Modified RSA Encryption Algorithm using Four Keys

Nivetha A
Dept of Information Technology
Anand Institute of Higher Technology,
Chennai, Tamil nadu

Preethy Mary S
Dept of Information Technology
Anand Institute of Higher Technology,
Chennai, Tamil nadu

Santosh kumar J
Dept of Information Technology
Anand Institute of Higher Technology,
Chennai, Tamil nadu

Abstract: **The proposed paper enhances the RSA algorithm through the use of four prime number in combination of public and private key. Hence by using this, factoring complexity of variable is increased, this makes the analysis process with the development of equipment and tools become much easier. The use of four prime number will give the ability to the modified encryption technique to provide more security in accessing, and also increased speed. This was developed from the original RSA algorithm the additional two prime numbers are going to provide secrecy. Many experiments have been done under this proving Modified RSA encryption Algorithm using four keys to be faster and efficient than the original encryption and decryption process. This thesis presents the implementation of successive subtraction operation instead of division operation. By applying this approach we can achieve the high computational speed and reduce the complexity of the mathematical steps.**

Keyword: Complexity, Prime number, Public key, four keys, algorithm.

1. INTRODUCTION

Encryption is one of the principal means to grant the security of sensitive Information also functioned with digital signature, authentication, secret sub-keeping, system security and etc. Therefore, the purpose of adopting encryption techniques is to ensure the information's confidentiality, integrity and certainty, prevent information from tampering, forgery and counterfeiting.

At present, the best known and most widely used public key system is RSA, which was first proposed in paper "A method for obtaining digital signatures and public-key cryptosystems" by RL Rivest in 1978. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. Its security is based on the difficulty of the large number prime factorization, which is a well-known mathematical problem that has no effective solution.

2. LITERATURE REVIEW

R.L. Rivest, A. Shamir, and L. Adleman[1] proposed a method for implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers. If the security of our method proves to be adequate, it permits secure communications to be established without the use of couriers to carry keys, and it also permits one to "sign" digitized documents. The reader is urged to and a way to "break" the system. Once the method has withstood all attacks for a sufficient length of time it may be used with a reasonable amount of condense.

The encryption function is the only candidate for a "trap-door one-way permutation" known to the authors. The large volume of personal and sensitive information currently held in computerized data banks and transmitted over telephone lines makes encryption increasingly important. In recognition of the fact that efficient, high-quality encryption techniques are very much needed but are in short supply, the National Bureau of Standards has recently adopted a "Data Encryption Standard", developed at IBM. The new standard does not have property (c), needed to implement a public-key cryptosystem.

Xin Zhou and Xiaofei Tang[2] proposed an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm. In addition, the encrypt procedure and code implementation is provided in details. Encryption is one of the principal means to guarantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security and etc. The encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. Encryption and decryption algorithm's security depends on the internal structure of the rigor of mathematics, it also depends on the key confidentiality.

Problem for RSA encryption on the file, it indicates the RSA mathematical algorithms in the computer industry's importance and its shortcomings. It discusses the questions of how to apply to the personal life of RSA information security issues. And also contains the use of RSA and the basic principles of data encryption and decryption. In the end, it proposed a new program to improve RSA algorithm based on RSA cryptography and the extensive application. In summary, this issue of the RSA encryption and decryption keys, RSA algorithm, the new use of the RSA and other issues to study and make some new programs, future work should be in the new RSA cryptographic algorithms and a wide range of applications continue to research.

3. PROBLEM DEFINITION

MREA is secure as compared to RSA as it based on the factoring problem as well as decisional composite residuosity assumptions which are the intractability

hypothesis. This scheme also presents comparisons between RSA and MRSA cryptosystems in terms of security and performance. This algorithm uses a mod operator for computational purposes. The objective of this thesis presents the implementation of successive subtraction operation instead of using division operator. For applying this approach we have to achieve the high computational speed and reduce the complexity of the mathematical steps.

3.1 Modulo Operation:

In computing, modulo operation finds the remainder of division of one number by another. .

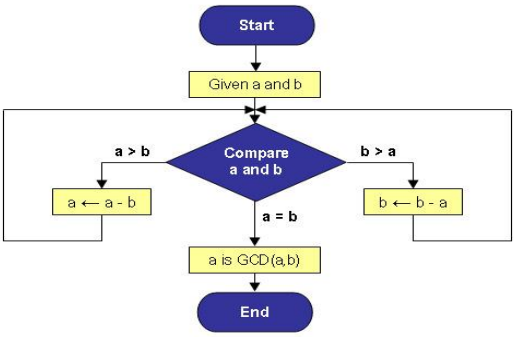

Figure 4: Euclidean algorithm diagram

3.2 Euclidean Algorithm

Euclid's method for finding the greatest common divisor (GCD) of two starting lengths BA and DC, both defined to be multiples of a common "unit" length. In mathematics, the **Euclidean algorithm**, or **Euclid's algorithm**, is a method for computing the greatest common divisor

By reversing the steps in the Euclidean algorithm, the GCD can be expressed as a sum of the two original numbers each multiplied by a positive or negative integer, e.g., the GCD of 252 and 105 is 21, and 21 = [5 × 105] + [(−2) × 252]. This important property is known as Bezout's identity.

The simplest form of Euclid's algorithm starts with a pair of positive integers and forms a new pair that consists of the smaller number and the difference between the larger and smaller numbers. The process repeats until the numbers are equal; then that value is the greatest common divisor of the original pair. The division form of Euclid's algorithm starts with a pair of positive integers and forms a new pair that consists of the smaller number and the remainder obtained by dividing the larger number by the smaller number. The process repeats until one number is zero. The other number then is the greatest common divisor of the original pair.

4. METHODOLOGY

4.1 RSA System

RSA is a commonly adopted public key cryptography algorithm. The first, and still most commonly used asymmetric algorithm RSA is named for the three mathematicians who developed it, Rivest, Shamir, and Adelman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data.RSA uses a variable size encryption block and a variable size key.

4.2 Attacks against plain RSA

There are a number of attacks against plain RSA as described below. When encrypting with low encryption exponents (e.g., $e = 3$) and small values of the m, (i.e., $m < n^{1/e}$) the result of m^e is strictly less than the modulus n. In this case, cipher texts can be easily decrypted by taking the eth root of the cipher text over the integers. If the same clear text message is sent to e or more recipients in an encrypted way, and the receivers share the same exponent e, but different p, q, and therefore n, then it is easy to decrypt the original clear text message via the Chinese remainder theorem. Johan Has tad noticed that this attack is possible even if the clear texts are not equal, but the attacker knows a linear relation between them. This attack was later improved by Don Coppersmith. RSA has the property that the product of two cipher texts is equal to the encryption of the product of the respective plaintexts. That is $m_1^e m_2^e \equiv (m_1 m_2)^e \pmod{n}$. Because of this multiplicative property a chosen-cipher text attack is possible

4.3 Key generation

RSA involves a **public key** and a **private key.** The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q. For security purposes, the integer's p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute n = pq.

   n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

3. Compute $\varphi(n) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$, where φ is Euler's totient function.

4. Choose an integer e such that $1 < e < \varphi(n)$ and gcd(e,φ(n)) = 1; i.e. e and φ(n) are co-prime is released as the public key exponent. e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16}+1=65537$. However, much smaller values of e(such as 3) have been shown to be less secure in some settings.
5. Determine d as $d^{-1} \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)).This

is more clearly stated as solve for d given d·e ≡ 1 (mod φ(n)).This is often computed using the extended Euclidean algorithm.d is kept as the private key exponent.

By construction, d·e ≡ 1 (mod φ(n)). The **public key** consists of the modulus n and the public (or encryption) exponent e. The **private key** consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

An alternative, used by PKCS#1, is to choose d matching de ≡ 1 (mod λ) with

λ = LCM(p − 1, q − 1), where LCM is the least common multiple. Using λ instead of φ(n) allows more choices for d. λ can also be defined using the Carmichael function, λ(n).

The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

6. THE EXISTING RSA ALGORITHM

Key generation

1. Select FOUR PRIME NUMBERS P,Q,R,S
2. Calculate n=p*q*r*s.
3. Calculate f(n)=(p-1)*(q-1) *(r-1)*(s-1)
4. Select integers e; gcd(f(n),e)=1;1<e<f(n).
5. Calculate d; d=e-1 mod f(n)
6. Public key KU ={e,n}
7. Private Key KR ={d,N}.

Encryption:
Plain text: M<n
Cipher text : **C= M^{e}mod n.**
Decryption:
Cipher text to Plain text**: M=C^d mod n**.
Here encryption and decryption using division operation instead of using that use of successive subtraction which is reduce the mathematical steps. And also to achieve the high computational speed.

5.1 Proposed Algorithm

Step1: Start the process

Step 2: initialize i =0

Step 3: Calculate power of e^i

Step 4: If e^i value is less than phi value then go to step5

Step 5: if e^i value is greater than phi value then goto step 6

Step 6: e^i value store in b go to step 7

Step 7: exit in for loop go to step 5

Step 8: subtract phi value in b and store to phi

Step 9: if phi value is negative the last value of phi vale is mod value

Step 10: Stop the process.

5.2 Previous work:

Let us take example of 125 mod 2. For that we take mod operator performing, the following steps,125-2=123-2=121-2=119……3-2=1. So that, we want compute more (21 steps) steps want to evaluate this expression. Finally got the output as 1.

5.3 Proposed work:

Now introduce the concept, of power subtraction. That is 125-64=61-32=29-16=13-8=5-4=1. In this concept, we use only the 4 steps of evaluation. 125 mod 2, the powers of 2 can be used. That is, nearest value of power is 64=2^6, so use of successful powers of sub tractor is used to get the answer as 1.So that speed can be increased whereas the previous system. And also reduced the complexity of the computation.

6. IMPLEMENTATION

This paper presents the purpose about modification in modified RSA encryption and decryption. Here artificially small parameters are used to clarify the concept. However, the method is applicable in general to all suitably selected parameters. Here four prime numbers will be used to get the public key and private key.
Select four prime numbers.
1. Calculate n=p*q*r*s
   P=2, q=3, r=5,s=17
   n=2*3*5*17
2. Calculate f(n)=(p-1) (q-1) (r-1) (s-1)
   f(510) = (2-1) (3-1) (5-1)(17-1) =128
   f (n)=128
3. Select any number 1<e<128
   F (n) must not be divisible by e
   Let e=3
4. Select d, multiplicative of e(mod f(n))
   d= 43
   The Public Key is (n = 510, e = 3)
   Private Key is (n = 510, d = 43)
   Given message m= 11.
5. Encryption:
   C= 11^3mod 510 = 311; C = 311
6. Decryption:
   M = 311^{43} mod 510 = 11

B got the original message (11) which is sent by A. In proposed algorithm use of mod function want to perform a division operation, instead of using that use of successive subtraction which is reduce the mathematical steps. The above encryption and decryption as follows:

Encryption: 11^3 mod 510 = 1331 mod 510=821-510=311

Decryption: Same as Encryption

7. RESULT AND DISCUSSION

The MREA cryptosystem is based on additive homomorphism properties and RSA cryptosystem, additive homomorphism scheme required four prime numbers, it will be more difficult and take long time to factor modulus, If RSA which is based on single modulus, and additive homomorphism based on dual modulus, then time required for MREA algorithm is higher than the proposed algorithm.

COMPARISON BETWEEN THE ORIGINAL ALGORITHM AND MODULUS ALGORITHM

In this thesis calculate the encryption and decryption time for 4 prime number, In modified RSA algorithm, the time taken for encryption and decryption is high using division of arithmetic operation in the following table1 and table2.

Calculate Total (Encryption and Decryption) Time for MREA MODULUS OPERATION

TABLE1:

File Size	Prime1 (P)	Prime2 (Q)	Prime3 (R)	Prime4 (S)	Time encryption msec	Time Decryption msec	Total Encryption and Decryption
16	47657	40879	39181	45413	1436	2294	3730
16	55249	38629	55261	44131	1248	2044	3292
16	45893	58363	53269	46091	1498	2215	3713
32	3749111581	3053962657	3804003727	3197015347	1904	2793	4697
32	3905572499	2468271571	3999631414	3217460247	2668	4025	6693
64	1494509931 656073351	9909002931 462119371	1339558228 907397613	1551208215 506190451	2231	3213	5444
128	2786093220 3889619493 2211627811 77477987	2445329867 8624812879 2867472053 56094559	2891299140 6194808368 4941886452 477565887	2241403107 1405811244 1430785544 0288593	1903	4945	6032
256	1013981169 3800364834 9023273831 0914569160 4048855461 3979577975 4463501229 91053857	7121346144 3347081131 4890910110 7436530482 6205447917 2988123177 5525294320 3645981080	9186414491 2503552316 0725480046 1237698220 3805447754 8610540185 6935237577 4035049	1085874292 0113460261 6212745402 4060950909 6647733100 8311461608 3652555668 4404331899	2418	5163	7581

Calculate Total time for RSA:

TABLE **2:**

File Size	Prime1 (P)	Prime2 (Q)	Time for encryption msec	Time for Decryption msec	Total Encryption and Decryption msec
16	62581	61871	1326	2184	3510
16	43451	57503	1466	3042	4508
16	41017	48311	1233	2106	3339
32	2303429669	2882496997	1320	2200	3520
32	2228591711	2776700159	1622	2542	4164
64	92783726807 48036401	151578035750 90599403	1888	2700	4618
128	27179167088 73709729139 12533344645 89759	271514666889 556658733897 596048196044 701	1939	2869	4808
256	58489458247 01209440574 91573670152 81011147965 25504418230 57975304032 2465049	581184692835 844979053839 688827399754 799547995631 780491692521 197163712154 2899211207	2154	3043	5197

Comparison of MREA and RSA algorithm:

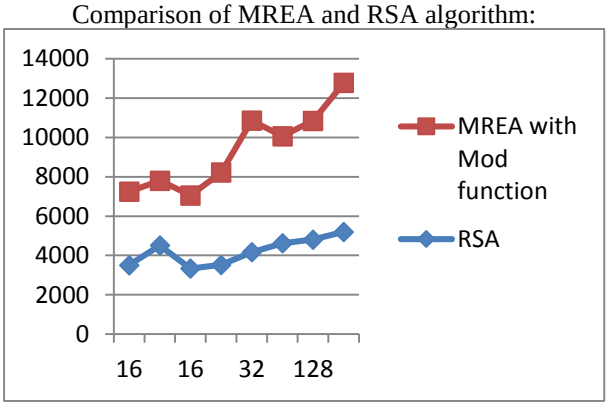

Figure 5: Analysis of RSA and MREA

The above table and figure shows that the process of encryption and decryption in the proposed method are faster than the original method by the apparent results. In modulus function instead of using that division operation, use of successive subtraction which is reduce the mathematical steps and also to achieve the high computational speed. And also this proposed algorithm is more secure for mathematical attacks

8. CONCLUSION

Encryption algorithm plays an important role in communication Security. The proposed cryptography procedure is the enhanced proposal of our previous research work where the concept of speed enhancement of modulus functions. Using this idea to reduce the mathematical steps to solve that expression. So we conclude that easily computation can be performed and complexity was reduced. Complexity time also decreased

by using successive subtraction technique. So that the speed can be increased.

In this thesis an algorithm is proposed for Modified RSA modulus factorization. The new algorithm aims to obtain the prime factors of modulus in Modified RSA algorithm. This algorithm is relatively simple and scalable. This method can be used for factorization of subtraction, very helpful to generate results in high speed.

REFERENCES:

[1] 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
[2] Bell, E. T. "The Prince of Amateurs: Fermat.", New York: Simon and Schuster, pp. 56-72, 1986.
[3] Gabriel Vasile Iana1, Petre Anghelescu1, Gheorghe Serban "RSA encryption algorithm implemented on FPGA" 1University of Pitesti, Department of Electronics and Computers, Romania, Arges, Pitesti, Str. Targul din Vale, No. 1, Code: 110040.
[4] Na Qi Jing Pan Qun Ding "The implementation of FPGA-based RSA public-key algorithm and its application in mobile-phone SMS encryption system" HeiLongjiang University Electronic Engineering Key Laboratory of Universities in Heilongjiang Province Harbin, China.
[5] Sonal Sharma, Prashant Sharma and Ravi Shankar Dhakar "RSA Algorithm Using Modified Subset Sum Cryptosystem" International Conference on Computer & Communication Technology (ICCCT)-2011
[3] João Carlos Leandro da Silva, "Factoring Semi primes and Possible Implications", IEEE in Israel, 26th Convention, pp. 182-183, Nov. 2010.
[4] Sattar J Aboud, "An efficient method for attack RSA scheme", IEEE 2009.
[5] L. Scripcariu, M.D. Frunza, "A New Character Encryption Algorithm", Proceedings of the Intern. Conference on Microelectronics and Computer Science, Chisinau, (Republica Moldova), ICMCS 2005, pp. 83 - 86, Sept., 2005.
[6] B. Schneier, Applied cryptography, second edition, NY: John Wiley &Sons, Inc., 1996.
[7] J. Pollard, "Monte Carlo methods for index computation (mod p)", Math. Comp., Vol. 32, pp.918-924, 1978.
[8] R. P. Brent, "An improved Monte Carlo factorization algorithm", BIT 20 (1980), 176-184. MR 82a:10007, Zbl 439.65001. rpb051.
[9] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," vol. 21 (2), pp.120-126, 1978.