eng., 2015: 1-6.

Bellare, M., A. Boldyreva and S. Micali, 2000. Public-key encryption in a multi-user setting: Security proofs and improvements. Proceedings of the International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT 2000), May 14-18, 2000, Springer, Berlin, Germany, ISBN:978-3-540-67517-4, pp: 259-274.

Elbaz, L. and H. Bar-El, 2000. Strength assessment of encryption algorithms. Master Thesis, Discretix Technologies Ltd, Santa Clara, California, USA.

Rubin, F., 2011. Device, system and method for fast secure message encryption without key distribution. U.S. Patent and Trademark Office, Washington, DC. USA. https://patents.google.com/patent/US7907723B2/en

Stallings, W. and L. Brown, 2008. Computer Security: Principles and Practice. Pearson Education India, India, ISBN:9788131733516, Pages: 799.

Stallings, W., 2006. Cryptography and Network Security: Principles and Practices. 3rd Edn., Pearson Education India, New Dehli, India, ISBN: 978-1-25-902988-2, Pages: 492.

Thomas, C.H., C.E. Leiserson, R.L. Rivest and C. Stein, 2001. 2.3: Designing Algorithms. In: Introduction to Algorithms, Thomas, C.H., C.E. Leiserson, R.L. Rivest and C. Stein (Eds.). MIT Press, Massachusetts, USA., ISBN:9780262032933, pp: 27-37.