Research Journal of Applied Sciences 11 (10): 1050-1053, 2016
ISSN: 1815-932X

Building the Primes P&Q (Of the Public Key Algorithm) by Using Function of Reals

Faez Al_Mamory, Ameer Kadhim Hadi and Ahmed AL-Salih
Department of Information Networks, University of Babylon, Babylon, Iraq

Abstract: Public key algorithm is a famous method for encryption which depends on the way of selecting the prime p and q to be secure enough. This study addresses a new generation of the primes p and q from reals using generating function of reals $\vartheta(x)$. Here, we don't need to think about getting primes p and q and how they are secure enough. The reason for this is the complicated function $\vartheta(x)$ generates these primes under such conditions. This is clearly addressed in the main body of this study. Moreover this study provided a construction in building any prime p.q from a real number x. This opened a new window for building security algorithm of the public key.

Key words: Public key algorithm, analytic number theory, primes, main body, security

INTRODUCTION

During 1978, several authors (such as Adi Shamir and Leonard Adleman) introduced a cryptographic algorithm in order to replace the less secure NBS algorithm, (i.e. to replace the National Bureau of Standards algorithm).Here, a public-key cryptosystems (as well as digital signatures) are regarded as The important things for the RSA implements, for instance Salomaa (2013), Duan (2014), Van-Dijk *et al*. (2010), Galbraith (2012) and Brakerski and Segev (2015). Many people think that the Public key algorithm is related to the research have been don for the authors " Di?e and Hellman" who described the idea of such an algorithm but never truly developed it. The RSA algorithm concentrated on the following important thing which is called the "Public-key encryption". Here the main goal of the first one is to omit the use of the courier in order to deliver keys to the receiver over another secure channel before transmitting the originally intended information or message. It's clear that the person with the correct decryption key can decipher an encrypted message and the reason for that is in the RSA algorithm the encryption keys are public but the decryption keys are not. The more important thing here is that the keys should be built in such a way that the decryption key may not be easily deduced from the public encryption key. It's obvious that the public key algorithm is beneficial and useful for several usage such as the electronic mail, electronic transactions and transmissions (Qin and Liu, 2014; Qin *et al*., 2003). The main part of the public key algorithm is the security. The public key algorithm has so far been validated. The reason for that is there is no known attempts to break it have yet been successful. The difficulty of factoring large number $s^n = pq$ where p and q are large prime numbers enable the public key algorithm to be secure. In this study we build the prime number p by using a mathematical technique of some number theory function of reals called $\vartheta(x)$. On the other word here the job of the function $\vartheta(x)$ for real number x) is to find the prime P. Knowing P leads to determine the prime q. Getting P and θ by using $\vartheta(x)$ (i.e, getting n = pq) gives a stronger line of security to the public key algorithm. The function $\vartheta(x)$ is so complicated function which generate the prime P from the real x under such conditions. These conditions with some applicable examples addressed in pp234 of the article.

MATERIALS AND METHODS

The $\vartheta(x)$ The generating function We define the sequence of the actual primes as and the sequence of $p = \{pk\}_{k=1}^{\infty} = \{2, 3, 5, 7, ...\}$ natural number to be:

$$p = \{N_k\}_{k=1}^{\infty} = \{1,2,3,4,5,6,7...\}$$

The following definitions of some counting functions are needed for our purpose.

Definition 2.1 : Let ? be the set of the actual primes. The counting function for any positive real x is defined to be $p \in p$ and$^k \in N$ where:

Corresponding Author: Faez Al_Mamory, University of Babylon, Department of Information Networks, Babylon, Iraq

$$\Psi(x) = \sum_{p^k \le x} \log p$$

as follows: Ψ (x) We can write:

$$\Psi(x)\sum_{k=1}^{\infty}\sum_{p\le x^{\frac{1}{k}}} \log p = \sum_{k=1}^{\infty}\vartheta\left(x^{\frac{1}{k}}\right)$$

(Apostol, 1976) for more $\vartheta(x) = \sum_{p\le x}\log p$ details). Where.

Now using the Mobius Inversion Formula we get:

$$\vartheta(x) = \sum_{n=1}^{\infty}\mu(n)\Psi\left(x^{\frac{1}{n}}\right)$$

we Ψ (x) = [x] - 1, function. Let mabius. Where (n) is:

$$\vartheta(x) = \sum_{n=1}^{\infty}\mu(n)\left(\left[x^{\frac{1}{n}}\right]-1\right)$$

Here, if you look carefully you would see that the n>log^x/log^{2}get function (x) is vanish for. In order to build q and p Our aim is to select the primes and in order to build a strong public key algorithm. In fact we do not select must be ax such that x them we select the real number that p gives the prime ϑ (x) large real number such that is ϑ (x), we are looking for. must be a large real number such that ϑ (x) we are looking for. So, firstly we shall show that increasing function. This is really important part. The x reason for this since we need for any large number (Apostol, 1974)). The ϑ (x) by x related to p there is a prime number goes to infinity the primes must goes to x So, when infinity as well. Other wise the work for the public key algorithm will be useless. The following theorem shows goes to infinity.^{x} is increasing function as ϑ (x) that.

Theorem 2.1: Suppose:

$$\vartheta(x) = \sum_{n=1}^{\infty}\mu(n)\left(\left[x^{\frac{1}{n}}\right]-1\right)$$

Then for, i.e:

$$\vartheta(x) = \vartheta(q) q \le x < q+1, q \in N,).\vartheta(x) = \vartheta([x])$$

Proof:

$$\vartheta(x) - \vartheta(q)\sum_{n=1}^{\infty}\mu(n)\left(\left[x^{\frac{1}{n}}\right]-\left[q^{\frac{1}{n}}\right]\right)$$

So, by showing +1 we will have completed $[1/q^{1/n}] \le x^{1/n} \le [1/q^{1/n}]$ the proof of the theorem since the above sum will equal zero. We have. Therefore, it's clear $q^{1/n} \le x^{1/n} \le (q+1)^{1/n}$ that It remains to show that $[x^{1/n}] \ge x^{1/n} \ge [[k]^{1/n}]$. Assume that $x^{1/n} \ge [[k]^{1/n}$. One n, q$\in$N for some $x^{1/n} \ge [[q]^{1/n}$ can easily show that this will leads to a contradiction by the condition of the integer numbers. This will complete the proof of the theorem ,let r,q $\in$ N.

Theorem 2.2 : For any. Then:

$$h(r,q) = \begin{cases} 1 \text{if } q = u^r \text{ forsmeuin N,} \\ 0 \text{if } q \ne u^r \text{ foranyuin N,} \end{cases}$$

Proof:

we have r,q $\in$ N For any.

Now we $\left[q^1\left(1/r\right)\right] \ge \left[(\sqcap q-1)\sqcap^1\left(1/r\right)\right)] \ge 0$ is either zero or one. That is, it h (r,q) show firstly that remains to show that:

$$\left[q^{(1/r)}\right] - \left[(q-1)^{(1/r)}\right] \le 1$$

we have r,q $\in$ N So, suppose for some:

$$\left[q^1\left(1/r\right)\right] \ge 1 + \left[\left(\sqcap_q - 1\right)\sqcap^1\left(1/r\right)\right)\right]$$

then our assumption $g = \left[([q-1])^{\frac{1}{r}}\right]$, If we assume tells us that:

$$q^{\frac{1}{r}} \ge \left[q^{\frac{1}{r}}\right] > 1 + g \to q > (g+1)^r, \ldots\ldots(*)$$

which tells us that $g \le [(q-1)^{\frac{1}{r}}]$. Clearly This is a contradiction with (*). Hence, $q \le [(g+1)^{\frac{1}{r}}]$.

$$0 \le \left[q^{\frac{1}{r}}\right] - \left[\left([q-1]\right)^{\frac{1}{r}}\right] \le 1$$

either zero or one and the reason h(r, q) This show that are both integers. Now, $[(q-1)^{1/r}]$ and $[q^{1/r}]$ for that is This $[q^{1/r}]$ = u. ,then u $\in$ N , for some q = u^r for inform us that.

Therefore, $[(q-1)^{1/r}] = [(u^r-1)^{1/r}] < u$. The h (r,q) = 1 if q = u^r, for some u $\in$ N. is either zero or one.h (r,q) we have proved that , for some q = u^r Moreover, when. U $\in$ N, h (r,q) = 1.

for any u ∈ N , q ≠ u^r Finally, for contradiction if and by following some h (r, q) = 1 assume that must be zero if h (r,q) calculation one can find that , for any u ∈ NN (we leave this for the reader). q ≠u^r This complete the proof of the theorem is q.

Note: It's obvious that for the particular case when is a perfect power we have that:

$$h(r,u^v)=\begin{Bmatrix}1\text{if r divides,}\\0\ \text{otherwise.}\end{Bmatrix}$$

a perfect power if there q ∈ N

Theorem 2.3: We call such that q = r > 1 and u > 1, exist natural numbers . Then q^r

$$\vartheta(q)-\vartheta(q-1)=\begin{Bmatrix}1\text{if q is not a perfect power } q\geq 2\\0\ \text{if } q\neq u^r \text{ for any u in N.}\end{Bmatrix}$$

Proof:
From Theorem 2.2 we have:

$$h(r,q)=\begin{Bmatrix}1\text{if } q=u^r \text{ for sme u in N.}\\0\text{if } q\neq u^r \text{ for any u in N.}\end{Bmatrix}$$

is not a perfect power, we have q Therefore, for

$$\vartheta(q)-\vartheta(q-1)=\sum_{n=1}^{\infty}\mu(n)h(r,q)=1+\sum_{n=2}^{\infty}\mu(n)h(r,q)=1$$

be a maximal ^v is a perfect power let q. Now, for q = u ^v natural number greater than or equal 2 such that So, by the above Note we have, q > 1,q ∈ N:

$$\vartheta(q)-\vartheta(q-1)=\vartheta(u^v)-\vartheta(u^v-1)$$
$$=\sum_{n=1}^{\infty}\mu(n)h(n,u^v)=\sum_{\frac{n}{v}}\mu(n)$$

By Theorem 2.1 of (Apostol, 1976) we have the last sum is zero This is the end of the theorem ^v > 1 (since).
from the real number, so the p Our aim is to get a prime following definition will end the job.
define the step ^x.

Corollary 2.4: For any real number where the $\hat{\vartheta}(x)$ = $(\theta(x))^{\vartheta(x)}$ as follows: $\hat{\vartheta}(x)$ function characteristic function

$$\gamma\theta(x)=\begin{Bmatrix}1\text{if } \vartheta(x)=u.v \text{ for any } u,v>1 \text{ in N.}\\0\text{ if q is a perfect power}\end{Bmatrix}$$

is either zero or prime $\hat{\vartheta}(x)$ Therefore the step function number From the mathematical technique we have done, if we are in some interval P looking for getting a prime number $\hat{\vartheta}(x)$ = P,. then if $^{X\in(A,B)}$ Let (a,b). a,b ∈ R .

Otherwise we replace q then we move to find the prime by In order to find the p. till get the prime $^{x+1}$ by $^{x}x^{2}$ other prime q we could substitute the real number (for instant) and follow the same steps as in finding the p. previous prime

Algorithm (1)generating p and q:
Input: x as big enough real number.
Output: p and q prime numbers.
Begin:
Set thetat_x _ 0; Set n_ 1.
While n<=LOG(1/x)/LOG(1/2)
Theta_x_=Theta_x+(Mu(n)*(x power(1/n)-1))
Increment n by 1
End while
p=Theta_x
q=greatest prime number larger than p
End algorithm

Algorithm function Mu:
Input: n as a real number
Output: -1 or 0 or 1
Begin:
If n= 1 then returned value of Mu is 1
ElseIf is a prime then returned value of Mu is 1
ElseIf n =p^a then returned value of Mu is zero
Else
Make factorize n to be as a^b *b^c and return value of Mu(a^b)*Mu(b^c) //recursive
End Mu Algorithm

RESULTS AND DISCUSSION

Other efforts could be added to this research to provide other goals in the future. It possible to add other parameters to the main work on θ(x) to be more secure and irreversible specially the application has a host on the cloud computing which provide high performance. Moreover, the authored planned to develop the algorithm in effect ways to be more suitable for integration with web service ,web 2.0 serves and all cloud computing facilities, for instance, Persis Urbana and Yitao.

CONCLUSION

This is clearly addressed in the main body of this study. Moreover this study provided a construction in building any prime p.q from a real number x. This opened a new window for building security algorithm of the public key.

ACKNOWLEDGMENTS

This research was partially supported by Network department college of IT University of Babylon. We are grateful to our colleagues who provided expertise that greatly assisted the research, although they may not come

to an agreement with the writing style provided in this study. We have to express our thanks to CISCO center for membership their treasures of knowledge and tools with us during the course of this study. We are also immensely grateful to academic writing and research student center in IT college for their comments on an earlier styles of the manuscript, although any errors are our own and should not tarnish the standings of these respected sides.

REFERENCES

Apostol, T.M., 1974. Mathematical Analysis. 2nd Edn., Wesley, Addison, Texas, .

Apostol, T.M., 1976. Introduction to Analytic Number Theory, Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg.

Brakerski, Z. and G. Segev, 2015. Function-Private Functional Encryption in the Private-Key Setting. In: Theory of Cryptography, Yevgeniy, D. and J.B. Nielsen (Eds.). Springer, Berlin, Germany, ISBN:978-3-662-46496-0, pp: 306-324.

Duan, Y., 2014. Distributed key generation for encrypted deduplication: Achieving the strongest privacy. Proceedings of the 6th ACM Workshop on Cloud Computing Security, November 3-7, 2014, ACM, Scottsdale, Arizona, ISBN:978-1-4503-3239-2, pp: 57-68.

Galbraith, S.D., 2012. Mathematics of Public Key Cryptography. Cambridge University Press, Cambridge, England, UK., ISBN:978-1-107-01392-6, Pages: 616.

Qin, B. and S. Liu, 2014. Leakage-flexible CCA-secure public-key encryption: Simple construction and free of pairing. Proceedings of the International Workshop on Public Key Cryptography, March 26-28, 2014, Springer, Berlin, Germany, ISBN: 978-3-642-54630-3, pp: 19-36.

Qin, B., S. Liu, K. Chen and M. Charlemagne, 2013. Leakage-resilient lossy trapdoor functions and public-key encryption. Proceedings of the first ACM Workshop on Asia Public-Key Cryptography, May 8-10, 2013, ACM, Hangzhou, China, ISBN: 978-1-4503-2069-6, pp: 3-12.

Salomaa, A., 2013. Public-Key Cryptography. 2nd Edn., Springer, Berlin, Germany, ISBN:978-3-662-03269-5, Pages: 274.

Van-Dijk, M., C. Gentry, S. Halevi and V. Vaikuntanathan, 2010. Fully Homomorphic Encryption Over the Integers. In: Lecture Notes in Computer Science, Rabin, T. (Ed.). Springer Verlag, France, PP: 24-43.