An Improved RSA Cryptographic System

Nikita Somani
Student
Department of Computer Science Engineering
MITM Rau Road
Indore,(MP)452001, India

Dharmendra Mangal
Associate Professor
Department of Computer Science Engineering
MITM Rau Road
Indore,(MP)452001, India

ABSTRACT
Paper introduced RSA cryptosystem and its security aspects. RSA is a public key algorithm that applied widely in the field of information security in the Internet-Banking and E-Commerce applications. The proposed scheme for RSA cryptosystem contains three prime numbers and overcome several attack possible on RSA. The proposed scheme has speed improvement on RSA decryption side by using the Chinese Reminder Theorem (CRT) and the scheme is semantically secure also.

General Terms
Cryptography, Prime Numbers, RSA Cryptosystem, Security analysis

1. INTRODUCTION
In Today's life the computer and the communication technologies are very important part of strong economy. That's why we need a suitable security standards systems [1] and technologies to meet that security needs. Now-a-days communication is blooming fast as well as reliable and it becomes part of daily life. The main concern related to reliable transmission of data is security. The secure transmission of data in which like online banking, Credit Card, ATM [2] etc needs strong security, because most of the transaction is held through IP cloud. In IP cloud the whole data is accessible and because of these there is chance that the data becomes hacked. For securing the knowledge, cryptography is used. Cryptography [3] is a technique to hide the data over communication channel or we can say it is a science of keeping secrets secret. For this reason, the term "Encryption" was brought out, and it is the main factor that should be available in protection system and take for a real process to manipulate and generate the security system. For securing information different kinds of cryptographic methods are used like message authentication code, symmetric and asymmetric cryptography, digital signature, hash function etc [4]. Public key cryptography are valuable for sending secure data from the insecure channels [5], which is recognize as the worse case used in the internet and e-commerce now a days. To secure the information over an unsafe channel first public key cryptography was presented by Diffie and Hellman [1] in 1976. They introduced a protocol for exchanging information over an unsecured channel. Afterwards various public key cryptographic algorithms were introduced but the most familiar and suitable for both encryption as well as signing is RSA algorithm. This algorithm is deliberated to be the first great development in public key cryptography systems, RSA [2] is a public key algorithm which has been being applied extensively in the area of information security because of its concise preliminary, believable security and understandability. However, RSA algorithm is confidential if and only if long key strategy is considering [3]. It is rapidly losing its attractiveness. This is mainly due to the enormous computation involved. Private Key algorithms are faster than the public key algorithms [5] and because of that many researchers are trying to boost up the computational efficiency of public key cryptography.

The rest of the paper is organized in seven sections. Section 2 briefly describes the RSA methodology and its algorithm. Section 3 contains the improvements over standard RSA. Section 4 describes the proposed method and then comparison. Section 6 explains attacks and their effect on proposed algorithm. The paper is concluding at last.

2. RSA METHODOLOGY
RSA algorithm was publically described by Ron Revister, Adi shamir and Leonard Adleman [2] at MIT in 1977.For Public key Cryptography RSA is the well known algorithm. The first algorithm suitable for signing as well as encryption is the RSA algorithm. The RSA algorithm uses modular multiplication and exponentiation [6, 8]. As in Public key cryptography or asymmetric key cryptography standard, separate keys are used for encryption and decryption. One is public and other one private key. The keys are generated by applying some computational effect on the product of two large prime numbers [9]. The public key is send to everyone in the system but the Private Key is kept secret in RSA. The private key can only be calculated by the public key. The security of the RSA cryptosystem depends upon the difficulty of factoring large prime numbers [10]. Of course the technique of factoring of numbers is improving but still the speed depends on the size of prime numbers. The improvement over the standard RSA is gradually done improving day by day.

2.1 Working of RSA
In RSA algorithm each user of the system makes the two number public (e, n) also called public key and keeps a number secret (d) is also called private exponent. If a user A wants to send a message to user B, user A wants to look up user B's public key and have message M (written in the form of integer value) then user A creates the block of message of size < n and then sends the cipher text $C=M^e \bmod (n)$ to user B. then the receiver user B decrypt the text by $M=C^d \bmod (n)$.the security of algorithm depends on the choice of public and private keys. They must be significantly large.

2.1.1 Key Generation of RSA
1. Choose random large prime integers p and q of roughly the same size.
2. Calculate the system modulus n= p*q.
3. Calculate Euler totient function [7] $\varphi(n) = (p-1) *(q-1)$.
4. Choose a random encryption exponent e such that gcd [e, $\varphi(n)$] =1 and $1<e<\varphi(n)$.
5. Calculate the decryption exponent d, $e*d \equiv 1 \bmod \varphi(n)$.
6. Public Key Ku = (e, n) and Private Key Kr = (d, p, q).

2.1.2 Encryption of RSA

In the RSA encryption process, the user B encrypt the message M by using the public key of user A. User B should do the following:

(a) Obtain user A public key (n, e).
(b) Represent the message M in integer form in the interval [0, n-1]
(c) Compute $c = m^e \bmod n$.
(d) Send the encrypted text C, to user A.

2.1.3 Decryption of RSA

To recover plaintext or message M from C, user A should do the following:
Use the private key d to recover $M = C^d \bmod n$.

3. IMPROVMENTS OVER THE STANDARD RSA

Asymmetric key cryptography such as RSA is much slower than the DES and other symmetric key cryptography and because of that lot of research work has been done to improve the speed of RSA cryptosystem.

In 1982, J.J. Quisquater and C. Couveur [11] describe a proposed technique to increase the speed of RSA decryption algorithm. Quisquater use the concept of Chinese remainder theorem (CRT), which was called QCRSA that improves the basic RSA decryption performance. Furthermore the concept of Batch RSA [12] was introduced in 1989, the concept of Batch RSA is that, if small public exponent e are used for some modulus n, the decryption of the two cipher text can be done at the cost of one but that technique is only valuable when the public key exponents e1 and e2 have small values. After that, In 1989 the concept of MultiPrime RSA [13, 14] was introduced, the RSA system modulus was enhanced so that it consist of k prime numbers p1, p2,……pk. instead of only two using in RSA. After that the concept of MultiPower RSA [15] was invented in 1998, in this method, $n = p^{(k-1)}.q$ here p and q are n/k bits long. Furthermore the concept of Rebalanced RSA [13] was proposed in 1990.This was design to fulfills requirement of that application where we need the faster decryption or signing algorithm by displacing the work to the encryption or verification algorithm and then after some algorithm has been generated by the combination of this algorithm. In 2009 D.Garg and S. Verma [17] gives the comparisons of RSA variants (Batch RSA [12],Multiprime RSA [13, 14], Multipower RSA [15], Rebalanced RSA [13], Rprime RSA [16]).The one of the proposed enhanced method of RSA was introduced by A.H. Al-Hamami and I.A. Aldariseh [18] and is describe here.

In 2012, A.H. Al-Hamami and I.A. Aldariseh [18] proposed a new concept in RSA cryptosystem by enhancing the RSA algorithm by the use of additional third prime number in the composition of the public and private key with reduced size, instead of two large prime numbers. In this method they generate the variable n Large and the process of analysis of the factors is more complex than the original algorithm.

3.1 Methodology

(a) Choose three distinct prime numbers p, q and s.

(b) Calculate value of n such that n = p*q*s and that n will be used for both public and private key.

(c) Find the Phi of n, $\varphi(n) = (p-1)(q-1)(s-1)$.

(d) Choose an e such that $1 < e < \varphi(n)$, and such that e and $\varphi(n)$ share no common divisors other than 1 (e and $\varphi(n)$ are relatively prime). e is kept as the public key exponent.

(e) As same as the original RSA determine d, by satisfies the congruence relation $d*e = 1 \pmod{\varphi(n)}$. d is kept as a private key exponent.

In this method the public key (e, n) and the private key (d, n) are same as RSA but generated differently. Here also the process of encryption and decryption are same as RSA. The encryption equation is $C = M^e \pmod n$ and the decryption one is $M = C^d \pmod n$.

In the Hamami and Aldariseh algorithm, factor n, e and d are involved in computation. All are lager number and approximate n bit long, so the encryption and decryption complexity of this algorithm is $O(n^3)$.

4. PROPOSED WORK

The proposed scheme is trying to provide an enhancement to the Hamami and Aldariseh [18] method by proposing a method that have speed improvement on the RSA decryption side and also provide the security by avoiding some attacks possible on RSA. Using the random number k if same message is encrypted more than one time it will look different every time. The general idea towards this scheme is to use the Key generation algorithm of Hamami and Aldariseh method and proposed a proposed scheme for encryption and decryption algorithm. The existence of three prime numbers, the difficulty of analysis of variable n must be increases and the key generation time must be reduces. The algorithm for the proposed scheme is as follows:

4.1 Key Generation for Proposed Scheme

To generate the key using three prime numbers user A should do the following:

(a) Generate three large prime numbers p, q, s.

(b) Calculate n=p*q*s and $\varphi(n) = (p-1)(q-1)(s-1)$.

(c) Select e such that (e, $\varphi(n)$) are relatively co-prime.

(d) Get the value of d by using $e*d = 1 \bmod \varphi(n)$.

(e) Find dp=d mod (p-1),dq=d mod(q-1), ds=d mod(s-1).

(f) Public Key Ku=<e, n>and Private key Kr=<d, p, q, s, dp, dq, ds>.

4.2 Encryption for Proposed Scheme

To encrypt the massage M user B should do the following:
User B should obtained the public key of user A <e, n>

(a) Represent the message M as an integer form in interval [0 to n-1].

(b) Select k as a random integer gcd(k, n)=1 and 1< k < n-1.

(c) Compute $C1 = k^e \bmod n$.

(d) Compute $C2 = M^e.k \bmod n$.

(e) Send the cipher text values (C1, C2) to user A.

4.3 Decryption for the Proposed Scheme

On decryption process use concept of RSA with CRT. To recover the message from cipher text C2 user A should do the following:

(a) Calculate Cp=C1 mod p,Cq=C1 mod q, Cs=C1 mod s. and then calculate $kp = Cp^{dp} \bmod p$, $kq = Cq^{dq} \bmod q$ and $ks = Cs^{ds} \bmod s$.

(b) By using the formula calculate k
$k=[kp.(qs)^{(p-1)} \bmod n + kq.(ps)^{(q-1)} \bmod n + ks.(pq)^{(s-1)} \bmod n]$.

(c) By using the Euclidean algorithm, calculate the value of the unique integer t, $t*k= 1 \bmod n$ and $1< t < n$.

(d) Then compute M^e, $C2*t = (M^e.k)t = (M^e)\ k.t = M^e \bmod n$.

(e) For getting the value of message M should do the following steps

First calculate $C'p=M^e \bmod p$, $C'q=M^e \bmod q$, $C's=M^e \bmod s$ and then calculate $Mp=C'p^{dp} \bmod p$, $Mq=C'q^{dq} \bmod q$, $Ms=C's^{ds} \bmod s$.

(f) Finally recover the message M by using the following formula:
$M= [Mp.(qs)^{(p-1)} \bmod n + Mq.(ps)^{(q-1)} \bmod n + Ms.(pq)^{(s-1)} \bmod n]$.

4.4 A Worked Example

Here, present an example for the proposed scheme in RSA encryption and decryption process .We have used artificially small values to clarify the concept. However, the method is applicable in general to all suitable selected values.

KEY GENERATION: User A should do the following

(a) Choose three prime numbers p, q and s.

(b) p=71, q=37, s=11.

(c) $n=p*q*s=28897$ and $\varphi(n) = (p-1)(q-1)(s-1) =25200$.

(d) Gcd $[e, \varphi(n)] =1$, $1 < e < \varphi(n)$.

(e) If e=29 then d=869 and dp=29, dq=5, ds=9.

(f) Ku= {29, 28897}, Kr= {869, 71, 37, 11, 29, 5, 9}

ENCRYPTION: User B should do the following

(a) Obtain public key of user A (29, 28897)

(b) Consider message M=45, $1 < M < n-1$.

(c) Random value k=46, Gcd[k, n] = 1.

(d) $C1=46^{29} \bmod 28897 = 12513$

(e) $C2=45^{29}.46 \bmod 28897 = 6756$

(f) Send (12513, 6756) to user A.

DECRYPTION: User A should do the following

By putting the values in formula motioned in the proposed scheme at decryption side.

(a) Get Cp=17, Cq =7, Cs=6. and then calculate kp=46, kq=9 and ks=2.

(b) Computing k = 46 then t=3141.

(c) Compute M^e, $6756*3141 = M^e \bmod 28897$, $M^e=10198$.

(d) Then after calculate the values of C'p=45, C'q=23, C's=1 and then calculate Mp=45, Mq=8, Ms=1.

(e) Finally recover the message M = 45.

5. COMPARISION

Now, compare the Hamami and Aldariseh algorithm and the proposed scheme on the basis of encryption and decryption time complexity. The proposed scheme is computationally less expensive than the Hamami and Aldariseh algorithm. The new scheme uses the concept of RSA with CRT that reduces the decryption time.

The table 1 shows the comparison of the Hamami and Aldariseh algorithm and the new scheme on the basis of encryption and decryption complexity.

Table 1 Comparison on the basis of complexities

Comparison	Hamami and Aldariseh Algorithm	New Shame
Encryption Complexity	$O(n^3)$	$22n^2 + O(n^3)$
Decryption Complexity	$O(n^3)$	$(8u+6n^e+10)\ n^2 + O(n^2)$

6. ATTACKS AND THEIR EFFECT ON PROPOSED METHOD

One straight method of breaking RSA is to enumerate all elements in the multiplicative group of n until M is found but such method are very complex and time consuming. During the past year various attacks [10] are possible on RSA and such attacks are considered below.

6.1 Common Modulus Attack

If also same message M is encrypted twice using the same modulus n, then common modulus attack (CMA) [10] can occur and by that attack one can retrieve the message M as follows: Let $C1=M^{e1} \bmod n$, and $C2=M^{e2} \bmod n$ be the cipher texts corresponding to message M, where gcd (e1, e2) = 1, then attacker recovers original message $M'=C1^a * C2^b \bmod n$ for $e1*a + e2*b = 1$. Using the extended great common divisor (GCD) one can determine a and b then calculate M without knowing private key d.

The CMA is applicable in Hamami and Aldariseh method because it uses the encryption and decryption as same as original RSA algorithm but in proposed scheme using a unique integer k by that there are two cipheretext generated and it seems to be impractical to apply that attack on proposed scheme.

6.2 Chosen Cipher Text Attack

RSA has follows the multiplicative property of the modular arithmetic [20]. That means product of the two cipher texts is equal to the encryption of the product of the corresponding plaintexts. That is $M1^e.\ M2^e = (M1.M2)^e \bmod n$ and because of this chosen-cipher text attack (CCA) [19] is possible in RSA. The algorithm can be explained as follows: Let $C = M^e \bmod n$, the attacker chooses a random number r where $1 < r < n$, such that gcd (r, n) =1 then compute $x = r^e \bmod n$, $C' = x * C \bmod n$, $z * r = 1 \bmod n$, and send C' to victim. The victim compute $M' = (C')^d \bmod n$, then send M' to the attacker, the attacker recovers original message $M = z * M' \bmod n$. That attack is depends on the logical presumption that the intruder has able to access the decryption mechanism that results the overall decryption for a chosen cipher text.

The CCA is applicable in both of the three algorithm means in original RSA algorithm, in Hamami and Aldariseh algorithm and in the proposed one but by applying CCA on proposed scheme for getting the value of message M, it seems to be complex and more time consuming as compare to the Hamami and Aldariseh algorithm because on that algorithm CCA is applicable faster.

The Table 2 shows time required to apply the CCA for getting the value of message M in Hamami and Aldarish algorithm (A1), and the proposed scheme (A2). Here it is consider that the value of k should be used in the proposed algorithm only and the other values means prime numbers, public and private keys and value of r is same for both the algorithm.

Table 2 Time required to getting the message by applying CCA

P	Q	S	N	Public key	Private Key	r	k	A1 Sec.	A2 Sec.
53	59	61	190747	80021	511011	131	103	2.45	4.18
59	61	67	241133	80041	452441	677	107	2.88	4.47
53	71	97	365011	80077	558133	73	110	3.30	5.39
73	83	79	478661	80167	462331	1481	127	3.55	5.78
97	89	83	716539	80177	131669	199	113	3.78	6.48

Now, graphically represent the comparison of the time required to recover the message M by applying CCA in Hamami and Aldarish Algorithm and in proposed scheme. For same value of modulus n the time required to getting the value of M is higher in the proposed scheme. The below Figure 1 represents this comparison.

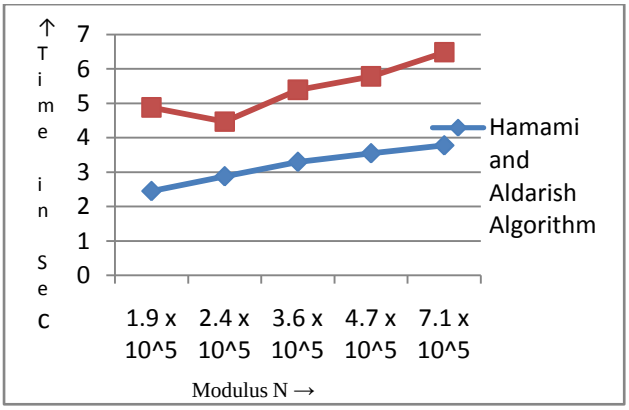

Figure 1 Comparison of Time required recovering message by applying CCA on different algorithm

6.3 Timing Attack

Timing attack is one that occurs at RSA implementation Kocher [21] shows that an attack can determine the value of private key by maintaining the track of how much time a computer takes to decrypt the encrypted message. Let us consider an example take a case of smartcard that contains the secret key of RSA algorithm. As know that, the smart card is tamper resistant, an intruder may not be able to see its contents and disclose the key. Kocher demonstrates that by preciously measuring the time taken by the smartcard to achieve the RSA decryption, intruder can speedily discover the private key exponent d.

Timing attack is applicable is the original RSA algorithm and the Hamami and Aldariseh algorithm because by preciously measuring the time for encryption and decryption, and time for key generation one can determine the value of the secrete key exponent d, but in proposed scheme is using a random unique integer k in the encryption and decryption process that makes it difficult to distinguish between the time for public key e or private key d and the time for k.

6.4 Small Private Key Exponent

It has been proven that the RSA algorithm takes longer time for decrypting the cipher text. In most of the real life appliance, the encryption process is achieved by some particular mechanism, such as a smart card. In such cases, raising a plaintext m to a high power might be costly in terms of power consumption or time. For reducing the time of decryption and signing process one can choose the small value of decryption exponent d instant of random value. Michael Wiener [22] explained an attack that shows small value of decryption exponent d should point to the total collapse of RSA cryptosystem. Wieners attack, will recover d, when d is acceptable to one third the size of n and e is less than the size of n. This hardly takes place if the value of e and d are picked at random, and don't take place if e has a small value.

6.5 Small Public Key Exponent

Very powerful attacks on small e are based on Coppersmith's Theorem [23]. In RSA Algorithm encryption and signature verification are quicker if choosing a small value of e (like e = 3), but that is also be apprehensive. If the distinct public key has equal value for e and generate encrypted texts e*(e + 1) / 2 by using these key for linearly dependent message, for that there is an attack occurs across the system. There is not any problem occurs if the messages are less than that encrypted texts, or the messages are irrelevant to each other. But if the messages are identical, then e messages are enough. The most straightforward explanation of this attack is to pad the message by those values that are independently random.

6.6 Known Plain-Text Attack

The known-plaintext attack is one where the attacker has known some quantity of plaintext and corresponding cipher-text [3].Given such a sorted set *S= {{p1, c1},{p2,c2},..., {pr, cr}}* (where *pi* Є *P* plaintext set, *ci* Є *C* cipher text set, *r < ø (n)* is the order of *Zn*)* an attacker can determine the plaintext *px* if the corresponding *cx* is in *S*.

The known-plaintext attack deals with the some known plaintext corresponding to the ciphertext and it is applicable in the original RSA algorithm and the Hamami and aldariseh algorithm. But it seems to be impractical in the proposed scheme because here, generating the two cipher text for the one particular plaintext and if it is applicable in the proposed scheme it is very difficult to getting the value of particular plaintext by applying these attacks.

6.7 Factorization Attack

Now days the most promising approach to solving RSA problem is to factor the modulus n [10], by that the whole algorithm becomes open. When attacker can find the prime factor an attacker can be capable to compute the secret key exponent d from (e, n), and then decrypt the cipher text by using the standard RSA algorithm. If one want to avoid the factorization attack on RSA cryptosystem the major requirement is that p and q should be about the same bits length and sufficiently larger. For a moderate security level p and q should be at least 1024 bits length [24], this will result in a 2048 bit length for modulus n. furthermore p and q should be

random prime numbers and they cannot be the some special case binary bit structure. The TWIRL hardware device proposed by Shamir and Tromer [25] in 2003, challenge the security of 1024 bit keys. That's why key of length at least 2048 bits is recommended.

Now, The Proposed scheme described in the paper can be protect us from the following attacks:

Table2 Proposed Scheme against the following attacks

ATTACK	PROPOSED SCHEME
Common Modulus attack	This attack is seems to be computationally impractical because the value of k is different for each message.
Chosen Cipher text attack	This attack is applicable but requires long time to get the value of message.
Timing attack	By using k in encryption and decryption has make it difficult to distinguish between the time for public key e or private key d and time for k.
Known plain text attack	This attack is computationally infeasible in Proposed scheme.

7. CONCLUSION AND FUTURE WORK

This paper describes the RSA cryptosystem and its variants. The proposed algorithm has speed improvement on the decryption side of RSA algorithm by using the concept of Chinese remainder theorem and the method also improves the security of RSA algorithm by avoiding some attacks that are possible on RSA algorithm like common modulus attack, chosen ciphertext attack, timing attack and known plaintext attack.

In future, work on those attacks that are not considering in this paper and provide more secure RSA cryptosystem. Here, also the encryption time is not considered. So in future also work on the encryption side so the time for encryption reduces.

8. REFERENCES

[1] W. Diffie and M. Hellman, "New Direction in Cryptography," IEEE Transaction on Information Theory, vol. 22, pp. 644-654, 1976.

[2] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public-key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[3] R. C. Merkle, "Secure Communications over Insecure Channels," Communications of the ACM, vol. 21, no. 4, pp. 294-299, 1978.

[4] A. Al-Hasib and A. A. M. Mahmudul Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," in IEEE Third International Conference on Convergence and Hybrid Information Technology, 2008.

[5] S. B. Sasi, D. Dixon and J. Wilson, "A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security," IOSR Journal of Engineering, vol. 4, no. 3, 2014.

[6] G. R. Blakey, "A Computer Algorithm for Calculating the Product AB Modulo M," IEEE Transaction on Computers, vol. 32, no. 5, pp. 497-500, 1983.

[7] N. Pabhopote and V. Laohakosol, "Cobinatorial Aspects of the Generalized Euler's Totient," International Journal of Mathematics and Mathematical Science, pp. 1-15, 2010.

[8] L. Harn, "Public-Key Cryptosystem Design Based on Factoring and Discrete Logarithms," IEE Proceedings: Computers and Digital Techniques, vol. 144, no. 3, pp. 193-195, 1994.

[9] T. Beth and D. Gollmann, "Algorithm Engineering for Public Key Algorithms," IEEE Journal on selected areas in communications, vol. 7, no. 4, pp. 458-465, 1989.

[10] D. Boneh, "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, vol. 46, no. 2, pp. 203-213, 1999.

[11] J. J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," Electronic Letters, vol. 18, no. 21, pp. 905-907, 1982.

[12] A. Fait, "Batch RSA," Advance in Cryptology CRYPTO '89, vol. 435, pp. 175-185, 1989.

[13] D. Boneh and H. Shacham, "Fast Variants of RSA," CryptoBytes, vol. 5, no. 1, pp. 1-10, 2002.

[14] T. Collins, D. Hopkins, S. Langford and M. Sabin, "Public Key Cryptographic Apparatus and Method". US Patent #5848, 1997.

[15] [T. Takagi, "Fast RSA-type Cryptosystem Modulo pkq," Advances in Cryptology - CRYPTO '98, vol. 1462, pp. 318-326, 1998.

[16] C. A. M. Paixon, "An efficient variant of the RSA cryptosystem," Cryptology ePrint Archive, 2002.

[17] D. Garg and S. Verma, "Improvement over Public Key Cryptographic Algorithm," in IEEE International Advance Computing Conference, Patiala, 2009.

[18] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm," IEEE International Conference on Advanced Computer Science Applications and Technologies, pp. 402-408, 2012.

[19] Y. Desmedt and A. M. Odlyzko, "A Chosentext Attack on RSA Cryptosystem and some Discrete Logarithm Schemes," Advances in Cryptology CRYPTO '85, vol. 218, pp. 5116-521, 1986.

[20] R. Kumar, "Security Analysis and Implementation of an Improved Cch2 Proxy Multi-Signature Scheme," International journal of computer network and Information security, vol. 4, pp. 46-54, 2014.

[21] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology-CRYPTO '96, pp. 104-113, 1996.

[22] M. Wiener, "Cryptanalysis of Short RSA Secret Exponents," IEEE Transaction Information Theory, vol. 36, no. 3, pp. 553-558, 1990.

[23] D. Coppersmith, "Small Solutions to Polynomial Equations and Low Exponent RSA Vulnerabilities," Journal of Cryptology, vol. 10, pp. 233-260, 1997.

[24] D. Gordon, "Discrete Logarithms in GF(p) using the Number Field Sieve," SIAM J. Discrete Math, vol. 6, pp. 124-138, 1993.

[25] A.Shamir and E. Tromer, "Factoring Large Numbers with the TWIRL Device," Proceedings, CRYPTO, LNCS 2729, pp. 1-26, 2003.