ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

ANALYZING THE STRENGTH OF PELL'S RSA

Chandrasegar T[1], Senthilkumar M[1], R.Silambarasan[2], Carlos Becker Westphall [3]
[1]Assistant Professor (Senior), SITE school, VIT University, India
[2]M.Tech Student ,SITE School, VIT University, Vellore, India.
[3]Professor, Federal University of Santa Catarina, Departamento de Informática e Estatística Florianópolis, Santa Catarina, Brazil.
Email: mosenkum@gmail.com

Received on: 18.10.2016 *Accepted on: 11.11.2016*

Abstract

By taking two distinct Diophantine equations with distinct large prime numbers and two different co-ordinates, two secret keys are generated at the same time so that two users can encrypt their messages / plaintext. Hence two sets of public key exponents with one set of private key exponents were the result of proposed algorithm.

Keywords: Pell's equation, Diophantine equation, Public key cryptosystem.

Introduction

The traditional RSA asymmetric key cryptographic system dates to be first in the public key cryptography comprising public key creation, encrypting original message, private key generation and decrypting the encrypted message. In this system the selection of prime numbers pairs larger and larger ensures the strong protection to cipher text from the third parties in cracking back to original plaintext with means of different attacking schemes in the existing literature including continued fraction method private key retrieval, Euclidean and extended Euclidean division algorithm method of tracking private key are some with few. Continued fraction constraint of private key value less than that of modular value to the power constant is admissible only when the two distinct prime numbers are limited to certain bit length. When this bit length increased the retrieval process with continued fraction method would lead to longer time for computing. Same scenario holds true for extended Euclidean division method as well. Next with RSA cryptography method only one user can make encryption (or) in other lines, user's single message only able to encrypt at the time. Albeit holds this fine as far as the asymmetric key cryptography, the time and cost computing raised the issue which tended further study in this regime. As an instance either of public key generation (or) private key generation cost only

can be made less also in time, by making large variations to one another. There hence give rise the study of re-balanced RSA where encryption key and decryption key are balanced with respect to the aspects of time and cost followed by the Chinese Remainder Theorem method of private key tracing from RSA and led to RSA-CRT Likewise in the different direction first method of dual key generation by taking small public key exponent at one time and small private key exponent on the other led to Dual RSA key generation where the results are provisioned with Lattice based breaking system and analyzed to re-balanced RSA and RSA-CRT. The similar kind of producing two public keys by the simple linear equations such as Diophantine equation what under influence called Pell's equation is explained in this work. This algorithm does not four sets of equations and two sets of co-ordinates system as in Dual RSA. Rather by simply taking two Diophantine equations the two sets of secret keys are produced thence two users at a time can encrypt their message. The proposed algorithm is proved with the help of numerical example calculations.

Literature Survey

In [1] taking four straight lines (linear equations) with two co-ordinates are comprised to give four set of prime numbers name yp 1 ;q 1 ;p 2 ;q 2 and iterated until q 2 satisfies for the prime numbers albeit other three too need to be prime. From these four prime numbers where x0 sandy 0s are chosen in such a way that two instances of public and private keys were the result. Exactness of the key generation in either case were verified through Dual RSA equations form its key. In [2] trailing the method of Euclidean algorithm, modified trial division method is employed in the private key generation which back from the known modulus value and public key as prime numbers be-come larger extent this method helped in encrypting digital data's.

In [3] the encryption key generation is explained in the means of prime pairs selected for Euler's totient function calculation followed by system modulus computation. This leads to public key generation study in terms of prime numbers and primitive roots. In [4] Knapsack problem with Merkle-Hellman number theoretic concepts are employed in public key exponent calculation and showed the hardness of breaking back of private key. Defined their strong ability of scheme against various known attacks including brute force. In[5] Prime number selection procedure in public key from modulus of system and totient function of Euler computation are further extended and studied and proved the proposed system secure against Shamir attacks. In [6] library function in C++ comprising encryption key generation and groupware technique in encapsulation method described in encrypting and decrypting files stored in windows platform.

In [7] n carry array is used in the calculation of public key when the prime numbers are larger and proved the efficiency in digital signature along with class lib in C++ were given. In [8] Pell's equation first introduced in RSA cryptography in key generation and management by fixing threshold value and proved there scheme is strong against coalition attack.

In [9] secret key generation from Pell's equation by taking the roots of Diophantine equation for the constant prime is proposed and analyzed its complexity with N-prime RSA, Dual RSA dn traditional RSA. Crypt analysis of Fermat's attack, Weiner's continued fraction and extended Euclidean method were compared along with numerical examples. In thick communication, two Diophantine equations are taken at a time and showed two secret key sets along with private key exponent set. Proposed system/ algorithm makes two different users to encrypt their messages and send while receiver receives two cipher texts and decrypt to original text with single private key set, thus the proposed scheme makes the communication to one receiver to two senders at a time. While in other go, the sender can encrypt their two different messages with two secret keys and communicate with receiver and receiver performs as explained earlier. The proposed algorithm is explained with numerical example to prove its efficiency.

Proposed Work

Prof Pell studied the Diophantine equation of the form y2 dx 2 = 1. For the given positive values d the x and y values should be found which satisfying the governing equation. One such solution is ford= 61, x and y has values respectively2261590and1776319041.In this work the secret key generation is based on the above mentioned Diophantine but he d values are chosen as prime number in due course positive prime integers. The proposed algorithm takes two Diophantine equations and followed by selection of two distinct prime integers for d and then values of x0s and y0s which satisfying Pell's equation. Detailed proposed system is given in algorithm 1.

Algorithm 1 Extended Pell's RSA key generation algorithm

1. Two large prime numbers P and Q are chosen.
2. Find two positive integers X_1 and Y_1 which satisfying Diophantine equation $Y_1^2 - PX_1^2 = 1$.
3. Find two positive integers X_2 and Y_2 which satisfying Diophantine equation $Y_2^2 - QX_2^2 = 1$.
4. Again select two large distinct prime number a and b, then calculate $N = a \times b$ and $\phi(N) = (a - 1) \times (b - 1)$.
5. Select e in $[1, \phi(N)]$ and $(GCD)(e, \phi(N)) = 1$.
6. Compute

$$\begin{aligned} \alpha_1 &= [Y_1 + \phi(N)]^2 - P[X_1 + e]^2 \\ &= Y_1^2 + (\phi(N))^2 + 2Y_1\phi(N) \\ &- P(X_1^2 + e^2 + 2X_1e) \\ &= Y_1^2 - PX_1^2 + (\phi(N))^2 \\ &+ 2Y_1\phi(N) - Pe^2 - 2PX_1e \\ &= 1 - Pe^2 - 2PX_1e. \end{aligned} \quad (1)$$

7. Compute

$$\begin{aligned} \alpha_2 &= [Y_2 + \phi(N)]^2 - Q[X_2 + e]^2 \\ &= Y_2^2 + (\phi(N))^2 + 2Y_2\phi(N) \\ &- Q(X_2^2 + e^2 + 2X_2e) \\ &= Y_2^2 - PX_2^2 + (\phi(N))^2 \\ &+ 2Y_2\phi(N) - Qe^2 - 2QX_2e \\ &= 1 - Qe^2 - 2QX_2e. \end{aligned} \quad (2)$$

8. Then

$$\alpha_1 + Pe^2 + 2PX_1e \equiv 1 \bmod \phi(N). \quad (3)$$
$$\alpha_2 + Qe^2 + 2QX_2e \equiv 1 \bmod \phi(N). \quad (4)$$

9. Find d such that $d \equiv e^{-1} \bmod \phi(N)$ and $d \in [0, N]$.
10. Calculate

$$s_1 = \alpha_1 d^3 + Pd + 2PX_1d^2 \equiv d^3 \bmod \phi(N). \quad (5)$$
$$s_2 = \alpha_2 d^3 + Qd + 2QX_2d^2 \equiv d^3 \bmod \phi(N). \quad (6)$$

11. For the plaintext M in $(0, N-1)$, Calculate the cipher text as,

$$C_1 = M^{s_1} \bmod N.$$
$$C_2 = M^{s_2} \bmod N. \quad (7)$$

12. Retrive the plaintext as,

$$M = C_1^{e^3} \bmod N.$$
$$M = C_2^{e^3} \bmod N. \quad (8)$$

Therefore output of algorithm 1 produces two set of public keys are obtained namely(1;d;P;X1;N)and(2;d;Q;X2;N) with the private key(e3;N).Continuing in same way Dual RSA is further expanded to generate one more pair set of instance in key, the following algorithm variant to Dual RSA is proposed and takes the following form

Algorithm 2 Variant of Dual RSA key generation

1. Select two random positive integers x_1, x_2 different from each other to compute $p_1 = x_1x_2+1$ which is prime.
2. Select integer y_2 so that $p_2 = x_1y_2+1$ gives prime number.
3. In same manner y_1 is chose which gives $p_3 = x_1y_1 + 1$ as prime.
4. $q_1 = y_1y_2 + 1$ is calculated for prime number.
5. Public key e is selected satisfying GCD$(e, x_1x_2y_1y_2) = 1$ and private key satisfying $ed = 1 + k_1(p_1 - 1)(q_1 - 1)$.
6. Next compute $q_2 = k_1x_2 + 1$ is prime.
7. Similarly $q_3 = k_1x_1 + 1$ is prime.

Hence the output of algorithm 2 is(e;N1 =p 1 q 1 ;n 2 = p 2 q 2 ;n 3 = p 3 q 3) and (d;p1;q1;p2;q2;p3;q3). Also it was found that algorithm 2 satisfies the three simultaneous equation so called key equations for variation of Dual RSA key generation.

Numerical Examples

Proposed system algorithm 1 is verified by taking numerical examples such as with respect to first Diophantine equation when P = 7the prime number the values satisfying are X1= 3and Y1= 8. For the second Diophantine equation when prime number Q= 11satisfies for X2= 3and Y2= 10where the first three steps are cover. From step 4 of algorithm 1 taking a = 13and b = 17givesN = 221and -(N) = 192. From step 5 the e value is taken as e= 5. From Eqs (1) and (2) of algorithm 1 calculations yields 1= 39552and 2= 40100 which satisfies Eqs (3) and (4) respectively. From step 9 the d values found to be d= 77. From Eqs (5) and (6) values of s1 and s2 are calculated and yielding s1= 149and s2 = 149. Considering the plaintext M= 19, step11 gives the cipher text C= 15and in turn step 12 retracts original message M= 19from Eqs (7) and (8) respectively. Therefore two set of public keys are (39552;77;7;3;221) and (40100;77;11;3;221). Along with the private key set(53;221).Example of proposed algorithm 2 takes, for x1= 20 and x2= 9if step 1 of algorithm 2 gives p1 =181 which is prime number. For y2 = 12 is step 2 yields p2= 241which is prime. For y1= 8 in step 3 gives p3 = 73which is prime. From step 4 q1= 97which is prime number. Step 5 takes e = 7and d = 12343where k1= 2is taken satisfying step 5. Then from steps 6 and 7 the values are q2= 19and q3= 41both are prime. Therefore output of algorithm 2 is (7;17557;4579;2993) and (12343;181;97;241;19;73;41). From this example it can be verified that three key equations are satisfied with above values similar to that of Dual RSA two key equations.

Conclusion

Upon this communication two algorithms are pro-posed in key generating scheme for RSA crypto-graphic system. While the Pell's RSA key generation produces single pair of key, an variant in aspects of two sets production in key generation by considering two distinct Pell's equations the strength is further improved to one step. Presented numerical example proves the efficiency of designed system also makes two users to encrypt their data. It can be further expanded by considering simultaneous Pell's system of equations in key generating where n users able to cipher their data concurrently.

Alternate to the Dual RSA scheme of key generation, further k values were considered and designed the so called trivial RSA one step ahead to Dual RSA where three instances of RSA are generated which improves the security than that of Dual RSA. In the pipeline working of variant of Dual RSA the trivial RSA algorithm 2 is explained and proved with numerical example. Also believed which can be further developed by taking n number of k 0 s and hence multiple instances of RSA well be deployed as algorithm 2.

References

1. H.-M. Sun, Mu-En. Wu, W-C. Tang and M. J. Hinek. ”Dual RSA and its security analysis.”IEEE Trans. Inf. Theory. Vol. 33,No. 8, pp 2922-2933, 2007.
2. Palchaudhury. Modified Trail division for Implementation ofRSA Algorithm with Large Integers Int. J. Advanced Network-ing and Applications Volume: 01, Issue: 04, Pages: 210-216 , 2009
3. Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma Modified RSA Encryption Algorithm (MREA) pgno: 426-429advance Advanced Computing & Communication Technolo-gies (ACCT), 2012, ISBN: 978-1-4673-0471-9
4. Sonal Sharma, Prashant Sharma, Ravi Shankar Dhakar, RSAAlgorithm Using Modified Subset Sum Cryptosystem Pgno:457-461, Computer and Communication Technology (ICCCT),2011, ISBN: 978-1-4577- 1385-9
5. H. C. WILLIAMS, A Modification of the RSA Public-Key Encryption Procedure pgno: 726-729, IEEE transaction on In-formation Theory.
6. Suli Wang, Ganlai Liu, File encryption and decryption system based on RSA algorithm pgno: 797-800, Computational and Information Sciences (ICCIS), 2011 , ISBN: 978-1-4577-1540-2.
7. Ying-yu Cao, Chong Fu, An Efficient Implementation of RSA Digital Signature Algorithm, pgno: 100-103, Intelligent Computation Technology and Automation (ICICTA), 2008,ISBN:978-0-7695-3357-5
8. Sarma, K.V.S.S.R.; Kumar, G.S.K.; Avadhani, P.S., Threshold cryptosystem using Pells equation,pgno: 413-416, Information Technology: New Generations (ITNG), 2011, ISBN: 978-1-61284-427-5.
9. Chandra Segar. T and Vijayaragavan. R.”Pell’s RSA key gener-ation and its security analysis.” Int conference of Computing, Communications and Networking Technologies (ICCNT), pp 1-5, 2013.