International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
1793-8201

Solovay-Strassen test in a RSA Pubic key Cryptosystem

L. Sreenivasulu Reddy , K.Ramakrishna Prasad, N.Ch. S.N.Iyengar, and V.Ramachandran

***Abstract*—In this paper, RSA type of Public key cryptosystem is designed based on Solovay-Stressen test known as S-RSA Cryptosytem. The efficiency of the S-RSA cryptosystem is nearly twice of the efficiency of basic RSA cryptosystem which is proved mathematically and is shown graphically with an illustration. Also, the Performance of this system is measured in terms of big theta notation for best approximation. This paper also describes and measures the capability of four basic attacks on S-RSA cryptosystem.**

***Key words*—Knapsack problem, Legendre symbol, congruence, in congruence, Factorization of numbers, Euler theorem, Solovay-Strassen test.**

I. INTRODUCTION

The concept of public key cryptosystem is a recent one: it was invented by Diffie, Hellman, and Merkle in 1976[1].In public key cryptosystems, the encryption key is different from decryption key, and further , it is infeasible to obtain the decryption key from the encryption key. Usually, the encryption key is made public. For this reason, the encryption key is also known as the public key and the decryption key is known as the private key. There are only a few public key cryptosystems that are both efficient and believed to be secure at present. The most popular among these is RSA cryptosystem [4] .It is the first practical realization of a Public key cryptosystem was accomplished by Rivest, Shamir and Adleman in 1978. The first public-key algorithm was proposed based on a hard-to-solve problem (known as knapsack problem) and it became insecure. In fact, there have been many systems proposed based on the same problem (such systems are called Knapsack ciphers) but nearly all of them have been shown to be insecure.

The additional hurdle in the design of a public-key system is that the decryption key should be difficult to obtain from the encryption key. At the same time, the encryption key should be easily obtainable from the decryption key. The Latter condition is needed for generating a new pair of keys easily (simple choose a random decryption key and compute the corresponding encryption key). These two conditions are naturally termed as functions .They are easy to compute but hard to inverse- the decryption key. Designing of an efficient and secure Public key cryptosystem is depended on a number of hard and complex mathematical problems in Algebraic Number theory. Most of these problems are based on the exponential and factorization of Numbers. Almost all of the public key cryptosystems of encryption space, key space and decryption space are represented by a multiplicative group $Z/(n)^*$ (the set of positive integers which are less than n and relatively prime to n). The RSA cryptosystem also based on the same space. The elements in this space satisfy only a single condition, called as relatively prime. According to the elementary set theory, the method to find an element, which is either a member of the given set or not followed by a single condition, is less complex than a set followed by more than one independent condition. Therefore, any public key cryptosystem based on any space in which the elements satisfy the more than one independent condition is high complex than that of the public key cryptosystem based on any space with only single condition.

Keeping it in view, we will design a high efficient Public key cryptosystem known as S-RSA cryptosystem with the space $E(n)$ in which the elements satisfy two conditions: solovay-strassen test condition and relatively prime condition. There are different approaches to measure the efficiency of the Algorithm in which best approach is "One possible approach is to count the number of times each of the algorithm's operations is executed". Most of the researchers measure the efficiency of the Algorithm in this approach. Generally, this efficency equal to a polynomial in some variable 'n'. The big-O notation method which gives only the at most value of the efficiency but the big- θ notation which gives both at least as well as at most efficiency value. So, we measure the efficiency interms of big- θ notation method.

The rest of the paper is organized as follows: In section 2: Explanation about the basic mathematical definitions, theorems with out proof and algorithms which are needed to our contribution. In section 3: Designing of the S-RSA cryptosystem, measuring the performance of the algorithm in terms of big- θ notation and the capability of the four important basic attacks are explained and measured. In section 4: theoretical and graphical comparison of the efficiency of the RSA and S-RSA cryptosystems and finally, in section 5,

Manuscript received August 7,2009

Dr.L.Sreenivasulu Reddy , presently is with Department of Mathematics Sri Venkateswara University, Tirupati, Andra Pradesh, India (sreenivasulu.lingam@gmail.com)

Dr.K.Ramakrishna Prasad presently Professor in, Department of Mathematics at Sri Venkateswara University, Tirupati , Andra Pradesh ,India(dr.k.ramakrishnaprasad@gmail.com)

Dr. N.Ch.S.N.Iyengar is a Senior Professor at the School Of Computing Sciences at VIT University, Vellore, T.N India (nchsniyengar48@gmail.com ,0416-2202146,Fax: 0416 2243092)

Dr.V. Ramachandran, presently Vice–Chancellor of Anna University, Trichy (T.N).India (rama@annauniv.edu)

summary and conclusion are given.

II. The Basic Concepts Which Are Needed To Our Contribution

Here some of the basic concepts are explained. For more details we refer [4],[5],[6],[7],[8].

For all $n \geq 1$ with prime factorization $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. We define the following functions:

$\nu_p(n)$ is the maximal power of p in n,

i.e., $\nu_p(n) = max\{\, i : p^i \ divides \ n\}$

$\phi(n)$ is the number of positive integer $<n$ relatively prime to n, i.e. $\phi(n) = \{\, x : x < n \, and \, \gcd(x,n) = 1\}$.

$\prod(n)$ is the number of primes $p < n$.

A. The Legendre symbol

For a prime p and an integer a ,

The Legendre symbol $(\frac{a}{p})$ is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ if } \gcd(a,p)>1 \\ 1 \text{ if } a \equiv x^2 \pmod{p} \ for \ some \ integer \ x \\ -1 \ otherwise \end{cases}$$

The Legendre symbol can be computed by (1), which was discovered by Euler. This is defined in the form.

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \qquad (1)$$

B. Definition

Two integers a and b leave same remainders when dividing by m ,we say that a **is congruent to** b **modulo** m ,and write $a \equiv b \pmod{m}$ .If the remainders are different, we say that a **and** b **are incongruent modulo** m **,** and write $a \neq b \pmod{m}$.

C. Definition

Let f and g be two functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $O(g(x))$ if there are constants c and k such that $|f(x)| \leq cg(x)$ Whenever $x > k$ .This is read as "$f(x)$ is big-oh of $g(x)$".The constants c and k in the definition of big- O notation are called witness to the relationship $f(x)$ is $O(g(x))$

D. Note

(i) if c and k are one pair of witnesses, then any pair c^1 and k^1, where $c < c^1$ and $k < k^1$, is also a pair of witnesses, since

$|f(x)| \leq cg(x) \leq c^1 g(x)$ whenever $x > k > k^1$.

(ii) when there is one pair of witnesses to the relationship $f(x)$ is $O(g(x))$, there are infinitely many pairs of witnesses.

E. Definition

Let f and g be two functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $\Omega(g(x))$ if there are constants c and k such that $|f(x)| \geq cg(x)$ Whenever $x > k$ .This is read as "$f(x)$ is big-omega of $g(x)$".

F. Definition

Let f and g be two functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $\Theta(g(x))$ if $f(x)$ is $O(g(x))$ and $f(x)$ is $\Omega(g(x))$. When $f(x)$ is $\Theta(g(x))$,we say that "$f(x)$ is big-Theta of $g(x)$".

G. Theorem

$F(n) = \{\, b \in Z/(n)^* : b^{n-1} \equiv 1 (\bmod\ n)\}$ is a subgroup of $Z/(n)^*$.

H. The solovay- strassen test

If n is an odd prime and b is relatively prime to n then

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) (\bmod n) \ implies \ b^{n-1} \equiv \left(\frac{b}{n}\right)^2 \equiv 1 (\bmod n) \ldots (2)$$

The Solovay-strassen test is based on this equation.

Solovay Strassen test :

Input: Two integers n and b such that $\gcd(n,b) = 1$

Step 1: If $b^{(n-1)/2} \neq \left(\frac{b}{n}\right) (\bmod n)$ then return "n is composite" else return "n is a probable Prime ".

Let $E(n)$ denote the set of bases satisfying equation (2)

i.e., $E(n) = \{\, b \in Z/(n)^* : b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) (\bmod n)\}$

$$\because b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) (\bmod n) \Rightarrow b^{n-1} \equiv \left(\frac{b}{n}\right)^2 (\bmod n)$$

I. Corollary

$$\#E(n) \leq \frac{1}{2} \varphi(n) \ for \ all \ odd \ composite \ n.$$

J. Theorem

Let $n > 1$ be odd. Then

$\#E(n) = \delta(n)\prod_{p/n} \gcd(\frac{n-1}{2}, p-1)$ Where

$$\delta(n)=\begin{cases} 2 \ if \ \ v_2(p-1) \geq v_2(n-1) \ \ \forall \ \ p/n \\ \frac{1}{2} \ if \ \exists p/n \ with \ v_2(p-1) < v_2(n-1) \& v_p(n) \ odd \\ 1 \ other \ wise \end{cases}$$

K. Algorithms

Analysis of algorithm means an investigation of an algorithm's efficiency with respect to two resources: running time and memory space. Time efficiency indicates how fast an algorithm in question runs. Space efficiency deals with the extra space the algorithm requires. An algorithm's efficiency as a function of some parameter n indicating the algorithm's input size. The parameter will be the size (length) of the input. Computer scientists prefer measuring size by the number b of bits in the $n's$ binary representation: $b = \lfloor \log_2 n \rfloor + 1.$

This metric usually gives a better idea about efficiency of algorithms. One possible approach is to count the number of times each of the algorithm's operations is executed. This approach is both executively difficult and, as we shall see, usually unnecessary. The thing to do is to identify the most important operation of the algorithm, called the basic operation, the operation contributing the most to the total running time, and compute the number of times the basic operation is executed. Let C_{0p} be the time of execution of an algorithm's basic operation on a particular computer and let $C(n)$ be the number of times this operation needs to be executed for this algorithm. Then we can estimate the running time $T(n)$ of a program implementing this algorithm on that computer by the formula $T(n) \approx C_{0p} C(n)$. The count $C(n)$ does not contain any information about operation that is not basic, and, in fact, the count itself is often computes only approximately. The efficiency analysis framework ignores multiplicative constants and concentrates on the count's order of growth to within a constant multiple for large-size inputs.

III. S-RSA Public Key Cryptosystem

A. The designing of S-RSA Pubic key Cryptosystem

The designing of S-RSA system is based on three aspects: key generation, encryption and decryption like basic RSA system [2],[3]. We describe these aspects as follows and then discuss the performance of the system and analyze its security.

Key generation:

The Key generation algorithm is depended on the spaces: encryption space, Key space and decryption space. In RSA system ,all the spaces: encryption space, Key space and decryption space are equal to $Z/(n)^*$ but in this system encryption space and decryption space are equal to $Z/(n)^*$ like RSA and Key space is a subset $E(n)$ of $Z/(n)^*$ which satisfies the solovay-strassen conditions.

Step 1: The Key generation algorithm takes a security parameter n as input.

Step 2: The algorithm generates two $(n/2)-$ bit primes, p and q ,and sets $n \leftarrow pq$.

Step 3: Next, it picks some small value e that is relatively prime to $\phi(n) = (p-1)(q-1)$, $e^{\left(\frac{n-1}{2}\right)} \equiv \left(\frac{e}{n}\right) (\mathrm{mod}\, n)$. The value e is called the encryption exponent. The public key consists of the two integers (n, e) .

Step 4: The private key is an integer d such that $d^{\left(\frac{n-1}{2}\right)} \equiv \left(\frac{d}{n}\right) (\mathrm{mod}\, n)$ and $e.d \equiv 1 \ (\mathrm{mod}\, \phi(n))$.

Step 5: Typically, one sends the public key (n, e) to a Certificate Authority (CA) to obtain a certificate for it.

Encryption:

Step 1: To encrypt a message X using public key $\langle n, e \rangle$, one first assign X to an integer M in $E(n) = \{ b \in Z/(n)^* : b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) (\mathrm{mod}\, n) \}$.

i.e., $(M, n) = 1$ and $M^{\left(\frac{n-1}{2}\right)} \equiv \left(\frac{M}{n}\right) (\mathrm{mod}\, n)$

Step 2: The ciphertext is then computed as $C \leftarrow M^e \ (\mathrm{mod}\ n)$

Decryption:

Step 1: To decrypt a ciphertext C the receiver uses its private key d to compute a $e'th$ root of C by computing $M \leftarrow C^d \ (\mathrm{mod}\, n)$. Science both d and n are large numbers (each approximately n bits long) this is a lengthy computation for the receiver.

Step 2: The formatting operation from the encryption algorithm is then reversed to obtain the original bit-string X from M .

B. Performance

In this section, we measure the efficiency of the Algorithms in terms of big-θ notation.

The time efficiency of the Key generation is $T(n) = C_{op} C(n)$ where C_{0p} is the unit time for the basic operation and the number of basic operations in this algorithm is $C(n) \approx \frac{\prod(n) \times (\prod(n) - 1)}{2}$ or $C(n) \approx \theta(\prod(n))^2$.

The time efficiency of the encryption algorithm is

$T(e) = C_{op}C(e)$ where C_{0p} is the unit time for the basic operation and the number of basic operations in this algorithm is $C(e) \approx 2(e-1)$ or $C(e) \approx \theta(e)$.

The time efficiency of the decryption algorithm is $T(d) = C_{op}C(d)$ where C_{0p} is the unit time for the basic operation and the number of basic operations in this algorithm is $C(d) \approx 2(d-1)$ or $C(d) \approx \theta(d)$

The time efficiency of this cryptosystem is $T(n,e,d) = C_{0p}C(n,e,d)$ where C_{0p} is the unit time for the basic operation and the number of basic operations is

$$C(n,e,d) \approx \left(\frac{\prod(n)\times(\prod(n)-1)}{2}\right)+\left(2(e-1)\right)+\left(2(d-1)\right)$$

Or

$$C(n,e,d) \approx Max\left(\theta(\prod(n)^2, \theta(e), \theta(d)\right)$$

Note that if $n \approx \prod(n) \approx e \approx d$ then

$$C(n,e,d) \approx \theta(n^2)$$

C. Security

1) Cipher text only attack:

If the public key (e, N) is known then the attacker decrypt the cipher text as follows: Let $C_i, C_j \quad for\ i \neq j$ be the any two cipher text letters(values). Suppose $A \leftarrow \left(C_i^e \bullet C_j\right)$.

Now consider

$$A^{1/e} \leftarrow \left(C_1^e \bullet C_2\right)^{1/e} \qquad \Leftrightarrow C_j^{1/e} = \frac{A^{1/e}}{C_i}$$

$$\Leftrightarrow M_j = C_j^{1/e} = \frac{A^{1/e}}{C_i}$$

Similarly we obtain $M_i = C_i^{1/e} = \frac{A^{1/e}}{C_j}$.

Here we observed that, the cipher text only attack is not useful to decrypt the cipher text with out decryption key.

2) Known-plaintext attack:

Let $(C_1, M_1), (C_2, M_2), ...(C_k, M_k)$ be the known cipher text and plain text pairs. Let $C_i, C_j \quad for\ 1 \le i \neq j \le k$ be the any two cipher text letters (values)

Suppose $A \leftarrow \left(C_i^e \bullet C_j\right)$.

Now,

consider $A^{1/e} \leftarrow \left(C_1^e \bullet C_2\right)^{1/e} \qquad \Leftrightarrow C_j^{1/e} = \frac{A^{1/e}}{C_i}$

$$\Leftrightarrow M_j = C_j^{1/e} = \frac{A^{1/e}}{C_i} \Leftrightarrow A^{1/e} = M_j \bullet C_i.$$

Similarly we obtain $M_i = C_i^{1/e} = \frac{A^{1/e}}{C_j}$

Here we observed that, the known-plaintext attack is useful to decrypt the cipher text with out decryption key.

3) Chosen-plaintext attack:

This attack is useful to decrypt the cipher text with out decryption key if the key space is known to the attacker. The probability for decrypting the cipher text approximately is $\ge \frac{1}{|S_k|}$ where the S_k is the key space.

4) Chosen-cipher text attack:

This attack is useful to decrypt the cipher text with out decryption key if the key space is known to the attacker. The probability for decrypting the cipher text approximately is $\ge \frac{1}{|S_k|}$ where the S_k is the key space.

Note that the security of this cryptosystem depends on the factorization of N like in RSA system.

IV. Theoretical And Graphical Comparison Of An Efficiency

In RSA cryptosystem, $e \bullet d \equiv 1(\text{mod } \phi(n))$ $\Rightarrow e \bullet d = k\phi(n)+1$ where, there exist k is an integer.

In S-RSA cryptosystem, $e \bullet d \equiv 1(\text{mod } \phi(n))$ $\Rightarrow e \bullet d = k\phi(n)+1$ where, there exist k is an integer and $e \bullet d \equiv 1\left(\text{mod}\left(\frac{n-1}{2}\right)\right) \Rightarrow e \bullet d = k^1\left(\frac{n-1}{2}\right)+1$ where, there exist k^1 is an integer. According to Number theory, $\left(\frac{n-1}{2}\right) < \phi(n)$ for all $n = p.q$ where $p \neq 2, q \neq 2$ and $2\left(\frac{n-1}{2}\right) \ge \phi(n)$. So, the constants k and k^1 are related such that $k \approx 2k^1$. In RSA cryptosystem: the number of binary operations are used in encryption is $2(e-1)$ ($(e-1)$ multiplications and $(e-1)$ modulo operations) and the number of binary operations are used in decryption is $2(d-1)$ ($(d-1)$ multiplications and $(d-1)$ modulo operations). Thus the total number of binary operations in RSA cryptosystem is $2(e-1)+2(d-1)$. Similarly, in S-RSA cryptosystem the total number of binary operations are $\left(\frac{2(e-1)+2(d-1)}{2}\right)$. Thus, the performance of S-RSA cryptosystem is nearly two times the performance of RSA cryptosystem.

1) Illustration for graphical explanation.

Consider the set of primes which are less than 50 not including 2 is

$$S = \{3,5,7,11,13,17,19,23,29,31,37,41,43,47\}$$

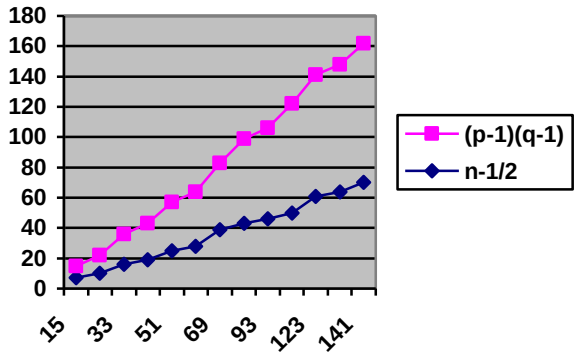

Fig.1

The X-axis indicates the value of the product of odd primes and Y-axis indicates the vales of $\phi(n)$ as well as $n-1/2$. Thus, the performance of the RSA crypto system is lesser (more than two times) than that of S-RSA cryptosystem.

It is noticed that it has a weak security since if n is known than every one can easily find $\left(\frac{n-1}{2}\right)$ value and then find private key d easily by using it's public key (n,e).

V. Summary And Conclusion

In this article, it is shown how the solovay-strassen test used instead of Euler theorem in RSA cryptosystem and mesure the efficiency interms of big- θ notation instead of big- O notation for the best approximate value .In this article, it is also shown the comparison between the efficiency of the RSA and the S-RSA cryptosystem. It is also explained about the four possible important basic attacks on the S-RSA cryptosystem.

References

[1] A.Fait, "Batch RSA, Advances in cryptology", proceedings of crypto'89, vol.435 of LNCS,pp.175-185, Springer-Verlag 1989.
[2] A. Menezes, P.Van Oorschot, and S.Vanstone, "Handbook of Applied Cryptography". CRC Press, 1997.
[3] D.Boneh and H. Shacham, " Fast variants of RSA",.RSA Laboratories,2002.
[4] D.E.G.Malm, " On Monte-Carlo primality tests" , Notices Amer. Math.Soc., pages A- 529,1977.
[5] D.H. Lehmer, "On Euler's totient function" Bull. Amer. Math. Soc. , 38 (1932), pp. 745–751.
[6] D.J.Newmann, "Simple analytic proof of the prime number theorem", American Math.Monthly, PP:693-696,1980.
[7] H.Cohen, "A Course in Computational Algebraic Number Theory", vol 138 of Graduate Texts in Mathematics, Springer-Verlag,1996.
[8] H.Riele, K.Aardal, J.Gilchrist," Factorization of a 512-Bit RSA Modulus", Proceedings of Eurocrypt'2000,vol.1807 of Lecture Notes in Computer Science (LNCS),pp.1-11,Springer-Verlag,2000.

`

Dr.L.Sreenivasulu Reddy, presently working as Teaching Assistant in the Department of Mathematics at Sri Venkateswara University, Tirupati, Andra Pradesh, India. He was born on 10th Jun 1983 at Kadapa in Andra Pradesh. He completed his Graduation and Post graduation in Mathematics at Sri Venkateswara University, Tirupati . He got Ph.D from Sri Venkateswara University in the discipline of Mathematics in the year of 2009. He is well versed scholar in cryptography which is one of the thirst areas of Mathematics. He has been paying attention on Cryptography, Coding theory, Boolean algebra, Ring theory and Graph theory .His specializations are Cryptography, Ring theory and Graph theory. He has been trying to apply interrelationships between Cryptography and Algebraic Number theory, Semi ring theory and Boolean algebra, Cayley Graphs and Arithmetic Graphs. He participated and presented papers in the area of cryptography, Graph theory and Semi ring theory in various international and national conferences.

Dr.K.Ramakrishna Prasad has been working as Professor in, Department of Mathematics at Sri Venkateswara University, Tirupati , Andra Pradesh ,India.He was born in the year 1954 at Ongole in Andra Pradesh. He did his Ph.D at I.I.T Kanpur in 1979. Worked as Lecturer at NBKRIS, Vidyanagar, Nellore, A.P during 1979-1988, worked as Reader at S.V.U Engineering College, Tirupati during 1989-1995 and became as Professor of Mathematics from 1996 at S.V.Uinversity. He worked as co-coordinator of Engineering Mathematics for 5 years and again worked as Head of the Department of Mathematics during 2005-2007. Presently ,he is Chairman of Board of Studies in the Department of Mathematics. He has published 25 research papers in various international and national journals and attended 20 international and national conferences. He is interested in the areas of Hydrodynamics, Lubrications, Bio-informatics, Cryptography, Mathematical Modeling .

Dr. N.Ch.S.N.Iyengar is a Senior Professor at the School Of Computing Sciences at VIT University, Vellore, Tamilnadu India. He received M.Sc (Applied Mathematics) & PhD from Regional Engineering College Warangal (Presently known as NIT Warangal).Kakatiya University, Andhra Pradesh, India, & M.E. (Computer Science and Engineering) from Anna University, Chennai, India. His research interests include Fluid Dynamics (Porus Media), Agent based E- Business Applications, Data Privacy, Image Cryptography, Information security, Mobile Commerce and cryptography. He has authored several textbooks and had research Publications in National , International Journals & Conferences. He is also Editorial Board member for many National and International Journals. He chaired many International conferences' and delivered invited , technical lectures along with keynote addresses beside being International programme committee member.

Dr.V. Ramachandran, presently Vice–Chancellor of Anna University, Trichy (T.N). He served as Professor in the Department of Computer Science at the College of Engineering, Anna University, India. He received his ME and PhD Degrees from Anna University, India in 1982 and 1991, with specialisation in Power Systems. He served as visiting professor in several national and international institutes. He has authored several research publications. He chaired many International conferences' and delivered invited technical lectures along with keynote addresses .His research interests include power systems analysis in distributed environment, networks and web technologies. He is serving as an editorial member of many international and national journals. al hobbies will be deleted from the biography.