International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Privacy Preserving Using Extended Euclidean Algorithm Applied To RSA-Homomorphic Encryption Technique

D.Chandravathi , P.V.Lakshmi

Abstract: ***Communication of confidential information over Internet is the key aspect of security applications. Providing protection to sensitive information is of major concern. Many cryptographic algorithms have been in use for providing security of confidential information. Providing security for data has become major challenge in this era. Classical cryptography is playing a major role in providing security for applications. In modern days securing confidential information in the cloud is considered as an important challenge. Homomorphic Encryption technique is one of the best solutions that provide security in the cloud[1]. In this paper, Extended Euclidean Algorithm is used for generating keys. This technique follows RSA Homomorphic encryption technique. .RSA Homomorphic encryption using Extended Euclidean algorithm (RSA-HE-EEA) is secure when compared to RSA as it based on the generation of private key which makes the algorithm complex .This technique of using Extended Euclidean Algorithm(EEA) is fast and secure when compared to RSA homomorphic encryption technique. The encryption process utilizes modulo operator which gives security as well.The beauty of this algorithm is in generation of private key which uses Extended Euclidean Algorithm (EEA) that helps in avoiding brute force attacks. Also, this technique uses Homomorphic operations which gives enhance security to confidential information in the cloud.***

Keywords: ***Classical Cryptography, Homomorphic encryption, RSA, EEA, private key, brute force attack.***

I. INTRODUCTION

In the world of computers, data communication plays a vital role. Confidential information is shared among different systems through Internet. There is a large misuse of Data tampering and attacks as well. So, Security of data is of major concern[2]. Cryptography plays an important role for providing security and also ensures with a secure communication of data over Internet. One of principle of cryptographic technique is to grant security of sensitive information which is functioned with digital signature, authentication, verification and validation, system security and etc. Hence, encryption techniques ensure that the information's confidentiality, integrity and consistency, attacks and forgery and counterfeiting are prevented. Classical Cryptography defines a pair of transformation with encryption and decryption process.

Manuscript published on 30 August 2019.
***Correspondence Author(s)**
D.Chandravathi, GVP College for Degree and PG courses (A), Rushikonda, Viakhapatnam-45
Prof.P.V.Lakshmi, GITAM University, Rushikonda, Viakhapatnam-45.

In Encryption process, the original plain text is encoded with help of encryption key to produce cipher text. In decryption Process, the cipher text is decoded using decryption key to obtain the original plain text[2][4]. If the encryption process and the decryption are done with the same key then it is symmetric key cryptography. This type is frequently prone to attacks and can be cracked easily. Hence, in 1976 Public key Cryptosystems was introduced to protect the mechanism. This was proposed by two great researches from Stanford University namely Whitfield Diffe and Martin Hellman.

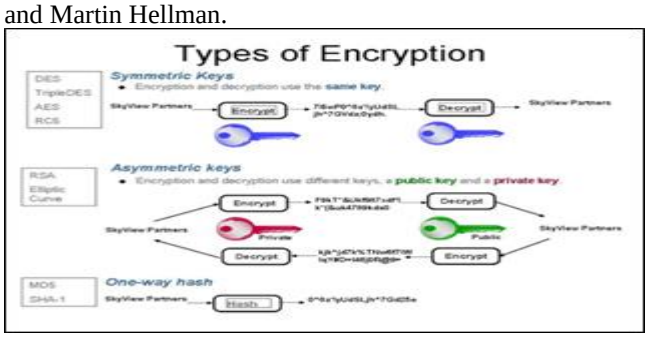

Fig 1

The Public key cryptosystems uses a pair of related keys for encryption and decryption. The mechanism utilizes public key for encoding the message and private key to decode it. The private key is kept secret where as the public key is known to all[5]. The mechanism is applied by using public key for encryption and the message can be decrypted only by using the private key. Hence, it becomes difficult to decrypt unless private key is known, which ensures security for confidential information. RSA is the best known and most widely used public key system which was proposed by RL Rivest in 1978.It follows the asymmetric (public key) cryptosystem which is based on number theory. This technique is secure since it uses large number prime factorization method which is a well-known mathematical problem that has no effective solution.

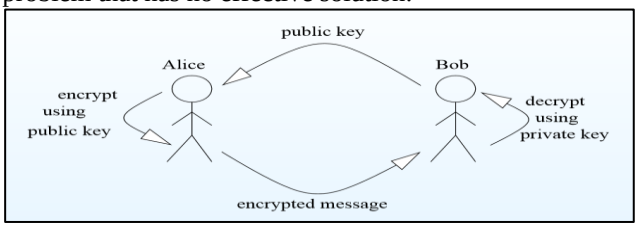

Fig 2

1. RSA Algorithm

The RSA scheme has involves three stages:

1. Key Generation process.
2. Encoding/Encryption process.
3. Decoding/Decryption process.

In RSA scheme, the process of encryption is followed by encrypting the plain text using public key of the sender and include it in public file which is denoted by 'E(n)'. Later, decryption process is carried out using sender's private key. The resultant cipher text is denoted by 'D(n)'[3]. The properties of RSA scheme is as follows:

1. Decryption process is done with the expression as D(n) * E(n(M)) = M, to get the original plain message.
2. Derive the values of E(n) , D(n).
3. None can compute the value of 'D(n)' by revealing 'E(n)'. Computing the value of 'D(n)' is done by the user followed by decrypting messages which were encoded with 'E(n)'.
4. Decrypting a message and then encoding it, results in original message i.e.,
5. En (Dn(M)) = M.

Researchers , Rivest, Shamir, and Adleman, observed that if a procedure satisfying third property is applied, it is extremely impractical for another user to try to decrypt the message by trying all possible messages until they find one such that E(n(M)) = C.

II HOMOMORPHIC ENCRYPTION SCHEME

Background

In 1978, Rivest, Adleman and Dertouzos first proposed an encryption scheme that worked with exponentiation function. This function utilises additive and multiplicative privacy homomorphisms which performed computations on encrypted data. But none of the functions by themselves provides the security for chosen plaintext[3].

Definition

A homomorphic cryptosystem is a cryptosystem which has set of possible plaintexts 'P' and set of possible cipher texts 'C' such that for any K ∈ K and any two ciphertexts c1 = e_K(m1), c2 = e_K(m2), the following condition holds: d_K(c1* c2) = m1* m2 , where * represents the respective group operations in 'C' and 'M'.

The aim of homomorphic encryption scheme is to ensure secure communication and storage with data privacy. We have several encryption schemes and one such scheme is RSA scheme which is multiplicative homomorphic .RSA scheme computes the product of cipher text and generates the result which is equal to the product of the original plain texts[11].

In 2009, fully homomorphic encryption was first introduced by the Gentry. He achieved "Somewhat Encryption Scheme "which limits only for few operations to be carried on encrypted data. The major operations are multiplication and addition. RSA does not support the addition operation. RSA works with multiplication operation. Fully Homomorphic scheme can be implemented by performing both addition and multiplication operations on the cipher text.

Fig 3

Gentry observed that the encryption functions Enc (x1) and Enc (y1) are easily computed from Enc (x1 + y1) and Enc (x1 * y1). Since noise is attached with each of the operation on the cipher text, there where limitations on the operations. To avoid the noise problem in the cipher text, Craig introduced a technique of bootstrape which converts the scheme into the Fully Homomorphic Scheme. Gentry's idea was to build a Cryptosystem with usual encryption and decryption function that encodes and decodes cipher text from plain text and vice-versa. The major applications of homomorphic encryption are in the cloud computing domain since the data is stored in encipherd format in cloud.Today, there are several partially homomorphic cryptosystems available along with many fully homomorphic cryptosystems. Any cryptosystem is malleable unintentionally and might be subjected to various types of attacks .This problem can be treated carefully with homomorphic operations that performs computations securely[2]. Viz.,

1. Partially- Homomorphic- Cryptosystems

- ELGAMAL cryptosystems
- Unpadded- RSA crypto systems.
- Micali and Goldwasser cryptosystems.
- Paillier cryptosystems.
- Benaloh cryptosystems
- Other partially homomorphic cryptosystems.

2. Fully Homomorphic Cryptosystems

- Traditional homomorphic cryptosystems, like
- ✓ Gentry's cryptosystem.
- ✓ Cryptosystem using integers.
- Second generation homomorphic cryptosystems.

III PROPOSED METHOD

The proposed method mainly focuses on the private key value generation. Classical RSA technique applies Euclidean Theorem for generating the'd' values which is considered to be the private key. This is done by taking the public key 'e' and the finding the relative primes 'e'. By doing so, we have avoided bruteforce attacks for finding the private key value to some extent[5].

Retrieval Number: J12360881019/19©BEIESP
DOI: 10.35940/ijitee.J1236.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

But still security is at vein. So, to overcome this problem Extended Euclidean Algorithm(EEA) plays a very important role which generates the secret key.Its highly impossible to find the 'd' value . Also, homomorphic operations on the encrypted cipher gives enhanced security for the data that is stored in the cloud. Hence, privacy is preserved.The proposed method applies various Theorems for RSA-Homomorphi encryption cryptosystem with Extended Euclidean Theorem.

Theorem 1:

Integer Factorization Problem

This method is most commonly used for providing security in many cryptographic algorithms. Suppose 'n1' be a positive integer such that

$N1 = p1^{e1} * p2^{e2} * \ldots * pk^{ek}$, where p_i is the pair wise distinct primes and $e_i <= 1$.

Let 'a',' b' be m-digit number and n-digit numbers respectively . Then the product n1= (a * b) has a time complexity of Order of m * n. If 'N1' is a large number, then finding the factors of 'N1' becomes exponentially complex. Hence, this class belongs to NP.RSA crypto system has been implemented basing on this factorization method. In the present scenario for public and private sectors the utilization provides more security.

Theorem 2:

The Powers of an Integer, Modulo n

Euler's Theorem states that, for every 'a_i' and 'n_i' which is relatively prime is represented as:

$$a_i^{\emptyset(n_i)} \equiv 1 \pmod{(n_i)},$$

where $\emptyset(n_i)$ denotes the Euler's function which is a positive integer less than 'n_i' and which are relatively prime to 'n_i'. Let the expression be :

1.

Table 1

Row	a	b	Ø(n)	e
1	1	0	Ø(n)	-
2	0	1	e	k_1
3	a_3	b_3	e_1	k_2
. . .	. . .	. . .	. . .	. . .
i	a_i	b_i	e_i	k_i
.	.	x .	y .	.
.	.	.	.	.
k	a_k	b_k	1	K_k

$$a_i^{\emptyset(ni)} \equiv 1 \bmod (n_i).$$

If 'm_i' and 'a_i' are relative prime numbers, then there exist at least one integer, 'm', that satisfies the equation as :

$$m = \emptyset(n_i).$$

The exponent 'm', can be referred in many ways as:

1) Order of Mod(a_i , n_i).
2) The exponent to which 'a_i' belongs to (Mod n_i).
3) The period length generated by 'a_i'.

Theorem 3:

Euler's Theorem and Fermat's Theorem

These theorems play a predominant role in number theory and modular arithmetic. They are used in modular calculations and also to find the inverse. Fermat's theorem states that if a prime number 'p1' and an integer 'a_i' does not divide such that 'p1' does not divide 'a_i', then $a_i^{p1-1} = [1 \pmod{p1}]$, where '$a_i$' is relative- prime to 'p1'.

According to Euler's theorem, an integer 'a' is said to be relative prime to 'n_i', if $a_i^{\emptyset(n_i)} \equiv \text{Mod}(1, n_i)$, such that $\emptyset(n_i)$ is the Euler's Function.If 'p1' is prime, then $\emptyset(n_i) = p1 - 1$ is observed as special case for Fermat's theorem .

Theorem 4: Euclidean Theorem

Let a,b two non-negative numbers such that the largest number divides both a and b.we denote this as gcd(a,b)=1.If gcd(a, b) = 1 then we say that *a* and *b* are **coprime** or **relatively prime**. The gcd is sometimes called the highest common factor (hcf).

Theorem 5: Extended Euclidean Theorem

Let a,b be two non-negative numbers and let x,y denote two integers such that ax+by = gcd(a,b) where a>b.

IV ALGORITHM

RSA Homomorphic Encryption technique using Extended Euclidean Algorithm

1. Select two large prime numbers p,q.
2. Derive the value of n as n=(p*q).
3. Calculate the totient value as Ø(n)= [(p-1)* (q-1)].
4. Choose 'e' such that the value is relatively prime.
5. Compute 'd' by using Extended Euclidean Algorithm

Extended Euclidean Algorithm:

The Extended Euclidean Algorithm has the equation as

$$[\emptyset(n)]x + ey = \gcd(\emptyset(n), e),$$

where Ø(n) and 'e' are generated as shown above. In order to find the values of x,y the steps are as follows:

2. A table is constructed comprising the values of a,b, Ø(n),e is shown below.
   The values of $a_3,a_4,a_5,\ldots a_k$ is computed by using the equation $a_n = a_{[(n-1)-1]} - a_{(n-1)}[k_{(n-1)}]$.
3. The values of $b_3,b_4,b_5,\ldots b_k$ is computed by using the equation $b_n = b_{[(n-1)-1]} - b_{(n-1)}[k_{(n-1)}]$.
4. Derive d_n as $d_n = d_{[(n-1)-1]} - d_{(n-1)}[e_{n-1}]$.
5. The value of e_n is obtained by
   $e_n = d_{[(n-1)-1]} / d_{n-1}$.
6. The table is formulated until **Ø(n)** becomes 1.

7. From the above table the values of x and y are obtained as shown.
8. Substitute the values of x,y in the given equation : Ø(n) x+ey=GCD(Ø(n),e) ,which yields 'd' value, known as private key.
9. The conditions for selecting 'd' value are:
   i. If d> **Ø(n)** , then d = d mod **Ø(n).**
   ii. If d<0 , then d= d + Ø(n).
10. The generated 'd' value is the private key for decryption process.

RSA Homomorphic encryption process:

Encryption: $C = [M^E \mod Ø(N)]$.

The sender 'A' does the following :

- Obtain the recipients B's public key (n , e).
- Compute the cipher text into two cipher text as c1 and c2.
- c1=[a^e mod n] , c2 =[b^e mod n] .
- Sends the C= [(c1*c2)^e mod n] to B.

Decryption algorithm:

The Recipient B does as follows:

- Uses this key (n , d) to compute the original message as M = [(c1*c2)^d mod n].

V RESULTS

From the Table 2, it is clear that for different file sizes which is taken in kilobytes, we have calculated the total encryption time and total decryption time for each file size .It is clear that the decryption process is lesser when compared to RSA Techniques. Homomorphic operations minimizes the process of decryption which makes the technique stronger that classical RSA and no person can identify what the information is and cannot access it without knowing the private key which is generated by using EEA. Hence, privacy is preserved.

Table 2

File Size (KB)	eTime (msec)	dTime (msec)
10	8	5
20	12	10
50	75	73
80	96	93
100	154	151
120	178	170
150	232	228
200	301	293
300	487	476
500	858	843

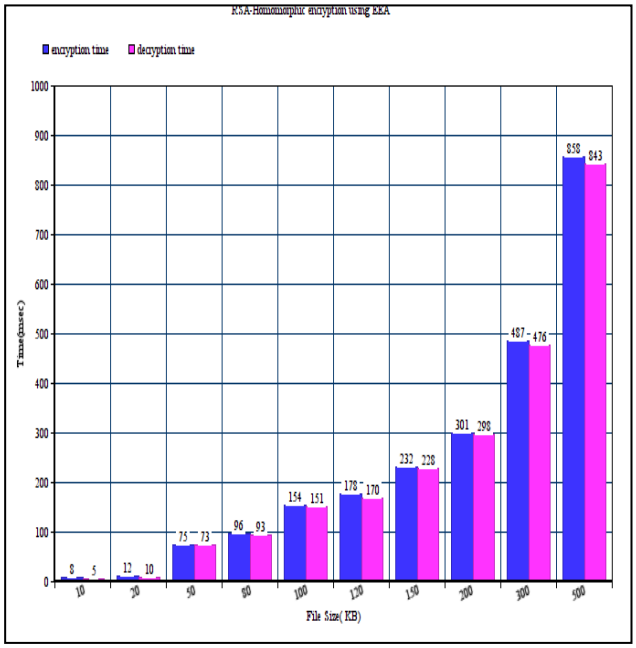

Fig 4

VI CONCLUSION

In modern days securing confidential information in the cloud is considered as an important challenge. Homomorphic Encryption technique is one of the best solutions that provide security in the cloud. The proposed Technique using Extended Euclidean Algorithm provides enhanced security for the private key. RSA Homomorphic encryption using Extended Euclidean algorithm (RSA-HE-EEA) is secure when compared to RSA as it based on the generation of private key which makes the algorithm complex .This technique of using Extended Euclidean Algorithm(EEA) is fast and secure when compared to RSA homomorphic encryption technique. Hence, privacy is preserved.

REFERENCES

1. Maheswari Losetti, Kanaka Raju Gariga "An Enhanced Rsa Algorithm for Low Computational Devices" International Journal of Advanced,Research and Innovations Vol.1, Issue .2, pp 114-118.
2. Kuldeep Singh, Rajesh Verma, Ritika Chehal "Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption",International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012, pp 204-206.
3. Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma, "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012, pp 134-138.
4. "Extended Euclid algorithm and its application in RSA",Jianqin Zhou ; Jun Hu ; Ping Chen The 2nd International Conference on Information Science and Engineering,IEEE, 10.1109/ICISE.2010.5691644, 4-6 Dec. 2010.
5. R Gennaro. (2000), "RSA-Based Undeniable Signatures", Journal of Cryptology, Vol 13, No. 4, pp 397-416.
6. R Cramer, V Shoup. (2008), "Signature schemes based on the strong RSA assumption", ACMTransactions on Information and System Security, Vol 3, No 3, pp 161-185.

7. Gennaro. (2008), “Robust and Efficient Sharing of RSA Functions”, Journal of Cryptology, Vol 13, No 2, pp 273-300.
8. D Boneh, M Franklin. (2001), “Efficient generation of shared RSA keys”, Journal of the ACM, Vol 48, No. 4, pp 702-722.
9. Rivest, R.; A. Shamir; L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 (2): 120–126, doi: 10.1145/359340.359342, 1977.
10. B. Schneier, Applied cryptography, second edition, NY: John Wiley & Sons, Inc., 1996.
11. William Stallings, Cryptography and Network Security, Pearson Education, Fourth Edition.
12. Atul Kahate, Cryptography and Network Security, Tata McGraw-Hill Publishing Company Limited.
13. Nidhi Singhal, J.P.S.Raina “Comparative Analysis of AES and RC4 Algorithms for Better Utilization”,
14. International Journal of Computer Trends and Technology- July to Aug Issue 2011.
15. Priti V. Bhagat, Kaustubh S. Satpute and Vikas R. Palekar “Reverse Encryption Algorithm: A Technique for Encryption & Decryption” International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 2013,pp 90-95.
16. Gagandeep shahi, Charanjit singh “Cryptography and its two Implementation Approaches” International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 3, May 2013,PP 668-672.

AUTHOR’S PROFILE

D.Chandravathi, MCA,M.Tech,(Ph.D)
Sr.Assistant Professor,
GVP college for Degree and PG Courses(A),Visakhaptanm-45.

My research area includes Cryptography and cloud computing. I have published various research papers in Various International Journals

Prof. P. V. Lakshmi
Professor , IT Department ,
GITAM University, VSP.

Worked as Hod of It Department in GITAM University. Has guided many Ph.D students and has many publications in various International Journals. Organized many conferences and seminars in the Department in the capacity of Head of the Department.