International Journal Of Information System & Technology
Vol. 1, No. 1, (2017), pp. 1-7

Generating Mersenne Prime Number Using Rabin Miller Primality Probability Test to Get Big Prime Number in RSA Cryptography

Dicky Apdillah[1], Muhammad Khoiruddin Harahap[2], Nurul Khairina[3]
[1]AMIK INTeL Com GLOBAL INDO
[2]Politeknik Ganesha Medan
[3]Politeknik Ganesha Medan
[1]dicky@nusa.net.id,[2]choir.harahap@yahoo.com,[3]nurulkhairina27@gmail.com

Abstract

Cryptography RSA method (Rivest - Shamir - Adelman) require large-scale primes to obtain high security that is in greater than or equal to 512, in the process to getting the securities is done to generation or generate prime numbers greater than or equal to 512. Using the Sieve of Eratosthenes is needed to bring up a list of small prime numbers to use as a large prime numbers, the numbers from the result would be combined, so the prime numbers are more produced by the combination Eratosthenes. In this case the prime numbers that are in the range 1500 < prime <2000, for the next step the result of the generation it processed by using the Rabin - Miller Primarily Test. Cryptography RSA method (Rivest - Shamir - Adelman) with the large-scale prime numbers would got securities or data security is better because the difficulty to describe the RSA code gain if it has no RSA Key same with data sender.

Keywords: *Primality Test, Rabin-Miller, Big Prime Number, RSA, Criptography*

1. Introduction

RSA Cryptography requires the use of the big prime numbers. In learning about the RSA is always use the small prime numbers, in the range of prime numbers < 100. However, in reality the necessary for a prime number is far greater than studied. The higher prime numbers are used, the higher securities obtained. Based on the background above, it is needs to study about how to generate the big prime numbers that really reality to use in cryptographic Rivest - Shamir - Adleman.

The Prime Numbers is a positive integer other than 0 and 1, which cannot be factorization and only divisible by 1 and the numbers itself. The numbers for this example are 2, 3, 5, 7, 11, 13, 17 ... and so on.And Composite numbers are positive integers greater than 1 and not included in the prime numbers. The numbers for this simple are 2, 4, 6, 8, 9, 10 ... and so on.

2. Rudimentary

2.1. Sieve of Eratosthenes

The easiest way to get prime numbers with a small number are using the Sieve of Eratosthenes method. This method is used by making a list of numbers from 1 to n, and strikethrough number multiples of the list. [1] Algorithm as follows:

1. Make a list of numbers from 1 to n.
2. Marking that number 1 is Primes (in some opinions stating that the number 1 is not prime)
3. Marking number 2 is primes, then cross all of numbers are multiples of 2. Because multiple of 2 is not a prime number.
4. Marking number 3 is primes, and cross all of the multiples of 3 as not primes.
5. Repeating the process at B and so on until all the numbers that are not prime has been exhausted crossed.

ISSN : 2580-7250
Copyright ⓒ 2017 IJISTECH

6. The numbers that are not crossed out is a list of primes. Based on the above algorithm, so he found the series of prime numbers with a range of 1500 <prime <2000 as shown in the image list below.

1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999

2.2. Mersenne Prime Number

A Mersenne prime numbers is a probability prime number. The formula is

$$M = 2^p - 1 \qquad (1)$$

for p is prime number. For example : $2^2 - 1$ equal 5 (a prime number), $2^3 - 1$ equal 7 (a prime number), $2^5 - 1$ equal 31 (a prime number), etc, but not all get result as prime number.

3. Research and Methodology

3.1. Prime Numbers Test Rabin – Miller

Rabin-Miller Primality Test is the step in determining a number there is a number is prime numbers or composite numbers. Rabin-Miller algorithm has advantages with the accurate ability to calculate the prime numbers are large. In some term is referred to as the Big Prime Numbers, Huge Prime Number also referred to as the Large Prime Numbers. Algorithm testing primes Rabin-Miller can be seen below.[2]

(a) Generate the random number a > p.
(b) Indicate j = 0 and calculate $z = a^m \bmod p$.
(c) If z = 1 or z = p - 1, then p escaped testing and possible prime.
(d) If z > 0 and z = 1, then p is composite.
(e) Indicate j = j + 1. If j < p - 1, state z = z2 mod p and go back to step (d). ≠b and z If z = p - 1, then p passed the test and may be primed.
(f) p - 1, then p is composite. ≠If j = b and z
(g) Repeat testing with Rabin-Miller algorithm above as *t* times (with the different value *a*).

4. Results and Discussion

In 1986, Goldwasser and Kilian filed a prime number testing algorithm using elliptic curve (elliptic curve) that is expected to require polynomial time for almost all of a given input (all inputs are in the trust hypothesis). [3] Based on their algorithms, similar algorithms developed by Atkin. [4] Adleman and Huang modify the algorithm Goldwasser-Kilian so that it can receive all input. [5] In August 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxena submitted a testing prime numbers which fast, only takes a $\log^{15/2} n$, and works without the use of assumptions. [6] Not only this test has never failed, this test also more simpler than another tests of prime numbers which approach polynomial time. This test is based on the nature of prime numbers $(X + a)^n \bmod n = (X_n + a) \bmod n$. But, on the other hand, this test also included slow. [7] The number of steps involved in testing primes using this algorithm increases the rates of the tested number raised to 12. A few months later, Lenstra remedy it and this is steps that taken to grow as many numbers raised to the number who tested 6. [8].

4.1. Huge Prime Number Test primarily

Based on the reviews that were outlined above, to get large prime number can follow the steps below. Get small prime number range (low Primes) by using the

Copyright ⓒ 2017 IJISTECH

Eratosthenes method. Range of small prime numbers are between 1500 - 2000. The number is still very easily to obtained by Eratosthenes method and can be seen below: [9]

Low Primes = [1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669 , 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877 , 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999]

Make the process of reappointment (2^{prime}) - 1 to the number of Low Primes taht obtained by Eratosthenes method above. Reduction function with numbers 1, here is useful to make the result as an odd number. Because besides the number 2 then all primes are odd.

Testing the primes numbers by using the Rabin-Miller methode. Because that is raised is prime number, so by itself the results that would be tested has a very far range, with a range that far, so this would strength the securities of cryptography. It repeatedly until the entire list is exhausted all tested Low Primes, To find Prima Large numbers needed. After understand about explanation above, we can try to perform testing of some primes from Low Primes, the results of Eratosthenes as follows:

Number 2^{1511}-1 =

718329080021689113551413001426551971707371845229175374
31707234354771893965953683873089701655726017047865652033
11705603563375523623213047757654228770407362733647863088
19539911976689719533229321145071251135286039131163759785
26610109491985652509317039400274027625986953903122942307
04359496867043268584566922099497822252576327154201960598
11937347078496094897657928977874601923420021290038545073
53108381696358509272123512587129205838615993392504244651
109122047.

Miller Rabin Primarily test results are false and expressed as **Composites**.

Number 2^{1657} -1 =

640770951290344130719124850287136336124046515705098442
37224596575526095067594218739908887518933790003533215529
23233358553334983520227585773337733421010419363224467944
36122017883768948800731289743036203467811039271025876896
35345173177954152445756285418668359871536377260802057185
88341324538158354471607522528735259587003891050175113295
62681320993874152763264724565443689308763524566180778944
00898135878769546014953347744455741697825330486520212303
62464956535737634962104720295113651480527052967247871

Results of testing methods Rabin Miller is False and expressed as **Composites**.

Number 2^{2203} - 1 =

14759799152141802350848986227373817363120661453331697751
47771216478570297878078949377407337049389289382748507531
49648047728126483876025919181446336533026954049696120111
34301569023960939890902262593269350252814096149834993882
22831448598601834318536230923772641390209490231836446899
60821079548296376309423663094541083279376990539998245718
63229447296364188906233721717237421056364403682184596496

Copyright ⓒ 2017 IJISTECH

32948538696905872650486914434637457507280441823676813517
85209934866084717257940842231667809767022401199028017047
48944874269247421088235368084850725022405194525875428753
49976558572670229633962575212637477897785501552646522609
988869914013540483809865681250419497686697771007

Test Results prime numbers by using Rabin - Miller method stated are **Prime number**

Numbers $2^{2281}-1$ =

446087557183758429571151706402101809886208632412859901
11199121996340468579282047336911254526900398902615324593
11243167023957587056936793647909034974611470710652541933
53938124978226307947312410798874869040070279328428810311
75484410809487825249486676096958699812898264587759602897
91715369625030684296173317021847503245830091718321049160
50157628886606372145501702225925125224076829605427173573
96481299525056941248072073847685529368166671284483119087
76206067866638621902401185707368319018864792258104147140
78935386562497968178729127629594924411960961386713946279
89927500695491713975879606122380339353738103466649440295
10520590479686932553886479304409251041868170096401717641
33172418132836351

Based on the testing methods of Rabin-Miller stated that the numbers is **Prime numbers.**

In search of the prime numbers in the method of Eratosthenes to Low Primes under 1.000.000 is still very easy and needs a short time. Making it possible to obtain a larger prime numbers again. In writing this paper, the author still had explore to Low numbers Primes with the range 2000> Low Primes> 5000, and get prime numbers at

$2^{4253}-1$ =

190797007524439073807468042969529173669356994749940177
39474188267352897978700505370636804983551490024430349595
49507097257621863112241488288119202169045422069607446661
69364221195289538436845390250168663932838805192055137154
39091266652753300730929268753909225704336251785736662469
99754023754629544902932592333031373306435315565397399219
26201438606439020075174723029056838272505051571967594608
35006340449597766065626902082396082556701234418990892795
66460119980579885486301076373809935198265823897818881357
05408653045219655801758081251164080554609057468028203308
71872465408105532321586018961139129603047110844314674567
19677663089258585472715073115637651710083182486471100976
14890313562856541784154881743146033909602737947385055355
96033185561454090008145637865906837031726769698000118775
09954910903501084170509179915621679722810701613059725180
44872048331306383715094854938415738549894606070722584737
97817668642213435452698944302835364403718737538539783825
95118331664161343236956603676768977222879187734209689823
26089026150031515424165462111337527431154890666327374921
44627683356451977679763387550354866509391455648203148224
88831270237770396677079765598573333570137273420790990644

Copyright ⓒ 2017 IJISTECH

00455741830654320379350833236245819348824064783585692924
881021978332974949906122664421376034687815350484991

And also the number

2^{4423}-1 =

285542542228279613901563566102164008326164238644702889
19924745660228440039060065387595457150553984323975451391
58961502978783993770560714351697472211079887911982009884
77531339214282772016059009904586686254989084815735422480
40902234429758835252600438389063261612407631738741688114
85924861883618739041757831456960169195743907655982801885
99035578448591077683677175520434074287726578006266759615
97075952132782855566278167838569158184443644481251156242
81367424904593632128101802760960881114010033775703635457
25120924073646921576797146199387619296560302680261790118
13292501232304644443862230887792460937377301248168167242
44936744744885377701557830068808526481615130671448147902
88366664062257274665275787127374649231096375001170901890
78626332461957879573142569380507305611967758033808433338
19875009029688319359130952698213111413223933564901784887
28982288156282600813831296143663845945431144043753821542
87127774560644785856415921332844358020642271469491309176
27164470416896780700967735904298089096167504529272580008
43500344831628297089902728649981994387647234574276263729
69484830475091717418618113068851879274862261229334136892
80566343844666463265724761672756608391056505289757138993
20211121495795311427946254553305387067821067601768750977
86610046001460213840844802122505368905479374200309572209
6732954750721718115531871310231057902608580607.

Both Numbers were based on the Rabin - Miller primality test is prime number and has reached 1332 Digit.

Primality test number between 2000 until 10000

5. Conclusion

5.1. Conclution

Prime numbers that are different in the range 1500 < prima < 2000, and the generation is processed by using the Rabin - Miller Primarily Test. Cryptography RSA method (Rivets - Shamir - Adelman) primes large-scale get securities or other better data security because the difficulty to describing the RSA code again if it does not have the same RSA key with the sender of the data.

5.2. Suggestions

The increase in computer attacks should be increased, so that the computer hacker (hackers) are continues to innovate in doing the process of assault to find the key RSA that caused by primes. Suggested for other researchers can develop a system or RSA method above in 1024, with the different technique and method but still combined with RSA method.

References

[1] A.B. Smith, C.D. Jones, and E.F. Roberts, “Article Title”, *Journal*, Publisher, Location, Date, pp. 1-10.

[2] Jones, C.D., A.B. Smith, and E.F. Roberts, *Book Title*, Publisher, Location, Date. Frobenius primality test with average and worst case error estimates. 2003.

Copyright ⓒ 2017 IJISTECH

[3] Goldwasser, S. dan J. Kilian. *Almost all prime can be quickly certified*. 1986.
[4] Atkin, AOL. Lecture notes of a conference, boulder (colorado). 1986.
[5] Adleman, LM. dan MD. Huang. *Primalitytesting and two dimensional Abelian varieties over finite fields*. 1992.
[6] Agrawal, Manindra, Neeraj Kayal, dan Nitin Saxena. *PRIMES is in P*. 2002.Kanpur: Department of Computer Science & Engineering Indian Institute of Technology Kanpur.
[7] Aaronson, Scott. The Prime Facts: From Euclid to AKS. 2003
[8] Lenstra, HW. Jr. Primality testing with cyclotomic rings. 2002.
[9] Damgard, Ivan B. dan Gudmund Skovbjerg Frandsen. An extended quadratic

Copyright ⓒ 2017 IJISTECH

Authors

1st Author
Dicky Apdillah
Lecturer of School of Information Engineering and Enginering Computer / AMIK INTeL Com GLOBAL INDO
dicky@nusa.net.id

2nd Author
Muhammad Khoiruddin Harahap
Lecturer of Politeknik Ganesha Medan
choir.harahap@yahoo.com

3rd Author
Nurul Khairina
Lecturer of Politeknik Ganesha Medan
nurulkhairina27@gmail.com

Copyright ⓒ 2017 IJISTECH