

Membangkitkan Bilangan Prima Mersenne di atas 512 Digit Menggunakan Kombinasi Eratosthenes dan Fermat Little Theorem Untuk Pendukung Kunci Publik RSA

Muhammad Khoiruddin Harahap
Magister Teknik Informatika, Universitas Sumatera Utara
choir.harahap@yahoo.com

ABSTRAK

Kriptografi Metode RSA (Rivest – Shamir – Adleman) membutuhkan bilangan prima berskala besar untuk mendapatkan sekuritas yang tinggi yaitu pada kisaran 512 digit ke atas. Sieve of Erathosthenes diperlukan untuk memunculkan daftar bilangan prima yang kecil untuk digunakan sebagai pembangkit bilangan prima yang besar. Dalam hal ini bilangan prima yang berada pada range $1500 < p < 2000$. Hasil pembangkitan bilangan prima tersebut selanjutnya diuji dengan menggunakan Metode Fermat.

Keyword : Bilangan Prima, Mersenne, Sieve of Eratosthenes, Fermat, Kriptografi, RSA

1. Pendahuluan

Kriptografi RSA membutuhkan penggunaan bilangan prima yang besar. Dalam pembelajaran tentang RSA selalu menggunakan bilangan prima yang kecil, kisaran bilangan prima < 100 . Namun dalam realitanya kebutuhan terhadap bilangan prima ini jauh lebih besar dari yang dipelajari. Semakin besar bilangan prima yang digunakan maka semakin tinggi sekuritasnya. Berdasarkan latar belakang di atas, maka perlu pembahasan bagaimana cara membangkitkan bilangan prima 512 digit ke atas untuk digunakan pada kriptografi RSA (Rivest – Shamir – Adleman).

Perumusan masalah ini membahas cara untuk membangkitkan bilangan prima Mersenne untuk bilangan 512 digit ke atas. Walaupun kebutuhan utamanya adalah untuk melengkapi kriptografi RSA, namun pembahasan tidak menyentuh algoritma kriptografi RSA itu sendiri.

Penelitian ini bertujuan untuk melengkapi Kriptografi Kunci Publik RSA dalam mendapatkan bilangan prima. Dalam hal ini adalah bilangan prima dengan skala 512 digit ke atas. Sehingga mampu mengaplikasikan Kriptografi Kunci Publik RSA dengan baik.

2. Landasan Teori

2.1. Bilangan Prima dan Komposit

Bilangan Prima adalah bilangan bulat Positif selain 0 dan 1, yang tidak bisa difaktorisasi dan hanya habis dibagi oleh bilangan 1 dan bilangan itu sendiri. Bilangan untuk ini misalnya 2, 3, 5, 7, 11, 13, 17 ... dan seterusnya.

Dan bilangan Komposit adalah bilangan bulat positif yang lebih besar dari 1 dan bukan termasuk dalam bilangan prima. Bilangan untuk ini sederhananya adalah 2, 4, 6, 8, 9, 10 ... dan seterusnya [1].

2.2. Bilangan Mersenne

Ahli Matematika Perancis pada tahun 1644, M. Mersenne merumuskan $M_p = 2^p - 1$, jika M_p maka bilangan tersebut dinyatakan sebagai Mersenne Prime. Bilangan yang dinyatakan oleh Mersenne tersebut adalah : $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257

$$\begin{aligned}M_1 &= 2^1 - 1 = 1 \\M_2 &= 2^2 - 1 = 3 \\M_3 &= 2^3 - 1 = 7 \\M_4 &= 2^5 - 1 = 31 \\M_5 &= 2^7 - 1 = 127\end{aligned}$$

Walaupun teori tersebut menghasilkan bilangan prima, namun tidak berlaku untuk semua bilangan prima. Untuk formula di atas akan mampu membangkitkan bilangan prima yang besar dengan bantuan Sieve of Eratosthenes sebagai pembangkit bilangan prima yang kecil [5].

2.3. Sieve of Eratosthenes

Cara paling mudah untuk mendapatkan bilangan prima dengan bilangan yang kecil adalah dengan menggunakan metode Sieve Eratosthenes. Metode ini dengan membuat daftar bilangan dari 1 sampai dengan n, dan mencoret bilangan kelipatan dari daftar. Algoritma sebagai berikut :

- Membuat daftar bilangan mulai 1 - n.

- b. Menandai bahwa bilangan 1 adalah Prima (dalam beberapa pendapat menyatakan bahwa bilangan 1 bukanlah prima)
- c. Menandai bilangan 2 adalah prima, kemudian mencoret semua bilangan kelipatan dari 2. Karena kelipatan 2 bukanlah bilangan prima.
- d. Menandai bilangan 3 adalah prima serta mencoret semua kelipatan 3 sebagai bukan prima.
- e. Mengulangi proses pada b dan seterusnya sampai kemudian semua bilangan yang bukan prima telah habis tercoret.
- f. Bilangan yang tidak dicoret adalah daftar bilangan prima [3].

Berdasarkan algoritma di atas, maka didapatkan deret bilangan prima dengan range $1500 < \text{prima} < 2000$ seperti terlihat pada daftar dibawah ini.

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

2.4. Pengujian Bilangan Prima Metode Fermat

Pierre De Fermat seorang matematikawan dari Perancis mengeluarkan karyanya disebut dengan **Little Fermat Theorem**. Pierre de Fermat mengatakan bahwa n adalah bilangan prima jika memenuhi persyaratan :

$$a^{n-1} \equiv 1 \pmod{n} \dots \dots \dots [4]$$

Dimana bilangan a merupakan bilangan bulat acak memenuhi persyaratan $1 < a < n-1$.

Fermat Little Theorem merupakan pengujian prima probabalistik dikarenakan tidak semua bilangan a yang memenuhi $1 < a < n-1$ diuji. Bilangan a yang digunakan adalah beberapa bilangan acak. Dikarenakan tidak semua nilai a yang memenuhi persyaratan di atas digunakan, maka masih ada kemungkinan hasil pengujian salah.

3. Membangkitkan Bilangan Prima Besar dan Pengujian Bilangan Prima Metode Fermat

Berdasarkan ulasan yang sudah dipaparkan di atas, untuk mendapatkan bilangan prima yang besar dapat mengikuti langkah – langkah berikut ini.

1. Dapatkan *range* bilangan prima yang kecil (low Primes) dengan menggunakan metode Eratosthenes. Range bilangan prima yang kecil ini adalah antara 1500 – 2000. Angka tersebut masih sangat mudah didapatkan dengan metode Eratosthenes dan dapat dilihat berikut ini :

lowPrimes = [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. Lakukan proses pemangkatan $(2^p - 1)$ dengan menggunakan p pada bilangan *LowPrimes* yang didapatkan oleh metode Eratosthenes di atas. Fungsi pengurangan dengan bilangan 1, disini berguna untuk menjadikan hasilnya sebagai bilangan ganjil. Karena selain angka 2 maka semua bilangan prima adalah ganjil.
3. Melakukan pengujian keprimaan bilangan dengan menggunakan metode Fermat. Karena yang dipangkatkan adalah bilangan prima, maka dengan sendirinya hasil yang akan diuji tersebut memiliki rentang yang sangat lebar, dengan rentang yang lebar tersebut, maka ini akan memperkuat sekuritas dari kriptografi tersebut.
4. Lakukan secara berulang sampai dengan semua daftar *LowPrimes* nya habis semua diuji Sampai menemukan bilangan Prima Besar yang dibutuhkan.

Setelah memahami penjelasan di atas, dapat kita coba untuk melakukan pengujian terhadap beberapa bilangan prima dari *LowPrimes* hasil Eratosthenes seperti berikut ini :

1. Bilangan $n = 2^{1511} - 1 =$
7183290800216891135514130014265519717
0737184522917537431707234354771893
9659536838730897016557260170478656
5203311705603563375523623213047757
6542287704073627336478630881953991
1976689719533229321145071251135286
0391311637597852661010949198565250
9317039400274027625986953903122942
3070435949686704326858456692209949
7822252576327154201960598119373470
7849609489765792897787460192342002
1290038545073531083816963585092721

2351258712920583861599339250424465
1109122047.

Pengujian Fermat :
Misal $a = 2$:

$$2^{n-1} \pmod{n} = 1$$

Misal $a = 3$ maka :

$$2^{n-1} \pmod{n} =$$

23915817326175933424177029756630777867
22596357645762134868706194414184722082
45157104906077314171570325559872584799
97641839453708892845764771036233247160
64943636853850411087523785414291347381
10163522873188304690877047320900824207
65503992913078045037743143521977278822
39175661542464789836902975695054764102
38057426608859471977079966068737112984
52900015359313343524948812248734668330
47124857901897695231541024878620419174
1485498356187262256491472019282458392

Hasil pengujian pada saat $a = 3$ menghasilkan tidak sama dengan 1. Disimpulkan n adalah **Komposit**.

2. Bilangan $2^{1657} - 1$ =

6407709512903441307191248502871363361
2404651570509844237224596575526095
0675942187399088875189337900035332
1552923233358553334983520227585773
3377334210104193632244679443612201
7883768948800731289743036203467811
0392710258768963534517317795415244
5756285418668359871536377260802057
1858834132453815835447160752252873
5259587003891050175113295626813209
9387415276326472456544368930876352
4566180778944008981358787695460149
5334774445574169782533048652021230
3624649565357376349621047202951136
51480527052967247871

Pengujian Fermat :
Misal $a = 2$:

$$2^{n-1} \pmod{n} = 1$$

Misal $a = 3$ maka :

$$2^{n-1} \pmod{n} =$$

25473334132482750744615288387730
34052810441469895682063645872234092762
74257329411175793610148905245999470403
04744454869983433435156416300621503766
29013852289848335327199918353501079401
0879831050506091480171756062828833257
74071197888566347881061851520077039114
43164362523315606659746391274014211069

29583329776835892535347268068535266235
23291472403672874582289236993189408093
20377667997069600306096485405182262550
46855539008969441249384733688217078192
18500742696173800093412292145989624299
1397986978

Hasil pengujian pada saat $a = 3$ menghasilkan tidak sama dengan 1. Maka dinyatakan sebagai bilangan **Komposit**.

3. Bilangan $2^{2203} - 1$ =
- 1475979915214180235084898622737381736
3120661453331697751477712164785702
9787807894937740733704938928938274
8507531496480477281264838760259191
8144633653302695404969612011134301
5690239609398909022625932693502528
1409614983499388222831448598601834
3185362309237726413902094902318364
4689960821079548296376309423663094
5410832793769905399982457186322944
7296364188906233721717237421056364
4036821845964963294853869690587265
0486914434637457507280441823676813
5178520993486608471725794084223166
7809767022401199028017047489448742
6924742108823536808485072502240519
4525875428753499765585726702296339
6257521263747789778550155264652260
9988869914013540483809865681250419
497686697771007

Misalkan nilai $a = 2$ maka :

$$2^{n-1} \pmod{n} = 1$$

Misalkan nilai $a = 3$ maka :

$$2^{n-1} \pmod{n} = 1$$

Misalkan nilai $a = 5$ maka :

$$2^{n-1} \pmod{n} = 1$$

Misalkan nilai $a = 2963641889062337$:

$$2^{n-1} \pmod{n} = 1$$

Hasil Uji keprimaan menyatakan adalah bilangan **Prima**.

4. Bilangan $2^{2281} - 1$ =
- 4460875571837584295711517064021018098
8620863241285990111199121996340468
5792820473369112545269003989026153
2459311243167023957587056936793647
9090349746114707106525419335393812

4978226307947312410798874869040070
 2793284288103117548441080948782524
 9486676096958699812898264587759602
 8979171536962503068429617331702184
 7503245830091718321049160501576288
 8660637214550170222592512522407682
 9605427173573964812995250569412480
 7207384768552936816667128448311908
 7762060678666386219024011857073683
 1901886479225810414714078935386562
 4979681787291276295949244119609613
 8671394627989927500695491713975879
 6061223803393537381034666494402951
 0520590479686932553886479304409251
 0418681700964017176413317241813283
 6351

Uji Bilangan Prima metode fermat :
 Misalkan nilai a = 2 maka :

$$2^{n-1} \pmod{n} = 1$$

Misalkan nilai a = 3 maka :

$$2^{n-1} \pmod{n} = 1$$

Misalkan nilai a = 5 maka :

$$2^{n-1} \pmod{n} = 1$$

Misalkan nilai a =
 64139020949023183644689960821079548
 29637630942366309454108327937699053
 99982457186322944729636418890623372
 17172374210563644036821845964963294
 85386969058726504869144346374575072
 804418236768135178:

$$2^{n-1} \pmod{n} = 1$$

Hasil Uji keprimaan menyatakan adalah bilangan **Prima**.

Dalam pencarian bilangan prima tersebut pada metode Eratosthenes untuk *LowPrimes* dibawah 1.000.000 masih sangat mudah dan membutuhkan waktu yang singkat. Sehingga memungkinkan untuk mendapatkan bilangan prima yang lebih besar lagi.

Dalam penulisan paper ini, penulis masih sempat berekplorasi untuk bilangan *LowPrimes* dengan range $2000 > \text{lowPrimes} > 5000$, dan mendapatkan angka bilangan prima pada $2^{4253} - 1 =$
 190797007524439073807468042969529173669
 35699474994017739474188267352897978
 70050537063680498355149002443034959
 54950709725762186311224148828811920
 21690454220696074466616936422119528

95384368453902501686639328388051920
 55137154390912666527533007309292687
 53909225704336251785736662469997540
 23754629544902932592333031373306435
 31556539739921926201438606439020075
 17472302905683827250505157196759460
 83500634044959776606562690208239608
 25567012344189908927956646011998057
 98854863010763738099351982658238978
 18881357054086530452196558017580812
 51164080554609057468028203308718724
 65408105532321586018961139129603047
 11084431467456719677663089258585472
 71507311563765171008318248647110097
 61489031356285654178415488174314603
 39096027379473850553559603318556145
 40900081456378659068370317267696980
 00118775099549109035010841705091799
 15621679722810701613059725180448720
 48331306383715094854938415738549894
 60607072258473797817668642213435452
 69894430283536440371873753853978382
 59511833166416134323695660367676897
 72228791877342096898232608902615003
 15154241654621113375274311548906663
 27374921446276833564519776797633875
 50354866509391455648203148224888312
 70237770396677079765598573333570137
 27342079099064400455741830654320379
 35083323624581934882406478358569292
 48810219783329749499061226644213760
 34687815350484991

Dan juga pada bilangan $2^{4423} - 1 =$
 2855425422282796139015635661021640083261
 642386447028891992474566022844003906
 006538759545715055398432397545139158
 961502978783993770560714351697472211
 079887911982009884775313392142827720
 160590099045866862549890848157354224
 804090223442975883525260043838906326
 161240763173874168811485924861883618
 739041757831456960169195743907655982
 801885990355784485910776836771755204
 340742877265780062667596159707595213
 278285556627816783856915818444364448
 125115624281367424904593632128101802
 760960881114010033775703635457251209
 240736469215767971461993876192965603
 026802617901181329250123230464444386
 223088779246093737730124816816724244
 936744744885377701557830068808526481
 615130671448147902883666640622572746
 652757871273746492310963750011709018
 907862633246195787957314256938050730
 561196775803380843333819875009029688
 31935913095269821311413223933564901
 784887289822881562826008138312961436
 638459454311440437538215428712777456

064478585641592133284435802064227146
949130917627164470416896780700967735
904298089096167504529272580008435003
448316282970899027286499819943876472
345742762637296948483047509171741861
811306885187927486226122933413689280
566343844666463265724761672756608391
056505289757138993202111214957953114
279462545533053870678210676017687509
778661004600146021384084480212250536
890547937420030957220967329547507217
18115531871310231057902608580607

Kedua angka tersebut berdasarkan Rabin – Miller primality test adalah bilangan prima dan sudah mencapai 1332 Digit.

4. Kesimpulan

Berdasarkan Pembahasan di atas, dapat diambil kesimpulan bahwa membangkitkan bilangan prima yang besar bisa dilakukan dengan mengkombinasikan antara Sieve of Eratosthenes, Bilangan Mersenne dan pengujian bilangan prima dengan metode Fermat. Pengujian yang dilakukan membutuhkan proses iterasi agar mendapatkan hasil yang maksimal.

Pengujian yang dilakukan pada paper ini hanya menggunakan metode Little Fermat Theorem, dan disarankan untuk menambahkan teori pengujian bilangan probabalistik prima seperti Solovoy – Strassen, Rabin-Miller Primality Test dan lainnya sehingga benar-benar diyakini keprimaan angka tersebut.

Daftar Pustaka

- [1] Hadi, Ahmaddul. 2011. *Rancang Bangun Sistem Pengamanan Dokumen Pada Sistem Informasi Akademik Menggunakan Digital Signature dengan Algoritma Kurva Eliptik*. Tesis. Semarang : Universitas Semarang.
- [2] Kromodimoeljo, Sentot. 2009. *Teori & Aplikasi Kriptografi*. SPK IT Consulting.
- [3] Safri Lubis, Muhammad, Andri Budiman, Muhammad, dan Lolo Manik, Karina. 2013. *Penggunaan Algoritma RSA dengan Sieve of Eratosthenes dalam Enkripsi dan Dekripsi Pengiriman Email*.Jurnal. SNATI : Yogyakarta.
- [4] Yus Trinity Irsan, Maria, Haryanto, Loeky, dan Kamal, Amir. 2014. *Uji Keprimaan Probabilistik Solovay - Strassen dan Rabin – Miller*. Universitas Hasanuddin
- [5] Zhang, Sibao, Zhou, Lihang, 2011. *The Numbers of Thousand Place of Mersenne Primes*. Applied Mathematics. Scientific Research. Kashgar : Cina.