RESEARCH ARTICLE OPEN ACCESS

To Design and Implement a Novel Method of Encryption Using Modified RSA Algorithm and Chinese Remainder Theorem

Ms. Bhumi J. Patel*, Prof. Nitin J. Janwe**
*(Department of Computer Science, Gondwana University, Gadchiroli
Email: bhumi19patel@yahoo.com)
** (Department of Computer Science, Gondwana University, Gadchiroli
Email: nitinj_janwe@yahoo.com)

ABSTRACT
RSA cryptosystem is the most attractive and popular security technique for many applications, such as electronic commerce and secure internet access. It has to perform modular exponentiation with large exponent and modulus for security consideration. The RSA cryptosystem takes great computational cost. In many RSA applications, user uses a small public key to speed up the encryption operation. However, the decryption operation has to take more computational cost to perform modular exponentiation by this case. This paper proposes an efficient decryption method not only based on Chinese Remainder Theorem (CRT) but also the strong prime of RSA criterion. Chinese Remainder Theorem is used for generating random number. The CRT-RSA algorithm is used for generating cipher text message from original message of blocks of data.

Keywords – Cryptography, Encryption, Decryption, RSA Algorithm, Chinese Remainder Theorem.

I. INTRODUCTION

Cryptography is defined as the study of techniques for ensuring the secrecy and authenticity of information. It is the science and study of secret writing which concerns the ways of communication and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message. With regards to confidentiality, cryptography is used to encrypt data residing on storage devices or travelling through communication channels to ensure that any illegal access is not successful. Also, cryptography is used to secure the process of authenticating different parties attempting any function on the system. The most classic and obvious credential are passwords. Passwords are encrypted to protect against illegal usage. Authorization is a layer built on top of authentication in the sense that the party is authenticated by presenting the credentials required (passwords, smart cards etc.). After the credentials are accepted the authorization process is started to ensure that the requesting party has the permissions to perform the functions needed.

Data integrity and Non-Repudiation are achieved by means of digital signature, a method that includes performing cryptography among other things. As the rapid progressing of modern information technology, security is an important technique of many applications including virtual private networks, electronic commerce and secure internet access. RSA algorithm is the most popular and well-defined security primary technique. RSA is widely used for digital signature and digital envelope, which provide privacy and authentication. However, the RSA operation has to take great computation cost for security consideration. In order to include RSA cryptosystem efficiently in many protocols, it is desired to devise faster encryption and decryption operations.

Cryptography can essentially be classified into two types, the symmetric and asymmetric type. With a secret or symmetric key algorithm, the key is a shared secret between two communicating parties. Encryption and decryption both use the same key. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are examples of symmetric key algorithms. With a public key (PKA) or asymmetric key algorithm, a pair of keys is used. One of the keys, the private key, is kept secret and not shared with anyone. The other key, the public key, is not secret and can be shared with anyone. When data is encrypted by one of the keys, it can only be decrypted and recovered by using the other key. The two keys are mathematically related, but it is virtually impossible to derive the private key from the public key. The RSA algorithm is an example of a public key algorithm.

In RSA cryptosystem, basically, implementation involved three different stages namely key generation, encryption and decryption processes. These stages depend very much on each other in order to optimize efficiency as well as computation costs. In the encryption process the key *e* is made public whereas in decryption process the key *d* is a private key. This key is very important as only the key holder can decrypt the ciphertexts to the original plaintexts. To obtain a secure and intractable key *d* a few algorithms have been developed. There are three well known methods for the key *d* generation, where these methods are used to obtain the key *d*. They are Euclid's extended GCD (greatest common divisor) algorithm, Derome's algorithm etc. All these methods had used modular arithmetic operations and infact the whole process of the RSA cryptosystem uses modular arithmetic and the correctness of the RSA algorithm has been proven mathematically.In many RSA cryptosystems, they usually select a small value for the public key *e*. This kind of choice can only speed up the encryption operation but do not forget that by this way, the corresponding decryption operation costs more computational time because of the larger decryption exponent *d*. The alternative way that can be taken to overcome this problem is to implement the decryption operation based on the Chinese Remainder theorem (CRT). The security of RSA is based on the difficulty of factoring problem. So, the prime factors of modulus of RSA algorithm must be strong primes. The large modular exponentiation result can be generated from small exponents and moduli. The proposed method enhances the performance of RSA algorithm.

II. EXISTING TECHNIQUES

2.1 RSA Algorithm:

The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L. Adleman, is the most widely used public key Cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization. The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n-1 for some n. A typical size for n is 1024 bits.That is, n is less than 2^{1024}. The scheme makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to log2 (n); in practice, the block size is i bits, where 2i < n <2i+1. Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

$C = M^e$ mod n

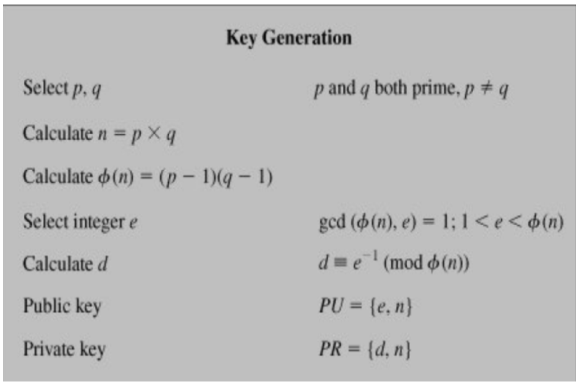
$M = C^d$ mod n = $(M^e)^d$ mod n = M^{ed} mod n

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PU = {d, n}. For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:
1. It is possible to find values of e, d, n such that M^{ed} mod n = M for all M < n.
2. It is relatively easy to calculate mod M^e mod n and C^d for all values of M < n.
3. It is infeasible to determine d given e and n.

We need to find a relationship of the form M^{ed} mod n = M. The preceding relationship holds if e and d are multiplicative inverses modulo φ(n), where φ(n) is the Euler totient function. For p, q prime, φ (pq) = (p-1) (q-1) The relationship between e and d can be expressed as:
ed mod φ(n) =1.
This is equivalent to saying:
ed ≡ 1 mod φ(n) and d ≡ e^{-1}mod φ(n)

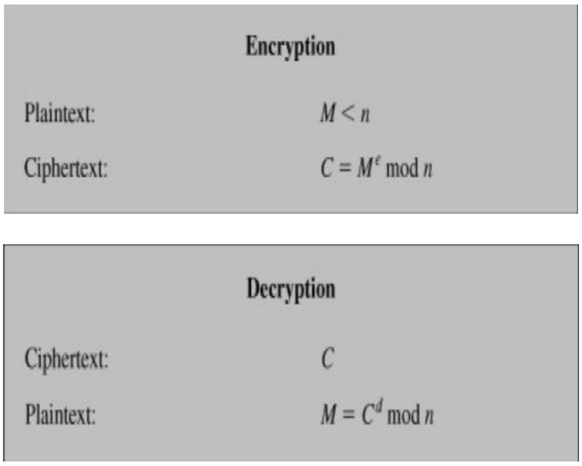
That is, e and d are multiplicative inverses mod φ (n).According to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to φ(n). Equivalently, gcd (φ (n), d) = 1.

It can be described briefly as follows:
1. Choose two large strong primes, *p* and *q*. Let *n* =*p.q*.
2. Compute Euler value of n: φ (*n*) = (*p* - 1)(*q* - 1).
3. Find a random number *e* satisfying 1 < *e* < φ (*n*) and gcd (*e*, φ (*n*)) = 1.
4. Compute a number *d* such that $d = e^{-1}$ mod φ (*n*).
5. Encryption: Given a message *M* satisfying *M* < *n*, then the cipher text $c = M^e$mod *n*.
6. Decryption: $M = C^d$ mod *n*.



Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$



Encryption

Plaintext: $M < n$

Ciphertext: $C = M^e \bmod n$

Decryption

Ciphertext: C

Plaintext: $M = C^d \bmod n$

Fig.1 RSA Algorithm

2.2 Chinese Remainder theorem:

Chinese Remainder Theorem, CRT, is one of the main theorems of mathematics. This can be used in the field of cryptography. It is a perfect combination of beauty and utility, CRT continues to present itself in new contexts and open vistas for new types of applications. So far, its usefulness has been obvious within the realm of “three C's”. *Computing* was its original field of application, and continues to be important as regards various aspects of algorithmic and modular computations. Theory of codes and cryptography are two more recent fields of applications.

The conventional Chinese remainder theorem (CRT) is to determine a single integer from its remainders from a set of modulos. It has tremendous applications in various areas, such as cryptography and digital signal processing. The Chinese Remainder Theorem (CRT) allows for an efficient implementation of the RSA algorithm. As we know, the CRT is an algorithm with so many applications in mathmatics, computing is the main area of its application and moreover, recently it is being used in cryptography also. But in the field of cryptosystem, the algorithm is used for functionality for modular computation. Random number generators have application in gambling, statistical sampling, computer simulation, cryptography, and other areas where a random number is useful in producing an unpredictable result. The random numbers also is useful for the prevention of reply attack also for counter measures.

CRT has various generalizations. A different generalization of CRT has been recently proposed in, where (instead of a single integer in CRT) multiple integers need to be determined from (not a sequence of remainders but) a sequence of sets, residue sets, of remainders. A residue set consists of the remainders of multiple integers modulo a modulus integer, and the residue set is not ordered, i.e., the correspondence between the elements in the residue set and the multiple integers is not specified. The generalized CRT was motivated from the determination of multiple frequencies in a super positioned signal of multiple sinusoids from its multiple under sampled waveforms. This has applications in a sensor network, where multiple sensors have low power and low transmission rates, and their sampling rates may be low and much lower than the Nyquist rate of a signal of interest in the field. The generalized CRT has been used in synthetic aperture radar (SAR) imaging of moving targets and polynomial phase signal detection. It has been found that the error rates of multiple frequencies are significantly reduced with the proposed algorithm considering residue errors compared to the one without considering residue set errors. This algorithm finds application in a sensor network with low sampling rates. Chinese Remainder Theorem has been used for hundreds of years and has been applied to many domains such as integers and polynomials.

The size of the decryption exponent, *d* and the modulus, *n* is very important because the complexity of the RSA decryption depends directly on it. The decryption exponent specifies the numbers of modular multiplication necessary to perform the exponentiation. The modulus, *n* play a role in determined the size of the intermediate results. A way to reduce the size of both *d* and *n* is by using the Chinese Remainder theorem.

Theorem 1: Let $m_1, m_2 \ldots\ldots\ldots, m_n$ be a pairwise relatively prime, i.e gcd(m_i , m_j) =1 for all *i* and *j* less than or equal to *n* where $i \neq j$. Then, the system of congruences:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

•

•

$$x \equiv a_n \pmod{m_n}$$

has a solution which is unique modulo the integer $m_1, m_2 \ldots m_n$. Further, if

$$M_j = \frac{\prod_{i=1}^{n} m_i}{m_j}$$

and z_j is a solution of $M_j z_j \equiv a_j \pmod{m_j}$ for each j, then solution is given by,

$$x = \sum_{j=1}^{n} M_j z_j$$

III PROPOSED TECHNIQUE

3.1 RSA using Chinese Remainder Theorem:

The Chinese Remainder Theorem (CRT) allows for an efficient implementation of the RSA algorithm. Given input, m, raise it to the e-th (or d-th) power modulo p and modulo q. The intermediate results are then combined through multiplication and addition with some predefined constants to compute the final result (the modular exponentiation to n). This approach is often used for implementing RSA in embedded systems. It requires four times less execution time and smaller amount of memory for intermediate results, since modular exponentiation is performed on half the bit size of n.

The complexity of the RSA decryption M = C^d mod n depends directly on the size of d and n. The decryption exponent d specifies the numbers of modular multiplications necessary to perform the exponentiation, and the modulus n determines the size of the intermediate results. A way of reducing the size of both d and n is to take advantage of properties stated by the Chinese Remainder Theorem (CRT).

The decryption operation based on the Chinese Remainder theorem is implemented as follows:
Since the recipient knows the secret primes *p* and *q*, he can compute the following modular components:
$d_p \equiv d \bmod (p-1)$ and $d_q \equiv d \bmod (q-1)$
$C_p \equiv C \bmod p$ and $C_q \equiv C \bmod q$
$M_p \equiv C_p^{\,dp} \bmod p$ and $M_q \equiv C_q^{\,dq} \bmod q$
Combining M_p and M_q we get original plaintext message.

There are many ways that we can get the original plaintext, *M* using the Chinese Remainder theorem. From the proof of Chinese Remainder theorem, we know that the unique solution *x* of the congruences can be written as:

$$x = \left(\sum_{i=1}^{k} x_i r_i s_i \right) \bmod n$$

Where r_i = n / n_i and si = $r_i^{-1(}$mod ni) for i = 1, 2…., k.

IV. PERFORMANCE

The propose method is faster as compared to simple RSA algorithm. The RSA algorithm with Chinese Remainder Theorem requires less number of iterations as compared to simple RSA algorithm. It reduces computational cost. The performance of RSA is enhanced using Chinese Remainder Theorem.

V. CONCLUSION

The above research is to be under taken in order to develop better and faster algorithms for implementation of RSA system in Cryptography. Chinese reminder theorem, provide benefits in computing, mathematics and also in the field of cryptography, where the algorithm provides relief in case of modular computation and also in case of generating the random numbers. In this paper, we propose an efficient method to implement RSA decryption algorithm. This efficient decryption method can enhance the performance of the RSA algorithm. The proposed method reduces the computational cost. Thus algorithm using CRT and strong prime has speed up the decryption process as well as cost saving.

VI. ACKNOWLEDGEMENT

I would like to articulate my deep gratitude to my guide Prof. Nitin J. Janwe who has always been my motivation for helping and carrying out the research. An assemblage of this nature could never have been attempted without reference to and inspiration from the works of others whose details are mentioned in reference section. I acknowledge my indebtedness to all of them. I would like to thank my friend Prof. Santosh Hedau who has patiently extended all sorts of help for accomplishing this undertaking.

REFERENCES

[1] V.Senthil Balaji and R.Rengaraj alias Muralidharan, "Secure Transmission of Data Using CRT-RSA"*Journal of Global Research in Computer Science TamilNadu India Volume 1, No. 1, August 2010.*

[2] Hailiza Kamarul Haili and Norfadhilah Basir, "RSA Decryption Techniques and the Underlying Mathematical Concepts" *International Journal of Cryptology Research Malaysia 1(2): 165-177 (2009).*

[3] Marc Joye Thomson R&D, "Protecting RSA Against Fault Attacks: The Embedding Method" *IEEE Computer Society Published in L. Breveglieri etal Eds, Fault Diagnosis and Tolerance in Cryptography (FDTC 2009), France pp. 41–45, 2009. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," IEEE Trans. Antennas Propagat., to be published.*

[4] Kalyani, P. and 2C. Chellappan , "Enhanced RSACRT for Energy Efficient Authentication to Wireless Sensor Networks Security" *American Journal of Applied Sciences Chennai,India 9 (10): 1660-1667, 2012 ,ISSN 1546-9239.*

[5] Ditipriya Sinha , Uma Bhattacharya ,Rituparna Chaki ," A CRT based Encryption Methodology for Secure Communication in MANET*"International Journal of Computer Applications (0975 – 8887) Volume 39– No.16, February 2012.*

[6] Saurabh Singh , Gaurav Agarwal, "Use of Chinese Remainder Theorem to generate random numbers for cryptography"*International Journal*

of Applied Engineering and Research Lucknow and Mysore, India of Volume 1, No1, 2010.

[7] Ren-Junn Hwang, Feng-Fu Su, Yi-Shiung Yeh, Chia-Yao Chen," An Efficient Decryption Method for RSA Cryptosystem" *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05) Taiwan 1550-445X/05 $20.00 © 2005 IEEE.*

[8] Xiaowei Li, Hong Liang, and Xiang-Gen Xia, Fellow, "A Robust Chinese Remainder Theorem With Its Applications in Frequency EstimationFrom Undersampled Waveforms" *IEEE Transactions on signal processing, Vol. 57, No. 11, November 2009.*

[9] Sonali S. Mhatre, "Enhanced Chinese Remainder Theorem based Broadcast Authentication in Wireless Networks"*International Journal of Computer Applications (0975 – 8887) Volume 50 – No.15, July 2012.*