Enhanced Method for RSA Cryptosystem Algorithm

Prof.Dr.Alaa Hussein Al-Hamami and Ibrahem Abdallah Aldariseh
alaa_hamami@yahoo.com ibrahem_aldariseh@yahoo.com
Department of Computer Science College of Computer Sciences and Informatics
Amman Arab University

Abstract: This paper proposed enhancing the RSA algorithm through the use of additional third prime number in the composition of the public and private key. This will increase the factoring complexity of the variable (n), where the process of its analysis with the development of equipment and tools becomes much easier nowadays.

The existence of three prime numbers will give the ability to the enhanced encryption method to increase the difficulty of factoring of the variable (n), as well as speed increasing in the process of encryption and decryption. To generate a variable (n) using the original RSA algorithm, which contributes generating the public and private key that have a number of 300 digits by using two primes number with 150 digits each. In this case the multiplication process will take longer than the time of generating the same variable (n) by using three prime numbers where each number with 100 digits.

We have conducted experiments on a set of numbers randomly, as they proved that the Enhanced Method for RSA Cryptosystem Algorithm is faster than the original algorithm in encryption and decryption process and generating public and private key. Also it shows that the analysis of the variable (n) will take a long time in the Enhanced Method for RSA Cryptosystem Algorithm and this indicates the increasing complexity in the analysis method.

Keywords: *Cryptography, Public Key, Prime Numbers, complexity, and Cryptosystem Algorithm.*

978-0-7695-4959-0/13 $25.00 © 2013 IEEE
DOI 10.1109/ACSAT.2012.102

1. Introduction

It should be noted that the business on the Internet, which require millions of exchanges, banking secrecy has become close to the reach of many, and respond market network security quickly for challenges of security the Internet by adopting the techniques of verification and encryption are available in this area to apply to links the Internet, and through the development of new products in the field of information security, today's markets are in chaos, standards, techniques and products [1].

The developed hardware and tangible tools are not sufficient to protect the data from unauthenticated parties and -more and more-most of encumbrance is under the software systems and controlling responsibilities. Therefore, the experts, researchers and developers have to build and develop security systems, protect the information and prevent the attackers from playing with the very important source (information). 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.

2. Rivest, Shamir, and Adelman (RSA) Algorithm

RSA is a form of public key encryption. In the RSA public-key cryptosystem, a participant creates his/her public and secret keys with the following procedure [2].

At the moment RSA seems to be extremely secure. It has survived over 20 years of scrutiny and is in widespread use throughout the world. The attack that is most often considered for RSA is the factoring of the public key. If this can be achieved, all messages written with the public key can be decrypted.

The point is that with very large numbers, factoring takes an unreasonable amount of time. It has not been proven that breaking the RSA algorithm is equivalent to factoring large numbers (there may be another, easier method), but neither has it been proven that factoring is not equivalent. There are different type's attacks on the RSA such as: Searching the Message Space, Guessing private key (d), Cycle Attack, Common Modulus [4], Faulty Encryption, Low Exponent, and finally Factoring the variable N which is factoring the public key and it seems as the best way to go about cracking RSA.

Encryption algorithms rely on its strength in certain matters. Each algorithm has properties of the mismatch depends strongly on the encryption key, which depends on the arrangement of, and denounced it tries to integrate the key with the text of certain deviation.

The RSA algorithm based on the variable N which consisting of multiplying each of the P and q, which are relying on that of where to find the variable d, as the variable d is, hence the higher value of n. The variable d increases its size, the higher value of p and q the value of d increases, which means that the algorithm depends entirely on the adoption of the prime numbers because they generate a key d, depending on p and q are already primes numbers [5] .

The weaknesses of RSA algorithm when we use two prime's number are the following points which are used to break the algorithm in most cases. These weaknesses are:

(a) Small encryption exponent, if you use a small exponent like e=3 and send the same message to different recipients.

(b) Using the same key for encryption and signing.

(c) Acting as an oracle: there are techniques to recover the plaintext if a user just blindly returns the RSA transformation of the input. So don't do that.

3. The New Approach RSA cryptosystem

The idea of the new approach is, instead of using two primes numbers to generate a public key and private key, we use three primes numbers with reduced size, generates the variable N Large and the process of analysis of the factors is more difficult than the original algorithm, as well as, increases the ease of generating Public key and private key. The key strength of the RSA depends on the two prime numbers p and q. The process of factorizing of n will lead to gain the values of p and q. It is much easier to find two numbers from factoring n than finding the value of three numbers from n. In this

case it is very difficult for the intruder to find the three values from factoring n.

3.1. Key Generation

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

(b) Find n such that n = p*q*s.n will be used as the modulus for both the public and private keys.

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

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

(e) Determine d (using modular arithmetic) which satisfies the congruence relation .d*e ≡ 1 (mod φ (n)).

In other words, pick d such that de - 1 can be evenly divided by (p- 1)(q-1)(s-1), the Phi, or φ(n).This is often computed using the Extended Euclidean Algorithm, since e and φ(n) are relatively prime and d is to be the modular multiplicative inverse of e*d is kept as the private key exponent. The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret [6]. The encryption equation is c ≡ me (mod n) and the decryption one is m ≡ cd (mod n).

3.2. Proof of the New Approach RSA Algorithm

Given positive integers n, e, and d such that [7]:
$n = pqs$, where p , q and s are distinct primes……..…...……..(1).
$gcd\ (e,\ \Theta(n)) = 1$…….(2).
$de \equiv 1\ (mod\ \Theta(n))$……..(3).

Define the public and private key algorithms of a message m to be respectively, for $0 \leq m < n$,
$RSAPublic(m) = m^e\ mod\ n$,…….(4).
$RSAPrivate(m) = m^d\ mod\ n$…….(5).

Prove that

$m = RSAPrivate\ (RSAPublic(m))$, and that….(6).
$m = RSAPublic\ (RSAPrivate(m))$……(7).

(Prove that the two algorithms (6) and (7) can be used inversely to obtain the message *m*, or "Does RSA Encryption actually work?")

Proof. By substituting equations (4) and (5) into (6) and (7) respectively, we can say that [7].

$RSAPrivate\ (RSAPublic(m)) = (m^e\ mod\ n)^d\ mod\ n = m^{de}\ mod\ n.$

We can also say that $RSAPublic\ (RSAPrivate(m)) = (m^d\ mod\ n)^e\ mod\ n = m^{de}\ mod\ n.$

Therefore, equations (6) and (7) are equivalent, or *RSAPrivate (RSAPublic(m)) = RSAPublic (RSAPrivate(m))*.

If we can prove: $m = m^{de}\ mod\ n$, then the proof will be complete [7]. It is given that:

$de \equiv 1\ (mod\ \Theta(n))$…… ……(3).

By definition of mods we can write (3) as

$\Theta(n) \mid de - 1$…….(8).

Since Θ(n) = Θ(p)Θ(q) Θ(s) only when p, q and s are relatively prime, as in this case, we have

$\Theta(n) = \Theta(p)\Theta(q)\ \Theta(s)$

And by substitution into (8) we have [7].

$\Theta(p)\Theta(q)\ \Theta(s) \mid de - 1.$

By properties of divisors, we can write:

$\Theta(p) \mid de - 1,$

$\Theta(q) \mid de - 1,$

$\Theta(s) \mid de - 1$

Where there must be an integer *k* such that:

$de - 1 = k\ \Theta(p).$

Since p is prime, the *Euler phi function* states that

$\Theta(p) = p - 1$, so

$de - 1 = k(p - 1)$…… ……(9).

By the symmetric property of mods, we can write.

$m^{de} \equiv m^{de}\ (mod\ p) \equiv m^{de - 1 + 1}\ (mod\ p)$

Which can also be written as?

$m^{de} \equiv (m^{de-1}) * m \pmod p$..... …….....(10).

Substituting (9) into (10), we obtain

$m^{de} \equiv (m^{k(p-1)}) * m \pmod p$..... ……..... (11).

Since p is prime any integer m for (11) will be either.

1) Relatively prime to p or will

2) Be a multiple of p.

When

1) m is relatively prime to p, Fermat's Little Theorem states that [7]: $m^{p-1} \equiv 1 \pmod p$.

By properties of mods, we can write:

$m^{k(p-1)} \equiv 1^k \pmod p$, or

$m^{k(p-1)} \equiv 1 \pmod p$..... …….....(12).

By combining (11) and (12), we obtain:

$m^{de} \equiv 1 * m \pmod p$, *or*

$m^{de} \equiv m \pmod p$.....….....(13).

In the second case where

2) m is a multiple of p, if p | m, then for any integer k p | m^k].

From the properties of mods we can write: $m^{de} \equiv 0 \pmod p$, $m \equiv 0 \pmod p$.

Thus we can write: $m^{de} \equiv m \pmod p$. Therefore, for all m,

$m^{de} \equiv m \pmod p$ .....…….....(14)

and applying the same process for q and s we can write:

$m^{de} \equiv m \pmod q$.

$m^{de} \equiv m \pmod s$.

By the modular property of congruence which states that when m and n are relatively prime (as in our given statements), $a \equiv b \pmod m$, and $a \equiv b \pmod n$, then $a \equiv b \pmod{mn}$, we can write [7].

$m^{de} \equiv m \pmod{pq} \equiv m \pmod n$.

By the modular property of symmetry, we can write.

$m \equiv m^{de} \pmod n$.....…..... (15)

Since we have limited m to $0 \leq m < n$, only one integer will satisfy (15), and so

$m = m^{de} \bmod n$..... (16)

If we substitute equation (16) with our original equations [45] we get:

$RSAPrivate\ (RSAPublic(m)) = m^{de} \bmod n$, *and*

$RSAPublic\ (RSAPrivate(m)) = m^{de} \bmod n$

We obtain, for $0 \leq m < n$,

$$RSAPrivate\ (RSAPublic(m)) = m, \&$$

$$RSAPublic\ (RSAPrivate(m)) = m.$$

4. ANALYSIS of the New Approach RSA CRYPTOSYSTEM

The new approach RSA Cryptosystem requires the use of a public key and a private key. Both these keys must fulfill certain conditions to ensure the integrity of the system. The following steps illustrate the key generation algorithm for the proposed RSA [8]:

a. Choose three large prime numbers of approximately the same size, namely p, q and s

b. Compute the product of these three primes, $n = pqs$.

c. Also, compute the value of $\varphi(n) = (p-1)(q-1)(s-1)$.

d. Choose an integer e between 1 and $\varphi(n)$ such that $gcd(e, \varphi(n)) = 1$.

e. Finally, compute d whereby $d = e^{-1} \bmod(\varphi(n))$.The public key is (n, e) whereas the private key is (n, d).

COMPLEXITY FOR STEP a:

1. For selecting the first prime number p, the complexity can be computed as the product of the number of numbers to be tested for primarily and the complexity of one primarily tests. Complexity of MILLER-RABIN

gives the above mentioned complexities so the complexity for finding a prime number is $O(s.\ (\log_2 p)^3\ .ln\ p)$ [8].

2.Similarly for the second prime number q, complexity is $O(s.\ (\log_2 q)^3\ .ln\ q)$.

4.Similarly for the third prime number s, complexity is $O(s.\ (\log_2 s)^3\ .ln\ s)$.

COMPLEXITY FOR STEP b:

As step 2 involves only the computation of *n*, which is the product of *p* , *q and s*. So the complexity of step 2 is $O(\log_2 p.\ \log_2 q.\ \log_2 s\ )$ binary operations.

COMPLEXITY FOR STEP c:

By MODULAR-EXPONENTIATION, the complexity for the second part is $\Theta(n)\ -1$. Therefore complexity of the step 3 is [8]: $O((\log_2(p-1).(q-1)\ .(s-1))^3.\ ((p-1).(q-1)\ .(s-1)-1))$.

COMPLEXITY FOR STEP d:

The complexity for step 4 is $O(\log_2\ (p-1).(q-1)\ .(s-1)+ gcd(e,\ (p-1).(q-1)\ .(s-1)))$, as we know that *e* and $\Theta(n)$ are prime to each other so $gcd(\ e\ ,\ (\ p\ -\ 1).(\ q\ -\ 1\ )\ .(s-1)) = 1$,and so complexity is

$O((\log_2(\log_2 p-1).(\log_2 q-1)\ .(\log_2 s-1))^3 + 1)$.

5. Comparison between the original Algorithm and the modified one:

5.1. Encryption and Decryption Time.

Tables 1 & 2 show the Encryption and decryption times for the generated public and private keys that using two prime numbers (Table 1) and three prime numbers (Table 2).

Prime1	Prime2	Prime3	N	phi	Public key	Private key	Time Encrypt Sec.	Time Decrypt Sec.
677	691	709	331675163	330239520	90401	259337441	1.09	1.3
733	829	683	415029731	413357472	90053	47645837	1.21	1.31
769	709	773	421455833	419770368	90379	51540643	1.25	1.31
677	887	751	450974749	449202000	90107	20474243	1.47	1.46
683	839	797	456710489	454926736	90407	25783895	1.47	1.47
823	821	691	466896953	465087600	90007	87197143	1.47	1.47
727	769	839	469053857	467241984	90439	306412663	1.62	1.47
911	757	823	567563021	565503120	90217	534105433	1.62	1.47
809	821	857	569209973	567151360	90001	490523761	1.63	1.52
907	761	919	634318613	632098080	90373	542731597	1.78	1.6

Table 1: Encryption And Decryption By using Two Primes

Prime1	Prime2	N	phi	Public key	Private key	Time Encrypt Sec.	Time Decrypt Sec.
21107	21023	443732461	443690332	90481	426669641	1.11	1.32
21023	21163	444909749	444867564	90371	419456687	1.46	1.46
21179	21139	447702881	447660564	90379	191285623	1.46	1.46
21169	21169	448126561	44804224	90187	29258851	1.62	1.47
21247	21187	450160189	450117756	90053	76909841	1.62	1.47
21163	21277	450285151	450242712	90073	25827985	1.63	1.47
21139	21347	451254233	451211748	90173	284078309	1.63	1.47
21121	21401	452010521	451968000	90001	273990001	1.79	1.47
21323	21211	452282153	452239620	90089	201549809	1.94	1.62
21419	21391	458173829	458131020	90163	147551287	2.62	1.62

Table 2: Encryption And Decryption By using Three Primes

Now we will compare between the Encryption time of the two algorithms (2 & 3 primes) from the two tables (1 & 2) and you will notice results in Figure 1:

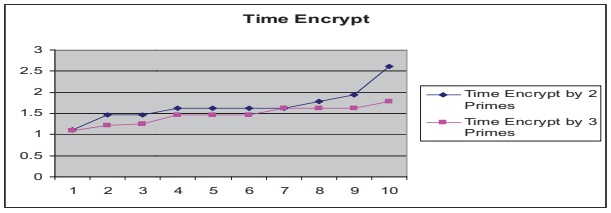

Figure 1: Comparison of Encryption Time.

Figure 2 shows the comparison of the Decryption time for the two algorithms (2 & 3 primes) from the two tables (1 & 2).

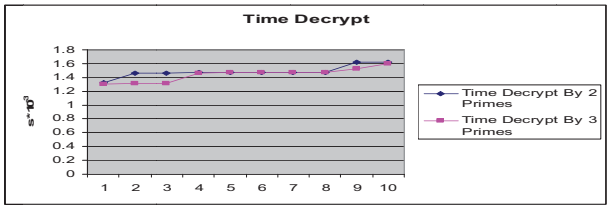

Figure 2: Comparison of Decryption Time.

Table 3 shows the comparison between the two algorithms according to some criteria.

Type	Two Prime Numbers (Table 1)	Three Prime Numbers (Table 2)
Average of N	449863773	478288838
Average of Phi (n)	409493354	476457824
Sum of Encryption Time	16.88	14.61
Average of Encryption Time	1.688	1.461
Sum of Decryption Time	14.83	14.38
Average of Decryption Time	1.483	1.438

Table 3 shows the comparison between table1 and 2:

From Table 3 we notice that the process of encryption and decryption in the proposed method are faster than the original method by the apparent results.

6. Second application: (Generation & Factorization of The Key, Composed from 18 Digits

Tables 4 and 5 show the key generation time in seconds and the key factoring time for the original algorithm (Table 4) and the enhanced method (Table 5) where the value of N consist from 18 digits.

Table 4: Generation And Factorization Key from 18 Digits by 2 primes.

Prime1	Prime2	N	Phi	Public key	Private key	Time generate key Sec.	Time factoring key Sec.
695147891	695146163	483229389146192000	483229387755898000	32416188191	1133933750071	0.15	2.858
695146619	695148347	483230023120488000	483230021730193000	32416190071	1832524625554	0.16	3.455
695146757	695148287	483230077342155000	483230075951860000	32416189987	1170338341678	0.2	4.125
695148227	695148347	483231140919030000	483231139528734000	32416188261	3415960300093	0.31	4.812

Prime1	Prime2	Prime3	N	Phi	Public key	Private key	Time generate key S	Time factoring key S
751871	800053	800287	481401960348709000	481400116829816000	32416187987	367225846967	0.15	3,114.930
751879	800077	800281	481417914414005000	481416070854363000	32416189909	2093559536111	0.16	8,867.920
751871	800159	800209	481418815807825000	481416972245455000	32416189381	2268509775597	0.16	9,588.630
751823	800077	800473	481497549502145000	481495705734158000	32416188601	3773843231190	0.31	12,332.340

Table 5: Generation And Factorization Key from 18 Digits by 3 primes.

Table 6 shows a comparison for the key generation Time and key factoring time in the two algorithms. The key size is 18 digits.

Table 6

Type	Algorithm 1 (2 Primes)	Algorithm 2 (3 Primes)
Key Generation Time	Average: 0.205 Sec.	Average: 0.195 Sec.
Key Factorization Time	Average: 3.812 Sec.	Average: 8475.95 Sec.

Figures 3 and 4 show the differences graphically. Figure 3 shows that the process of generating the key to be faster in the proposed method because of the prime numbers values which consisting variable N are less than the values in the old method. Therefore, the multiplication in the proposed method is easier and faster while in the original method is more complex and requires more time, and this explains the speed of generating the key in the proposed method. Figure 4 shows the difference of the factoring time between the old algorithm and the enhanced one.

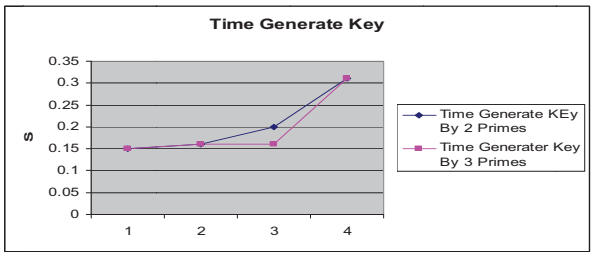

Figure 3: Time Generate Key

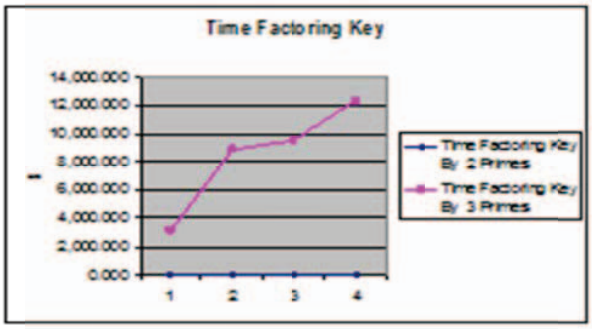

Figure 4: Time Generate Key

7. Conclusion

The encryption system is the most important operations in the protection of information and data for the users. We have studied one of the encryption systems that are very important and used in the daily lives, RSA System. We have studied the strengths and weakness in the RSA algorithm. We have focused in this paper on the analysis process of the variable n to

make it more complex for the factorization of the variable n.

We can sum up the conclusions in the following points:

- The proposed method has succeeded in increasing the difficulty of analysis the variable N.
- Increasing speed in the process of generating keys.
- It increases the speed of the encryption and decryption process, and this means the provision of time on the user.

References

[1] Stallings, William; cryptography and network security; fourth edition; 2005; ISBN: 0-13-187316-4.

[2] Cromen, Thomas; and others; introduction algorithms; second edition; 2003; ISBN: 0-262-03293-7.

[3] John Wiley & Sons; Applied Cryptography; Second Edition; 1996; ISBN 0-471-11709-9 .

[4] Al-Hamami Alaa and saad al ani; Technology of information security; first edition; dar wa'ael for publishing; 2007.

[5] Strength Assessment Of Encryption Algorithms, Discretix Technologies Ltd. Limor Elbaz & Hagai Bar-El, October 2000.

[6] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"

[7] RSA THEORY , avid Ireland, Last updated: 5 May 2007. This Latex version first published: 2 October 2006.

[8] "Step-wise calculation of Performance and Complexity Analysis of Safer with RSA Algorithm" , Amar Kumar Mohapatra , Dr. Nupur Prakash, University School of Information Technology.

[9] Sattar j Abboud and Mohammad a AL-Fayoumi. Efficient method for breaking RSA scheme. Ubiquitous Computing and Communication journal.2008.

[10] Attacks On the RSA Cryptosystem, Dr. Kartik Krishnan, Xiao-lei Cui,2005.

[11] P. KOCHER, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems ,CRYPTO '96, Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp. 104–113.

[12] Mathematical Attacks on RSA Cryptosystem , 1Imad Khaled Salah, 2Abdullah Darwish , Amman Arab University for Graduate Studies, Science Publications 2006.

[13] Experience in Factoring Large Integers Using Quadratic Sieve, D. J. Guan, National Sun Yat-Sen University, April 19, 2005.

[14] Coppersmith, D. "Attack on the Cryptographic Scheme", Advances in Cryptology–CRYPTO '94, Springer-Verlag, LNCS 839, pp.294-307,1994.

[15] "CRYPTANALYSIS OF RSA USING ALGEBRAIC ANDLATTICE METHODS", Glenn Durfee, stanford university ,2002