ISSN:0975-9646

An Efficient RSA Based Technique for the Encryption and Decryption

Sharad Morolia, Manoj Dhawan

Department of Information Technology
Shri Vaishnav Institute of Technology & Science, Indore(M.P.), India
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal(M.P.), India

Abstract— **The high growth within the networking technology leads a typical culture for interchanging of the digital pictures terribly drastic. Thus, it's additional vulnerable of duplicating of digital image and re-distributed by hackers. So the knowledge needs to be protected whereas sending it, Sensitive data like credit cards, banking transactions and social insurance numbers have to be compelled to be protected. For this several cryptography and decoding techniques are a unit existing that area unit accustomed avoid the knowledge stealing. In the recent days of the web, the cryptography and decoding of information play a serious role in securing the information in on-line transmission focuses chiefly on its security across the web. Totally different cryptography and decoding techniques are a unit accustomed defends the confidential knowledge from unauthorized use. This paper proposes a faster version of the RSA algorithm.**

Keywords—**Cryptography,Data Services,RSA variant.**

I. INTRODUCTION

Cryptography is that the study of mathematical techniques associated with aspects of data security like confidentiality, knowledge, integrity, entity authentication, and knowledge origin authentication. Cryptography isn't the sole means that of providing info security, however instead of that it's a collection of techniques. If an identical secret is employed for coding and secret writing, we tend to tend to call the mechanism as Symmetric key cryptography. On the various hand, if 2 fully totally different keys square measure used in science mechanism, then we tend to tends to call mechanism as uneven Key or asymmetric key [1].

Network-based vs. host-based systems: in a network-based system or NIDS, the particular packets flowing through the network are analyzed. The NIDS can identify malicious packets that are designed to be overlooked by firewalls simplistic filtering rules. In a host-based system, the IDS observe activity on each individual computer or host.

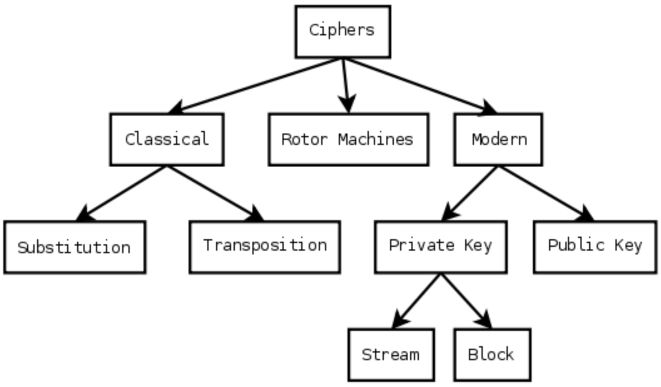

Figure 1.1: Cryptography Classification

The above figure 1 shows cryptography classification named bilaterally symmetric key and uneven or Asymmetric key cryptography.
The security services include [1]:

Data Confidentiality: The principal of confidentiality specifies solely the sender and meant recipient(s) ought to be ready to access the content of the message. Confidentiality has been defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that info is accessible solely to those licensed to possess access and is one at all the cornerstones of security ". Message of Confidentiality is one of the planning goals for several cryptosystems, created doable in the follow by the techniques of contemporary cryptography. It is designed to shield the knowledge from revelation attack.

Data Integrity: Data Integrity is intended for the protection of knowledge from unauthorized modification, insertion, Deletion associate degrees replaying by an informant. It will defend the complete message or the part of the message.

Authentication: In the affiliation orienting communication, it provides the authentication of the sender or receiver throughout the affiliation institution (peer entity authentication], it authenticates the source of data (also called data origin authentication).

Non repudiation: Non-repudiation service protects against repudiation by either the sender or the receiver of the Data. In this with the proof of origin, the receiver of the data can later prove the identity of the Sender, if denied. In non-repudiation with the real proof of delivery the sender of the data can later prove the data were delivered to the intended recipient.Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate. Although this concept can be also applied to any transmission including a television and radio, the most common application is in the verification and trust of signatures.

Access Control: Access management could be a system that permits associate degree authority to regulate access to areas and resources during a given physical facility or computer-based data system. Associate degree access system, with within the field of physical security. It provides security against unauthorized access against knowledge. The term access during this definition is extremely broad and may involve reading, writing, modifying, death penalty programs.

II. RELATED WORKS

Fault-based attacks are the attacks which are capable of recovering secret keys by. The fault based attacks introducing one or more faults in and then analyzes the output. It is a very powerful method to crack the key. The work done by Kun Ma et al in [2] contains a novel Concurrent Error Detection scheme to overcome the problem due to fault-based attack against RSA. This proposed method is based on the concept of the multiplicative homomorphic property. The time overhead of this technique is more.

Alexandra Boldyreva, Hideki Imai proposed another variant of RSA [3] it is known as RSA-OAEP. It is based on OAEP. The work done in [4] focuses on the problem of how to prevent the fast RSA signature and decryption computation with residue number system speedup from a hardware fault cryptanalysis in a highly reliable and efficient approach.

Giraud [5] proposed a new countermeasure scheme based on the concept of Montgomery Ladder Exponentiation. The proposed algorithm performs two modular multiplications for each bit of exponent. Whereas the square and multiply algorithm which performs on average 1.5 modular multiplications per bit of the exponent. Therefore the proposed method is faster.

The authors of [6] proposed an enhance algorithm for the RSA cryptosystem. This new proposed cryptosystem uses a third prime number in calculating the value of n.

In the setting of electronic commerce systems should run on a totally different package platforms like windows, Unix, and Linux. If the RSA is developed with C language, it'll talk about a drug that the system cannot run on all platforms, though the system developed with c language is straightforward to transplant. As an equivalent data type has totally different length on different platforms, this makes it tough to transplant. To make it simple to maintain the system, develop quickly and to unravel the matter of cross platforms. Author tries to develop this method with Java language. Java is an associate degree object orientating language, and the system developed with Java language will run all platforms[7].

The substance of cryptanalysis attacks on the RSA cryptosystem has been studied; all possible known attacks on the system are overwhelming. However, these attacks demonstrated pitfalls in the implementation and obvious misuse of the RSA system. Most of the attacks cannot be avoided. The RSA system remains secure and can be trusted if a proper implementation of the system is adequately taken into consideration. The attacks have been classified into three categories which include: Attacks on the RSA function, Attacks based on the extraction of details in the implementation, and the Factorization methods attacks. These attacks have demonstrated the dangers behind improper usage of the RSA system[8].

III. THEORETICAL BACKGROUND

In order to develop an efficient and accurate algorithm for security purpose many algorithm are present.RSA is one of them, well known public key cryptography. Soon after Merkle's knapsack algorithm came the first full-fledged public-key algorithm, one that works for encryption and digital signatures: RSA. Of all the public-key algorithms proposed over the years, RSA is one of the easiest to understand and implement. RSA algorithm also the most popular.

Named after the three inventors-Ron Rivest, Adi Shamir, and Leonard Adleman-it has since withstood years of extensive cryptanalysis. Although the cryptanalysis neither proved nor disproved RSA security, but also it does suggest a confidence level in the algorithm.

To generate the two keys two large prime numbers P & Q are chosen at random. For maximum security the value of the choose p and q should
n= p*q
Then randomly choose the encryption e, such that e and (p - l)*(q - 1) are relatively prime. Finally use the extended Euclidean algorithm to compute the decryption key d.
ed= 1 mod (p- l)*(q- 1)
$d = e^{-1} \bmod ((p - l)(q - 1))$
Encrypting:
$c=m^e \bmod n$
Decrypting
$m=c^d \bmod n$
This new proposed cryptosystem uses a third prime number in calculating the value of n. In this new apporach a new methodology to change the original modulus with the fake modulus. It is as follows [9]:

Reference RSA algorithm is as follows:

1. First choose random large prime integers p and q of roughly the same size but not too close to each other.
2. Calculate the product n = pq (ordinary integer multiplication)
3. Choose a random encryption exponent e It must not has any common factor with either p-1 or q-1 (ø(n)=(p-1)(q-1)).
4. Compute the "Pe" (possible values of e).
5. Selecting at random the encryption key e

   - where 1<e<ø(n), gcd(e,ø(n))=1

6. Solve following equation to find decryption key d

   - e.d=1 mod ø(n) and 0≤d≤n

7. Then select "Se"(are special values of "Pe")
8. Compute fake modulus Fn=n*Se
9. Publish their public encryption key: KU={e,Fn}
10. Keep secret private decryption key: KR={p,q,d,n}
11. For encrypt a message M the sender:
    - obtains public key of recipient KU={e,Fn}
    - computes: $C=M^e \bmod Fn$ where $0 \le M < Fn$

12. For decrypt the cipher text C the owner:
    - uses their private key KR={p,q,d,n}
    - computes: $M=C^d \bmod Fn$

IV. DOMAIN DESCRIPTION AND PROPOSED SYSTEM

The high growth in the networking technology leads a common culture for interchanging of the digital images very intensely. Hence it is more vulnerable of duplicating of digital image and re-distributed by hackers. Therefore the images has to be protected while transmit, sensitive information like debit cards, credit cards, online banking transactions and social network security numbers need to be protected. For this many encryption/decryption techniques are existing which are used to avoid the information theft. In recent days of Internet, the encryption/decryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption/decryption techniques are used to protect the confidential data from unauthorized use.
In recent development there are some problems in current RSA cryptosystems the following issues are considered for improvement.
1. The decryption it's slower speed: To decrypt any message time required more as compare to other algorithm. By applying new concept in decryption step as compare to pervious cryptosystem, decryption time is less as compare to previous algorithm.

2. Low decryption exponent attack if we know the decryption exponent and wiener's attack: If we know the value of decryption key **d** then it's factorized in polynomial time by applying randomized algorithm. Private decryption exponent value to be small in order to accelerate decryption or signing operations Selection of small value for the decryption exponent can result in breaking the entire system.
The Wiener's attack, named once decipherer Archangel J. Wiener. The wiener's attack uses the fraction technique to show the non-public key d once d is less. Its continued fraction method to exploit a mistake in the use of RSA cryptosystem.

A wiener's attack is based on two facts:

-If N=pq is a "good" RSA modulus (with p (approx) ≈ (approx) ≈√N), then N (approx) ≈φ(n).

-The wiener's set up is this: as a result of ed ≈ one mod m for variety of modulus m>=1 and positive number e and d, then d looks as a divisor at intervals the convergence of e/m.

Both attack are solve by choosing large vale of decryption key d.

3. Problem arises to common modulus attack: To avoid generating a special modulus N=pq for every user one would like to repair N once and for all. A similar N is employed by all users. A trusty central may offer user I with a novel combine ei,di from that user I type a public key(N,ei) and a secret key (N,di).Solution is:
In the decryption step we split the common modulus N into p and q by applying Fermat's theorem.

-Fermat's theorem such as: If p is prime and gcd (p,a) =1, then a^{p-1}=1 mod p

Proposed Algorithm:

1. First choose random large prime integers p and q of roughly the same size but not too close to each other.
2. Calculate the product n = pq (ordinary integer multiplication)
3. Choose a random encryption exponent e It must not has any common factor with either p-1 or q-1 (ø(n)=(p-1)(q-1)).
4. Selecting at random the encryption key e

- where 1<e<ø(n), gcd(e,ø(n))=1

5. Solve following equation to find decryption key d

- e.d=1 mod ø(n) and 0≤d≤n

6. For encrypt a message M the sender:

- obtains public key of recipient KU={e,Fn}
- computes: C=M^e mod Fn where 0≤M<Fn

7. In decryption step, we have made certain changes & it is as follows: we will split the n in to p and q by applying the Fermat's theorem. Then we will compute the plain text:

7.1 First compute:
X1 = c^{dp} mod p
X2 = c^{dq} mod q
Where dp = d mod (p-1) & dq = d mod (q-1)
7.2 Find vale of W:
W = (X2 – X1) * W1 mod q
Where W1 = p modinverse q
7.3 Then finally compute plain text M:
M= c^d mod n = X1 + W * p

V. Result Analysis

After completing implementation get the result according to given input.In this proposed cryptosystm give the input value of different hardware and software requriment and get the otput vale. Detail comparsion table such as:

System Requirement	Key Length in bits	Decryption Time in ms	
		Fake Cryptosystem	Proposed Cryptosystem
Processor:- I3 ,RAM:-1 GB	1024 bit	32ms	16ms
Processor:- I3 ,RAM:-1 GB	2048bit	172ms	47ms
Processor:- I5 ,RAM:-4 GB	1024 bit	28ms	15ms
Processor:- I5 ,RAM:-4 GB	2048bit	125ms	32ms

Table 5.1: Comparison of Decryption Time with different System Requirement and Key Length

In Table 5.1 compare decryption time of different hardware processor and different ram. Also apply two different key length are used.According to this get the result graphy such as:

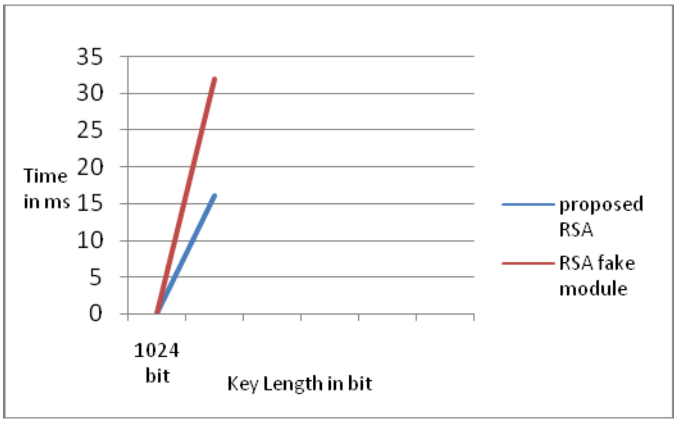

Figure 5.1 Decryption Time with Processor:- I3 ,RAM:-1 GB

In Figure 5.1 show the decryption time of proposed RSA algorithm is 16 ms and RSA fake module is 32 ms with key lenth 1024 bit.

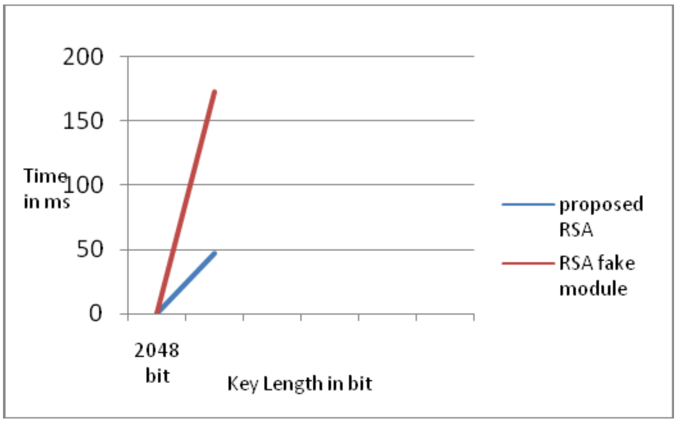

Figure 5.2 Decryption Time with Processor:- I3 ,RAM:-1 GB

In Figure 5.2 show the decryption time of proposed RSA algorithm is 47 ms and RSA fake module is 172 ms with key lenth 2048 bit.

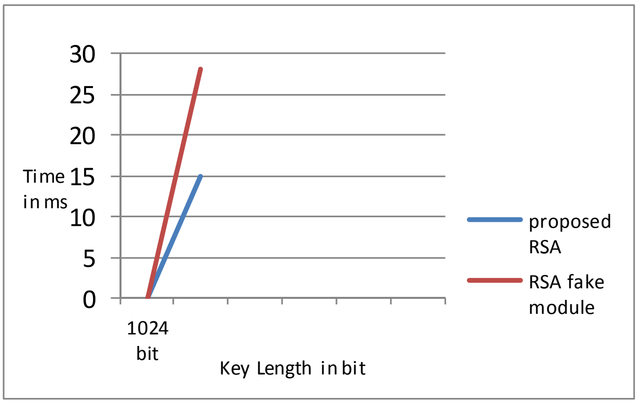

Figure 5.3 Decryption Time with Processor:- I5 ,RAM:-4 GB

In Figure 5.3 show the decryption time of proposed RSA algorithm is 15 ms and RSA fake module is 28 ms with key lenth 1024 bit.

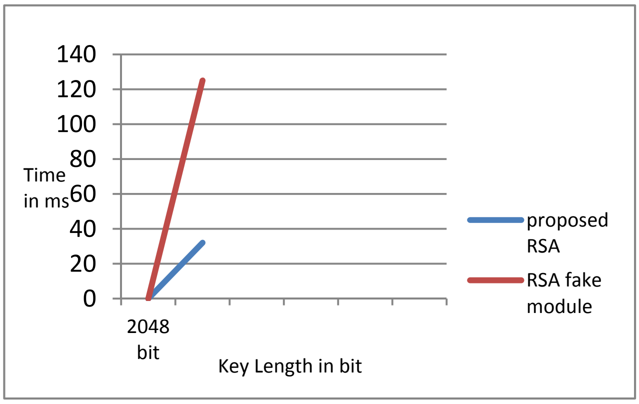

Figure 5.4 Decryption Time with Processor:- I5 ,RAM:-4 GB

In Figure 5.4 show the decryption time of proposed RSA algorithm is 32 ms and RSA fake module is 125 ms with key lenth 2048 bit.

VI. Conclusion and Future Work

In this paper, the introduction & the application of cryptography is given. The problems related to the RSA current version are also discussed. The public key cryptography & its utility in so many areas of the life are discussed. The paper also proposes an enhanced variant of the RSA algorithm. The experimental result has shown that the execution time of the proposed method is less than that of the existing variant. In near future some suggestion such as:

1. The present system works for small scale applications. In future it can be extended for the large scale applications.
2. The high speed encryption algorithm may be proposed.
3. The proposed algorithm can be extended to handle rich text, audio, video etc.
4. The performance of the cryptosystem used more than 2048 bit such as 3072 bit key length are used.
5. The proposed method can be upgraded to perform image encryption in the same efficient manner.

References

[1] Prof.Dr.Alaa Hussein Al-Hamami, Ibrahem Abdallah Aldariseh,"Enhanced Method for RSA Cryptosystem Algorithm" 2012International Conference on Advanced Computer Science Applications and Technologies, IEEE 2012.

[2] Kun Ma, Han Liang, and Kaijie Wu, Member, IEEE, Homomorphic Property-Based Concurrent Error Detection of RSA:A Countermeasure to Fault Attack", IEEE TRANSACTIONS ON COMPUTERS,VOL.61,NO.7, JULY 2012.

[3] Alexandra Boldyreva, Hideki Imai, Life Fellow, IEEE, and Kazukuni Kobara, "How to Strengthen the Security of RSA- OAEP", IEEE TRANSACTIONS ON INFORMATION THEORY,VOL.56, NO. 11, NOVEMBER 2010.

[4] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sang-Jae Moon," RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis"IEEE TRANSACTION ON COMPUTERS,VOL.52,NO.4, APRIL 2003.

[5] Giraud, "An RSA Implementation Resistant to Fault Attacks and to Simple Power Analysis," IEEE Trans. Computers, vol. 55, no. 9, pp. 1116-1120, Sept. 2006.

[6] Prof.Dr.Alaa Hussein Al-Hamami, Ibrahem Abdallah Aldariseh , "Enhanced Method for RSA Cryptosystem Algorithm" 2012 International Conference on Advanced Computer Science.

[7] Guicheng Shen, Bingwu Liu , Xuefeng Zheng, "Research on Fast Implementation of RSA with Java" International Symposium on Web Information Systems and Applications, a, May 22-24, 2009, pp. 186-189.

[8] Adamu Abubakar, Shehu Jabaka, Bello Idrith Tijjani, Akram Zeki, Haruna Chiroma, Mohammed Joda Usman, Shakirat Raji, Murni Mahmud" Cryptanalytic Attacks on Rivest, Shamir, and Adleman (RSA) Cryptosystem: Issues and Challenges", Journal of Theoretical and Applied Information Technology, Vol. 61, No.1, pp.37-43 March 2014.

[9] "Enhancing Security Features in RSA Cryptosystem", 2012 IEEE Symposium on Computers & Informatics, IEEE 2012.

[10] Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method",2012 Second International Conference on Applications and Technologies, IEEE 2012.