Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange

Research · October 2018

DOI: 10.13140/RG.2.2.30495.61602

CITATION
1

READS
2,674

3 authors, including:

Abdul Ghaffar Khan
University of Management and Technology (Pakistan)
7 PUBLICATIONS **32** CITATIONS
SEE PROFILE

Muhammad Usama Riaz
University of Management and Technology (Pakistan)
5 PUBLICATIONS **28** CITATIONS
SEE PROFILE

Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange

Abdul Ghaffar Khan, Sana Basharat, Muhammad Usama Riaz

Abstract— Asymmetric cryptography is a cryptographic system in which public and private keys uses as a pair. Public key dispersed publicly and the other side private key known by owner only. Public key is very efficient for authentication as well as for encryption. Public key for encrypt (conversion form data or information to code) and private key for decrypt (reciprocal of encryption or reverse process of encryption) a message. Nowadays a very difficult to decide the key length to use for proper information security. The long length of the keys takes huge time, but more security. In this article, we propose that to explore authentication and confidentiality of information during transportation by implementing the RSA algorithm. Rivest-Shamir-Adleman (RSA) algorithm widely use in asymmetric (public key) cryptography for encryption and decryption of information

Index Terms— Asymmetric Cryptography, authentication, Cryptography, Confidentiality, Information security, RSA algorithm.

1 Introduction

Asymmetric key is also known as a public key. Key pairs (public, private) used in asymmetric cryptography where public key distributed publicly and private key used on the decryption side to convert the cipher text in plain text. Highly use of the asymmetric key is to secure exchange of communication on the internet. For encryption of asymmetric key, we use the RSA algorithm for better and secure transaction on the internet. Asymmetric is the little bit slower rather than symmetric due to computations on cryptography of asymmetric key. SSL is the well-known example where the asymmetric key is used for safe and secure communication on the internet. In this article, we propose that how to maintain authentication and confidentiality of information during transportation by implementing the RSA algorithm, where it will ensure confidentiality of information. RSA algorithm widely uses in asymmetric cryptography for encryption and decryption of information. Remember that confidentiality means protection of message from observer and authentication means that the receiver needs assurance as the identity of the sender.

2 Related work

In this paper [1] they highlighted the RSA's computational complexity, encryption and authentication of asymmetric. In symmetric cryptosystems, the sender and receiver key either same or ease to compute them. But the other hand, where we cannot have the same case like symmetric, we have three possible ways. 1) Forward asymmetric: Here private key is very difficult to be computed given sender's key. 2) Backward asymmetric: At this point public key is very tough to be computed given receiver's key. 3) Bidirectional asymmetric: Both public and private keys cannot be computed given the other. Bidirectional encryption has to two characteristics .1) Secure communication is possible. Even sender's key has been compromised during communication. Its use in forward asymmetric encryption.2) Sender's message authentication is possible, even if receiver key's compromised. It uses in the backward encryption system. Factorization trapdoor is a public key encryption concept RSA. It can find prime numbers in time O(d3), if we take large number(n) than its complexity of factoring exceeds from any polynomial limit. Now O(n(ln(ln n)/ln n)1/2).In Suggested system p and q are pairs of primes so n=pq is away from all expected computational capabilities. Pairs of e and d where (e, φ(n)) =1and ed≡ 1 mod φ(n); φ(n)=(p-1) (q-1). Here e and d are the multiplicative inverse of remains classes modulo φ(n). When we start cryptosystem as public keys, e and n goes in public key list and d is set aside secret. The receiver knows p and q, the system is forward asymmetric.

In paper [2] they focus on cryptography techniques as they mention in conclusion that a cryptographic scheme that comprises symmetric and asymmetric algorithms is projected for securing safe data transmission via satellite-based communication channel. Java programming is used to develop software based on this scheme. Results show that, by utilizing information confidentiality, integrity and information authentication, which are the essential features for information security in satellite-based communication. They discussed confidentiality, integrity; authentication and identification are the key properties of proposed scheme. In authentication and identification by using a hashing algorithm with a combination of asymmetric algorithm and it gives the digital signature which provides assurance for validity of origin of the information. IDEA (utilize 128 bit key), RSA (1024 bit key) and MD5 (128 bits hash) algorithms are used for secured communication

Here [3] they have seen a complete analysis of the asymmetric key algorithms. Author of this paper publicize a picture of their encryption and decryption procedures to categorize their current gap grounded on ending drawn from the analysis, with certain weight on an algorithm utmost well-matched for industrial ap-

plication specified the current inclinations in cryptography in the direction of quantum computing. The earnest necessity for an algorithm that has nearly no trade-off in encryption and decryption work action speed has low computation above and is protected sufficient to resist quantum algorithm attacks. In this paper author totally target on the public key cryptography algorithms. It is very important to notice that private key algorithms almost so far faster as I have said that 2 to 3 orders of degree faster than public key methods or algorithms. However, public key algorithms offer extra higher security and have extensive enactment. Author tried to provides a in order understanding for the development of different keys especially public key algorithms. According to a performance evaluation conducted in 2000, in comparison to RSAI024 and ECC168 (EcElGamal), NTRU had the fastest encryption, decryption and key generation speed. NTRUs speed was approximately two orders of magnitude more rapidly than ECC (in a CPU). However, NTRU had the largest public key size and the message expansion is twice as much as that of ECC at an equivalent security level.

In this paper [4], author given a sketch on implementation of cryptography and briefly discussed on symmetric and asymmetric cryptography. Embedded hardware and software were target of author where to implement cryptosystem. They tell the difference or distinguish symmetric and asymmetric ciphers, because the latter offers more security functionality and therefore have different application scenarios. Symmetric ciphers serve primarily used for text or string which sent to check its integrity, secondly it used for entity authentication, thirdly and at the last is used to check encryption.

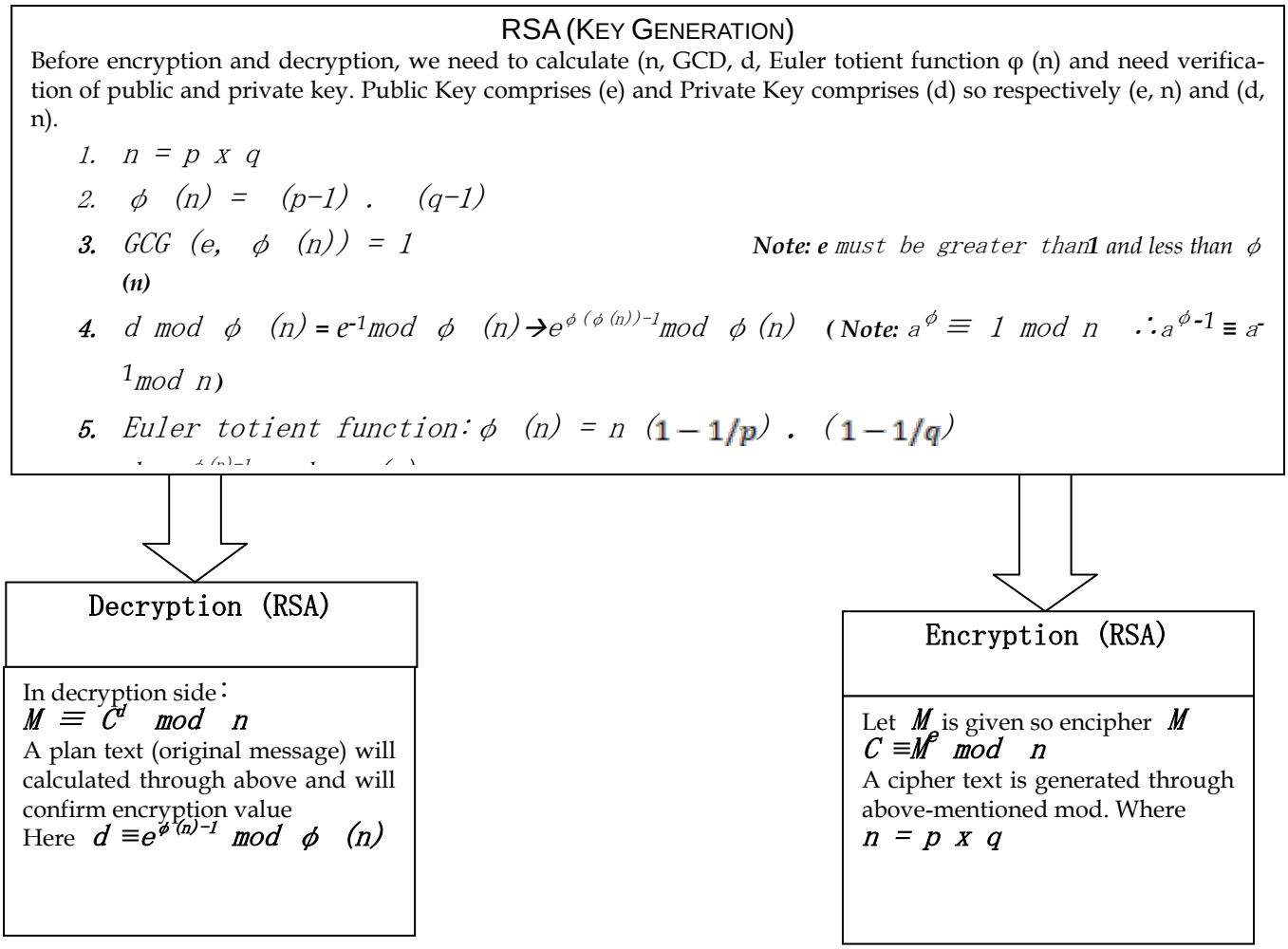
In this paper [5] they have discussed literature reviews the daily used algorithms, in consort with the anticipated algorithms based on their positivity and negativity, associated to Symmetric and Asymmetric Key Cryptography. They have also likened the value of mutually these techniques. The anticipated algorithms showed to be cryptographic extremely well-organized in their particular grounds but there is a related part that persisted open, interrelated to these algorithms, and have still not been thoroughly discussed. This paper [5] also presents an appropriate future scope associated to these open fields. They have highlighted the basic as well as proposed algorithms related to these cryptographic (encryption and decryption) methods. The public key will remain open or public and the private keys not shared. This technique ensures better security than the former. Furthermore, the main part which make data highly confidential and non-repudiation is the use of digital signature.

3 Problem Statement

In this cryptographic scenario, it is very hard to achieve authentication and confidentiality with integrity just in a single step. In public key encryption and decryption carry out with a dissimilar key, but where symmetric key will not be as like shareable entity. As like asymmetric key cryptography where we use symmetric key for encryption of message, but using its public key anyone can decrypt the message. When we attempt to achieve authentication, then it is difficult to maintain confidentiality. When we use a public key for the purpose to encrypt the message, only anticipated receiver can decrypt the message. Here we managed confidentiality, but simultaneously we cannot maintain authorize the sender. Now we need to overcome the above-mentioned problem. For this, after private key we use public key encryption. After that, only anticipated recipient would be capable to decrypt the message and simultaneously he will also be capable to check the authenticity sender by decrypting cipher message using public key.

4 RSA Algorithm For Authentication And Confidentiality

RSA implementation form initialization of a message from encryption side to decryption of a message is given below, for general sketch about RSA implementation and their corresponding steps. Confidentiality and proper confirmation of message is given in below example.



4.1 IMPLEMENTATION OF RSA ALGORITHMS

i. Key Generation

First of all we need to generate two distinct but random prime numbers like p and q.

Let suppose p= 11, q= 5 so

n = p x q→ (11). (5)=55

So key length is 55

φ (n) = (p-1) . (q-1)→(11-1). (5-1)

φ (n) = 40

e = 3

Note: e must be greater than1 and less than φ **(n)**

GCD calculation through Euclidean Algorithm

40 = 3(13) + 1

3= 1(3) + 0

So (3, 40) = 1

Here GCD (e, φ (n)) = 1,

Calculation of d by following steps number 4 to onward from (**Error! Reference source not found.**) declaration as we know that

$d.e \equiv 1 \mod \phi(n)$

$d \mod \phi(n) = e^{-1} \mod \phi(n) \rightarrow e^{\phi(\phi(n))1} \mod \phi(n)$

(Note: $a\varphi \equiv 1 \mod n \ \therefore a^{\phi-1} \equiv a^{-1} \mod n$)

$d \mod \varphi(n) = e^{\phi(n)-1} \mod \varphi(n)$

$d \mod \varphi(n) = e^{40-1} \mod 40$

$d \mod \varphi(n) = e^{39} \mod 40$

→Euler totient function←

$\varphi(n) = n\,(1 - 1/p)\,.\,(1 - 1/q)$

$\varphi(40) = 40(1-1/2).(1-1/5)$

$\varphi(40) = 16$

Now $d \equiv e^{\phi(n)-1} \mod \varphi(n)$

$d \equiv e^{16-1} \mod 40$

$d \equiv e^{15} \mod 40$

$d \equiv e^{8+4+2+1} \mod 40$

$d \equiv e^8 . e^4 . e^2 . e^1 \mod 40$

$d \equiv 1^8 . 1^4 . 3^2 . 3^1 \mod 40$

$d \equiv 1.1.9.3 \mod 40$

$d \equiv 27 \mod 40$

→**Verification** ←

Public Key (e ,n)

Private Key (d, n)

We know that

$d.e \equiv 1 \mod \varphi(n)$

so,

$(27.3) \equiv 1 \mod 40$

$81 \equiv 1 \mod 40$

It satisfies the relation

$d.e \bmod (n) = 1$

ii. Encryption

Let M = 8,

$C \equiv Me \mod n$

$C \equiv 83 \mod 55$

$C \equiv 82+1 \mod 55$

$C \equiv 82.81 \mod 55$

$C \equiv 9.8 \mod 55$

$C \equiv 72 \mod 55$

$C \equiv 17 \mod 55$

Decryption

$M \equiv Cd \mod n$

$M \equiv 1727 \mod 55$

$M \equiv 1716+8+2+1 \mod 55$

$M \equiv 1716.178.172\ .171 \mod 55$

$M \equiv 16.26.14.17 \mod 55$

$M \equiv 99008 \mod 55$

$M \equiv 8 \mod 55$

Here decryption successfully done.

4.2 Confidentiality and Authentication

In introduction as we discussed that confidentiality mean protection of message from observer and authentication mean that receiver needs assurance as the identity of sender. In following figure 1; PUA and PRA are respectively designated as public and private keys, same like above PUB and PRB are respectively designated as public and private keys. In figure 1; A wants to send a message to B by maintaining confidentiality and authentication.

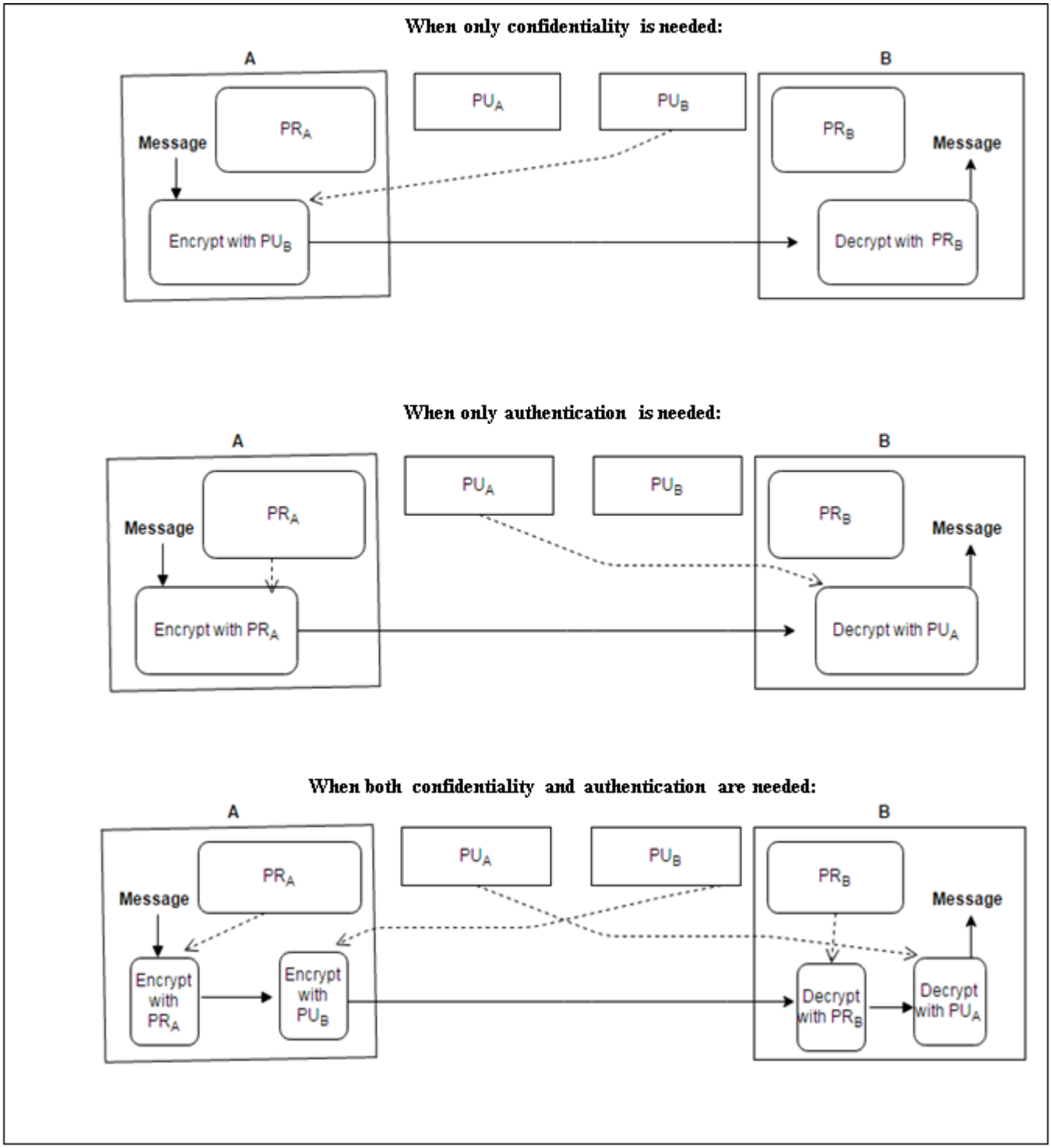


Figure 1: A wants to send a message/text to B

In figure 1 we have shown that how asymmetric key cryptography can be used for confidentiality and as well as for digital signatures. The steps undertaken by A to convert message into encrypted form C is given below: C= $E(PU_B, E(PR_A, Message))$ here E denoting encryption. B side to recover message from C are given $\rightarrow Message = D(PU_A, D(PR_B, C))$ here D denoting decryption. So, as we have seen that sender A encrypt message through its own private key PR_Awhich provides authentication. The sender A encrypting message with its personal private key PR_A gives authentication. This step comprises A putting digital signature on the message. Instead of applying the private key to the whole message, a dispatcher may also "sign" a message by applying private key to just a minute block of data that is resultant from the message to be sent. The cost compensated for achieving confidentiality and authentication simultaneously is that now the message must be processed 4 times in all for encryption and decryption. Tow encryptions of message will do on the side of the sender and two decryptions on the side of the receiver. Every of these four steps involve independently the computationally complex public-key algorithm. Public-key cryptography does not make outdated the more conventional symmetric-key cryptography. Larger computational aloft is reason which connected with public-key cryptographic systems. However, public-key encryption has proved crucial for key management, for distributing the keys needed for the more conventional symmetric key encryption and decryption of the content, for digital signature applications, etc.

5 Implementation & Key Generation

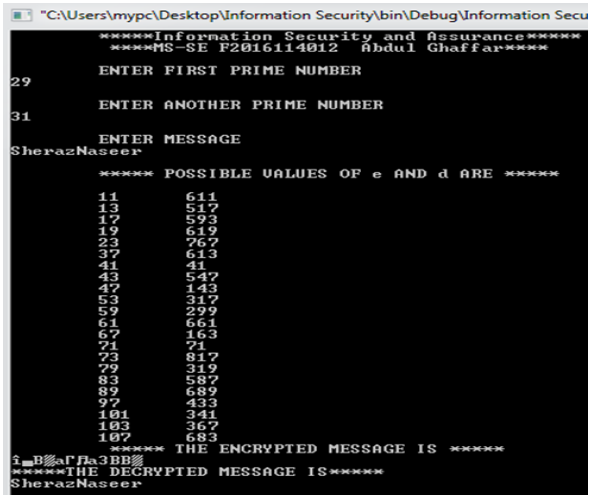


Figure 2: RSA implementation in C

When we increase key size, key generation time increase.

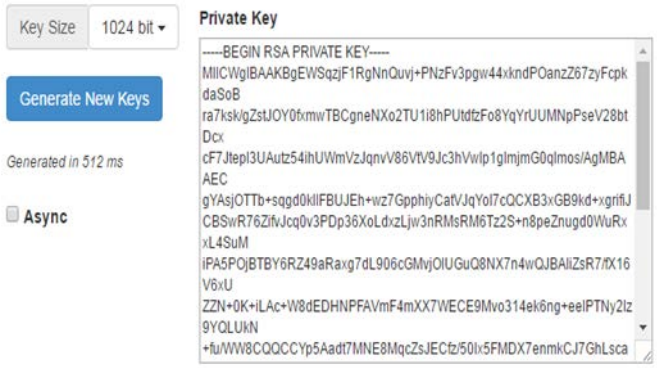


Figure 3 Key Size 1024 bit and Key Generation Time 512 ms.

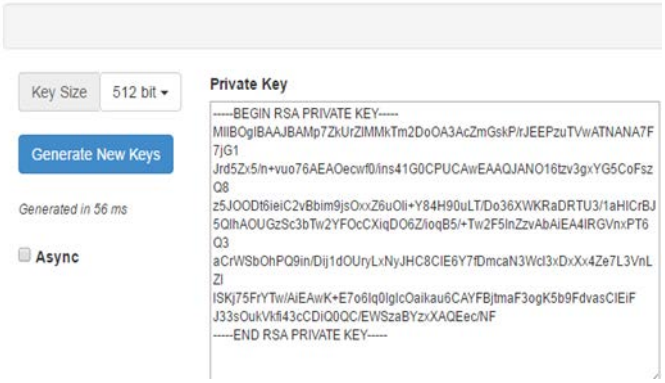


Figure 4 Key Size 512 bit and Key Generation Time 56 ms

6 Conclusions

In this paper, we try to analyze, ensure the confidentiality and authentication in information during sharing through cryptography of asymmetric key. As we discussed that confidentiality mean protection of message from observer and authentication mean that receiver needs assurance as the identity of sender. In figure 1 we show a detailed concept how to attain confidentiality and authentication of information. We implemented RSA algorithm for encryption and decryption. We also analyze that when we increase the key size in RSA algorithm than key generation time increase respectively as we show in figure 3, 4.

References:

[1] Symmetric and asymmetric encryption
[2] GJ Simmons - ACM Computing Surveys (CSUR), 1979 - dl.acm.org
[3] Secure Communication using Symmetric and Asymmetric Cryptographic Techniques
[4] OM Barukab, AI Khan, MS Shaik… - International …, 2012 - search.proquest.com
[5] A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap JN Gaithuru, M Bakhtiari, M Salleh… - … (MySEC), 2015 9th …, 2015 - ieeexplore.ieee.org
[6] A survey of lightweight-cryptography implementations
[7] A comparative survey of symmetric and asymmetric key cryptography S Chandra, S Paira, SS Alam… - Electronics, …, 2014 - ieeexplore.ieee.org
[8] Double Chaining Algorithm A Secure Symmetric-key Encryption Algorithm
[9] A comparative survey of symmetric and asymmetric key cryptography