Buletin Ilmiah Mat. Stat. dan Terapannya (Bimaster)
Volume 04, No. 1 (2015), hal 85 – 94.

METODE SOLOVAY-STRASSEN UNTUK PENGUJIAN BILANGAN PRIMA

Sari Puspita, Evi Noviani, Bayu Prihandono

INTISARI

Bilangan prima merupakan bilangan bulat positif yang lebih besar dari satu dan hanya habis dibagi oleh satu dan dirinya sendiri, sedangkan bilangan bulat positif selain prima disebut bilangan komposit atau bilangan yang terdiri dari minimal dua faktor prima. Untuk mencari faktor prima dapat menggunakan uji probabilistik. Uji probabilistik merupakan uji yang menggunakan konsep acak. Salah satu uji probabilistik yaitu metode Solovay-Strassen. Pengujian pada metode Solovay-Strassen diuji berdasarkan Euler pseudoprima. Langkah pertama pengujian bilangan prima pada metode Solovay-Strassen yaitu menentukan bilangan yang diuji yaitu n, n yang dimaksud adalah bilangan bulat positif ganjil. Kemudian menentukan basis b yang dipilih secara acak, basis b yang dimaksud adalah sebarang bilangan bulat positif yang berada pada interval 0<b<n. Kemudian dilanjutkan dengan mencari d=gcd(b,n) dengan menggunakan algoritma Euclid. Jika didapat bahwa d>1, maka n dikatakan komposit. Namun jika didapat bahwa d=1, maka n diuji dengan menggunakan Euler pseudoprima. Jika n lulus uji Euler pseudoprima untuk basis b, maka n disebut Euler pseudoprima untuk basis b. Dengan demikian n dapat dikatakan bilangan prima. Jika n tidak lulus uji persamaan Euler pseudoprima, maka n disebut sebagai komposit.

Kata Kunci : *Solovay-Strassen, Simbol Jacobi, Simbol Legendre.*

PENDAHULUAN

Bilangan prima merupakan bilangan bulat positif yang lebih besar dari satu dan hanya habis dibagi oleh satu dan dirinya sendiri. Bilangan komposit adalah bilangan yang terdiri dari minimal dua faktor prima [1]. Beberapa manfaat dari bilangan prima yaitu sebagai kodetifikasi pesan yang bersifat penting dan rahasia, misalnya pada sistem keamanan, perhitungan-perhitungan peluru kendali, bank, dan asuransi [1].

Bilangan prima yang dianggap baik untuk kodetifikasi adalah bilangan prima yang besar karena semakin besar bilangan prima maka semakin sulit seseorang untuk memecahkan pesan yang sudah disandikan [2]. Salah satu konsep kriptografi yang memanfaatkan faktor bilangan prima yaitu konsep kriptografi publik. Kriptografi publik merupakan kriptografi yang memiliki sepasang kunci, yaitu kunci publik (boleh diketahui oleh orang lain) dan kunci privat (bersifat rahasia). Pada aplikasi kriptografi publik, pemecahan bilangan bulat yang digunakan kurang lebih 200 digit akan dicari faktor bilangan prima. Karena mencari faktor prima dari bilangan bulat ini membutuhkan waktu yang cukup lama, sehingga keamanan dari kriptografi publik dapat digunakan untuk kodetifikasi pesan yang bersifat penting dan rahasia. Dengan demikian diperlukan cara atau metode untuk mencari faktor prima yang besar tersebut. Untuk mencari faktor prima yang besar maka digunakanlah uji probabilistik, uji probabilistik merupakan uji yang menggunakan percobaan acak [3].

Salah satu uji probabilistik adalah metode *Solovay-Strassen*. Metode *Solovay-Strassen* menggunakan definisi Euler pseudoprima untuk menguji suatu bilangan bulat positif apakah prima atau komposit. Pada definisi Euler pseudoprima disebutkan bahwa bilangan bulat positif merupakan Euler pseudoprima, jika n dapat lulus uji persamaan $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) (\mathrm{mod}\, n)$ untuk basis b. Dimana basis b dipilih secara acak dengan cara mengambil sebarang bilangan bulat positif yang berada pada interval $0 < b < n$ [3].

Sehingga tujuan dari penelitian ini adalah bagaimana menguji suatu bilangan bulat positif merupakan bilangan mungkin prima atau komposit dengan menggunakan metode *Solovay-Strassen*.

Dengan demikian langkah-langkah yang digunakan untuk penelitian ini adalah mengkaji definisi dari simbol Legendre, mengkaji definisi simbol Jacobi dan teorema yang terkait simbol Jacobi, mengkaji definisi pseudoprima, mengkaji definisi Euler pseudoprima serta teorema yang berkaitan dengan pseudoprima dan Euler pseudoprima. Kemudian langkah-langkah yang digunakan untuk menyelesaikan uji bilangan prima, pertama menentukan bilangan bulat positif yang akan diuji (yaitu n), lalu menentukan basis b secara acak, dengan cara mengambil sebarang bilangan bulat positif yang berada pada interval $0 < b < n$. Menentukan $d = \gcd(b, n)$ dengan menggunakan algoritma Euclid (yang menggunakan konsep pembagian $n = bq + r$, q hasil bagi sedangkan r sisa). Jika $d > 1$ maka n komposit dan pengujian selesai. Jika $d = 1$ maka uji dilanjutkan dengan menguji n pada persamaan $\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod{n}$ untuk basis b. Dengan demikian persamaan kiri dan kanan harus memiliki nilai yang sama, maka n disebut sebagai bilangan mungkin prima. Jika n bilangan mungkin prima maka jelas bahwa n merupakan Euler pseudoprima. Namun jika didapatkan nilai yang tidak sama pada persamaan kiri dan kanan, maka dapat dikatakan bahwa n komposit.

Metode *Solovay-Strassen* untuk Pengujian Bilangan Prima

Metode *Solovay-Strassen* merupakan salah satu uji probabilistik yang digunakan untuk uji bilangan prima [3]. Bilangan prima merupakan bilangan bulat positif yang lebih besar dari satu dan hanya habis dibagi oleh satu dan dirinya sendiri, sedangkan bilangan selain bilangan prima adalah bilangan komposit. Atau dapat diartikan juga bahwa bilangan komposit adalah bilangan bulat positif yang terdiri dari minimal dua faktor prima [1]. Salah satu uji probabilistik yaitiu metode *Solovay-Strassen*, dimana pengambilan basis b dipilih secara acak, dengan cara mengambil sebarang bilangan bulat ganjil positif yang berada pada interval $0 < b < n$ [3]. Sebelum membahas metode *Solovay-Strassen*, perlu diketahui dahulu definisi dari kongruen

Definisi 1 [4] *Jika bilangan bulat m tidak nol, membagi selisih $a - b$, dapat dikatakan bahwa a kongruen pada modulo m dan ditulis dengan $a \equiv b \pmod{m}$, jika $a - b$ tidak habis dibagi m, maka dapat dikatakan bahwa a tidak kongruen pada modulo m, dan ditulis dengan $a \not\equiv b \pmod{m}$.*

Dari definisi 2 diperoleh bahwa kongruen ($a \equiv b \pmod{m}$) adalah selisih dari $a - b$ dapat habis dibagi oleh m, jika ternyata selisih dari a dan b tidak habis dibagi oleh m, maka $a \not\equiv b \pmod{m}$.

Contoh 2: Jika $16 \equiv 4 \pmod{6}$ maka berdasarkan definisi 2, 6 dapat membagi habis selisih $16 - 4 = 12$, sehingga benar bahwa $16 \equiv 4 \pmod{6}$.

Tingkat kesalahan yang terjadi pada algoritma *Solovay-Strassen* dibuktikan dengan teorema berikut,

Teorema 3 [4] *Teorema Binomial, untuk setiap bilangan bulat $n \geq 1$ dan untuk setiap bilangan real x dan y, $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$.*

Definisi 4 [4] *Untuk semua b sedemikian sehingga $(b, n) = 1$, b dikatakan kongruen terhadap residu kuadratik modulo n jika $x^2 \equiv b \pmod{n}$ memiliki solusi, jika $x^2 \equiv b \pmod{n}$ tidak memiliki solusi, maka b dikatakan bukan residu kuadratik modulo n.*

Pada Definisi 4 untuk semua b sedemikian sehingga $(b, n) = 1$, yang berarti bahwa b dan n relatif prima. Dua bilangan dikatakan relatif prima jika faktor persekutuan dari b dan n adalah 1 atau dapat

ditulis $\gcd(b,n)=1$ atau $(b,n)=1$ [3]. Pada Definisi 4 juga disebutkan bahwa b disebut kongruen terhadap modulo n jika $x^2 \equiv b \pmod n$ memiliki solusi, jika tidak memiliki solusi maka b bukan residu kuadratik.
Pembahasan pada metode *Solovay-Strassen* juga membahas simbol Legendre, dimana simbol Legendre didefinisikan sebagai berikut,

Definisi 5 [3] *Simbol Legendre dinotasikan dengan* $\left(\frac{a}{p}\right)$

$$\left(\frac{a}{p}\right)=\begin{cases} 0, & \textit{Jika } p|a \\ 1, & \textit{Jika a merupakan residu kuadratik (mod p)} \\ -1, & \textit{Jika a merupakan non-residu kuadratik (mod p)} \end{cases}$$

dimana a adalah bilangan bulat dan p adalah bilangan prima.

Contoh 6: buktikan bahwa $x^2 \equiv 10 \pmod{89}$ atau dapat ditulis $\frac{10}{89}=\frac{x^2}{89}$

$\left(\frac{10}{89}\right)=\left(\frac{2}{89}\right)\left(\frac{5}{89}\right)=(1)\left(\frac{5}{89}\right)=\left(\frac{89}{5}\right)=\left(\frac{4}{5}\right)=\left(\frac{2}{5}\right)\left(\frac{2}{5}\right)=(1)(1)=1.$

jadi, benar bahwa $a=10$ merupakan residu kuadratik modulo 89, karena $\left(\frac{10}{89}\right)=1$.

Salah satu uji bilangan prima adalah *Fermat's little theorem*, teorema ini sering sekali digunakan untuk dasar dari uji bilangan prima yang lain, serta dapat juga digunakan untuk pembuktian teorema penting dari simbol Legendre.

Teorema 7 [2] *Jika n adalah bilangan prima dan b adalah bilangan bulat yang tidak habis dibagi dengan n, yaitu* $\gcd(b,n)=1$ *maka*

$$b^{n-1} \equiv 1 \ (mod\ n).$$

Teorema terpenting untuk simbol Legendre adalah.
Teorema 8 [3] *Jika a bilangan bulat positif dan p adalah bilangan prima, maka*

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

Bukti:
Ada dua kemungkinan dalam pembuktian teorema 8;

i. Jika $p|a$ maka kedua sisi dari persamaan akan sama dengan 0.
   Jika p habis dibagi a, maka kedua persamaan akan sama dengan 0, berdasarkan definisi 5, maka $a^{(p-1)/2} \equiv 0 \pmod p$, sehingga dapat disimpulkan bahwa
   $$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p \equiv 0 \pmod p.$$
ii. Jika $p \nmid a$ maka berdasarkan Teorema 7, didapat $a^{((p-1)/2)2}=a^{p-1} \equiv 1 \pmod p$.
   jadi $a^{(p-1)/2}=\pm 1$. Jika g adalah suatu generator untuk $\mathbf{F}_p^*$ maka terdapat bilangan j dimana $a=g^j$, a merupakan residu kuadratik jika dan hanya jika j genap, dan $a^{(p-1)/2}=a^{j((p-1)/2)}=1$ jika dan hanya jika $j(p-1)/2=1$ dapat dibagi oleh $(p-1)$ (karena generator menghasilkan 1 jika dan hanya jika dipangkatkan oleh kelipatan $(p-1)$). Jadi $j(p-1)/2$ dapat dibagi oleh $(p-1)$ jika dan hanya jika j dapat dibagi oleh 2 (j genap). Sehingga kedua sisi dari persamaan tersebut sama dengan 1 jika dan hanya jika j genap. Karena $p \nmid a$ kedua sisi persamaan menghasilkan ± 1, menghasilkan 1 jika dan hanya jika j genap dan kedua sisi menghasilkan -1 jika dan hanya jika j tidak genap (ganjil). Kedua sisi selalu menghasilkan nilai yang sama.

Kemudian pada teorema Lagrange juga diperlukan untuk membuktikan teorema tingkat kesalahan pada metode *Solovay-Strassen*,

Teorema 9 [5] *Misalkan G adalah grup berhingga dan misalkan H adalah subgrup dari G, maka banyaknya anggota H (dinotasikan dengan $|H|$ membagi banyaknya anggota G (dinotasikan dengan $|H|$).*

Teorema 9 menyatakan bahwa subgrup $|H|$ membagi grup $|G|$ atau dapat ditulis bahwa $|H|\big||G|$.

Pada metode *Solovay-Strassen* terdapat pembahasan mengenai simbol Jacobi, adapun simbol Jacobi didefinisikan sebagai berikut.

Definisi 10 [3] *Diberikan $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_m^{\alpha_m}$ adalah prime factorization dari n, sedemikian sehingga simbol Jacobi didefinisikan sebagai berikut $\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)^{\alpha_1}\left(\frac{b}{p_2}\right)^{\alpha_2} \dots \left(\frac{b}{p_m}\right)^{\alpha_m}$.*

Contoh 11: Tentukan nilai dari $\left(\frac{b}{n}\right)$, jika diketahui $a = 40$ dan $n = 97$

$\left(\frac{40}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{20}{97}\right) = (1)\left(\frac{20}{97}\right) = \left(\frac{20}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{10}{97}\right) = (1)\left(\frac{10}{97}\right) = \left(\frac{10}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{5}{97}\right) = (1)\left(\frac{5}{97}\right)$
$= \left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1.$

Jadi, nilai dari $\left(\frac{40}{97}\right) = -1$.

Sifat-sifat dari simbol Jacobi yang disebutkan pada teorema berikut, dapat digunakan untuk mencari nilai dari simbol Jacobi.

Teorema 12 [3] *Sifat-sifat simbol Jacobi, dimana m, n adalah bilangan ganjil positif, dan a, b adalah bilangan bulat,*

i. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

ii. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

iii. $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ *jika* $a \equiv b \ (mod\ n)$

iv. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$

v. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

vi. $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{(a-1)}{2}\frac{(n-1)}{2}}$ *jika* $gcd(a,n) = 1$, $a > 0$, *a ganjil*

Bukti:

i. Akan dibuktikan bahwa $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, berdasarkan Definisi 10 dan persamaan dimana $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_m^{\alpha_m}$, maka
$\left(\frac{ab}{n}\right) = \left(\frac{ab}{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}}\right) = \left(\frac{ab}{p_1}\right)^{\alpha_1}\left(\frac{ab}{p_2}\right)^{\alpha_2} \dots \left(\frac{ab}{p_m}\right)^{\alpha_m} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
jadi terbukti bahwa $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

ii. Akan dibuktikan bahwa $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$, berdasarkan Definisi 10 dimana $m = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_j^{\alpha_j}$ dan $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}$ maka,
$\left(\frac{a}{mn}\right) = \left(\frac{a}{p_1\,p_1}\right)^{\alpha_1\alpha_1} \dots \left(\frac{a}{p_jp_k}\right)^{\alpha_j\alpha_k}$
$= \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_j}\right)^{\alpha_j}\left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_k}\right)^{\alpha_k} = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
Terbukti bahwa $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

iii. Akan dibuktikan bahwa $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ jika $a \equiv b \pmod n$

Dari Definisi 10 bahwa $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, sehingga jika $a \equiv b (\text{mod } p_m^{\alpha_m})$ maka $\left(\frac{a}{p_m}\right)^{\alpha_m} = \left(\frac{b}{p_m}\right)^{\alpha_m}$ yang berarti bahwa $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

iv. Akan dibuktikan $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$. Berdasarkan definisi 10 diketahui bahwa $\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)^{\alpha_1} \left(\frac{-1}{p_2}\right)^{\alpha_2} \dots \left(\frac{-1}{p_m}\right)^{\alpha_m} = \left((-1)^{(p_1-1)/2}\right)^{\alpha_1} \dots \left((-1)^{(p_m-1)/2}\right)^{\alpha_m}$

Akan ditunjukkan jika m, n bilangan ganjil, maka $\frac{m-1}{2} + \frac{n-1}{2} \equiv \frac{mn-1}{2} \pmod 2$

Karena m, n ganjil, maka terdapat m', n' ganjil, dimana $m = 2m' + 1$, $n = 2n' + 1$, sehingga didapat

$\frac{m-1}{2} + \frac{n-1}{2} = \frac{(2m'+1)-1}{2} + \frac{(2n'+1)-1}{2} = \frac{2m'}{2} + \frac{2n'}{2} = m' + n'.$

dan didapat juga

$\frac{mn-1}{2} = \frac{(2m'+1)(2n'+1)-1}{2} = \frac{4m'n'+2m'+2n'+1-1}{2} = \frac{4m'n'+2m'+2n'}{2} = 2m'n' + m' + n'$

Sehingga $m' + n' \equiv 2m'n' + m' + n' \pmod 2$ dimana selisih antara $m' + n'$ dan $2m'n' + m' + n'$ dibagi habis oleh 2 maka didapat $\frac{m-1}{2} + \frac{n-1}{2} \equiv \frac{mn-1}{2} \pmod 2$. Karena produk bilangan ganjil juga ganjil, maka didapatlah $\frac{n_1-1}{2} + \dots + \frac{n_m-1}{2} \equiv \frac{n_1 \dots n_m - 1}{2} \pmod 2$. Dengan demikian diperoleh bahwa,

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)^{\alpha_1} \dots \left(\frac{-1}{p_m}\right)^{\alpha_m}$$
$$= \left((-1)^{(p_1-1)/2}\right)^{\alpha_1} \dots \left((-1)^{(p_m-1)/2}\right)^{\alpha_m} = (-1)^{\alpha_1(p_1-1)/2 + \dots + \alpha_m(p_m-1)/2} = (-1)^k$$

Dengan $k = \sum_{i=1}^{k} \alpha_i (p_i - 1)/2$, jadi

$$k = \underbrace{(p_1 - 1)/2 + \dots + (p_1 - 1)/2}_{\alpha_1} + \dots + \underbrace{(p_m - 1)/2 + \dots + (p_m - 1)/2}_{\alpha_m}$$
$$\equiv (p_1 \dots p_1 \dots p_m \dots p_m - 1)/2 \pmod 2$$
$$\equiv p_1^{\alpha_1} \dots p_m^{\alpha_m} - 1/2 \pmod 2 \equiv (n-1)/2 \pmod 2$$

Karena $(-1)^k = (-1)^{(n-1)/2}$ sehingga $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$, jadi terbukti bahwa $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

v. Akan dibuktikan bahwa $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$. Berdasarkan definisi 10 diketahui bahwa $\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right)^{\alpha_1} \left(\frac{2}{p_2}\right)^{\alpha_2} \dots \left(\frac{2}{p_m}\right)^{\alpha_m} = \left((-1)^{(p_1{}^2-1)/2}\right)^{\alpha_1} \dots \left((-1)^{(p_m{}^2-1)/2}\right)^{\alpha_m}$

Akan ditunjukkan jika m, n adalah bilangan ganjil maka,

$\frac{m^2-1}{8} + \frac{n^2-1}{8} \equiv \frac{m^2n^2-1}{8} \pmod 2$

Karena m, n ganjil, maka terdapat m', n' dimana $m = 2m' + 1$, $n = 2n' + 1$, sehingga diperoleh

$\frac{m^2-1}{8} + \frac{n^2-1}{8} = \frac{(2m'+1)^2-1}{8} + \frac{(2n'+1)^2-1}{8} = \frac{4m'^2+4m'+4n'^2+4n'}{8}$

dan diperoleh juga,

$$\frac{m^2n^2-1}{8} = \frac{(2m'+1)^2(2n'+1)^2-1}{8}$$
$$= 2(m'^2n'^2 + m'^2n' + m'n'^2 + m'n') + \frac{4m'^2+4n'^2+4m'+4n'}{8}$$
$$\equiv \frac{4m'^2+4n'^2+4m'+4n'}{8} \pmod 2$$

Dengan demikian terbukti bahwa $\frac{m^2-1}{8} + \frac{n^2-1}{8} \equiv \frac{m^2n^2-1}{8} \pmod 2$, karena produk bilangan ganjil juga ganjil, maka didapat $\frac{n_1^2-1}{8} + \dots + \frac{n_m^2-1}{8} \equiv \frac{n_1^2 \dots n_m^2 - 1}{8} \pmod 2$. Dengan demikian diperoleh bahwa,

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right)^{\alpha_1} \dots \left(\frac{2}{p_m}\right)^{\alpha_m}$$
$$= \left((-1)^{(p_1^2-1)/8}\right)^{\alpha_1} \dots \left((-1)^{(p_m^2-1)/8}\right)^{\alpha_m}$$
$$= \left((-1)^{\alpha_1(p_1^2-1)/8}\right) \dots \left((-1)^{\alpha_m(p_m^2-1)/8}\right) = (-1)^k$$

Dengan $k = \sum_{i=1}^{k} \alpha_i(p_i^2 - 1)/8$, jadi

$$k = \underbrace{(p_1^2 - 1)/2 + \dots + (p_1^2 - 1)/8}_{\alpha_1} + \dots + \underbrace{(p_m^2 - 1)/2 + \dots + (p_m^2 - 1)/8}_{\alpha_m}$$
$$\equiv (p_1^2 \dots p_1^2 \dots p_n^2 \dots p_m^2 - 1)/8 \pmod 2$$
$$\equiv \left(p_1^{\alpha_1}\right)^2 \dots \left(p_m^{\alpha_m}\right)^2 - 1/8 \pmod 2 \equiv (n^2 - 1)/8 \pmod 2$$

Jadi karena $(-1)^k = (-1)^{(n^2-1)/8}$, sehingga terbukti bahwa $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

vi. Akan dibuktikan $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{(a-1)}{2}\frac{(n-1)}{2}}$ jika $\gcd(a, n) = 1$, $a > 0$, a ganjil, dimana

$$a = p_1 p_2 \dots p_k$$
$$n = q_1 q_2 \dots q_l$$

dengan $1 \le i \le k$ untuk setiap p_i dan $1 \le j \le l$ untuk setiap q_j merupakan bilangan prima, dengan demikian pangkat bilangan prima telah diuraikan, sehingga

$$\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{k_1 k_2}$$

Dimana $k_1 = \sum_{i=1}^{k} \frac{p_i - 1}{2} \equiv (a-1)/2 \pmod 2$ dan $k_2 = \sum_{j=1}^{l} \frac{q_j - 1}{2} \equiv (n-1)/2 \pmod 2$.

Jadi terbukti bahwa $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{(a-1)}{2}\frac{(a-1)}{2}}$.

Menentukan nilai dari simbol Jacobi dapat juga dicari dengan Teorema 14, dengan syarat bahwa m dan n merupakan bilangan ganjil positif.

Teorema 13 [3] *Untuk dua bilangan ganjil positif m dan n,* $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$

Bukti:

Akan dibuktikan bahwa untuk dua bilangan ganjil positif m dan n diperoleh

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$$

Karena $\left(\frac{m}{n}\right)$ dan $\left(\frac{n}{m}\right)$ mempunyai nilai ± 1 maka $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right)$.

Pengujian bilangan prima pada metode *Solovay-Strassen* menggunakan definisi Euler pseudoprima. Sebelum mengetahui definisi dari Euler pseudoprima, perlu diketahui dahulu definis pseudoprima. Teorema 8 memberikan persamaan berikut,

$$b^{(n-1)/2} \equiv 1 \pmod n \qquad (1)$$

sehingga pseudoprima didefinisikan sebagai berikut.

Definis 14 [3] *Jika n adalah Bilangan bulat positif ganjil yang memiliki minimal dua faktor prima dan terdapat b dengan* $gcd(b, n) = 1$ *yang mematuhi persamaan (1), maka n disebut pseudoprima pada b.*

Dimana jika n merupakan bilangan prima maka teorema 9 memberikan,

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

dimana $\left(\frac{b}{n}\right)$ adalah simbol Jacobi, dengan demikian definisi Euler pseudoprima adalah,

Definisi 15 [3] *Bilangan bulat positif ganjil yang memiliki minimal dua faktor prima (yaitu n) yang lulus uji persamaan (2) untuk basis b disebut Euler pseudoprima untuk basis b.*

Definisi 15 menyatakan bahwa n dapat dikatakan mungkin prima jika n dapat lulus uji persamaan $\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} (\mathrm{mod}\, n)$ untuk basis b. Jika n tidak lulus uji persamaan $\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} (\mathrm{mod}\, n)$ untuk b, maka n komposit. Pernyataan Definisi 14 dan 15 saling mendukung, dimana jika n merupakan Euler pseudoprima maka n merupakan pseudoprima. Sebagaimana disebutkan pada teorema berikut,

Teorema 16 [3] *Jika n merupakan Euler pseudoprima untuk basis b, maka n merupakan pseudoprima untuk basis b.*

Bukti: Akan ditunjukkan jika persamaan (2) berlaku maka persamaan (1) juga berlaku,

$$\left(b^{(n-1)/2}\right)^2 \equiv \left(\frac{b}{n}\right)^2 (\mathrm{mod}\, n)$$
$$b^{n-1} \equiv 1 (\mathrm{mod}\, n)$$

Jika n bilangan komposit ganjil, maka akan ditunjukkan bahwa persamaan (2) tidak lulus uji paling sedikit 50% dari semua basis $b \in (\mathbb{Z}/n\mathbb{Z})^*$.

Akan ditunjukkan basis b_1 lulus uji persamaan (2) dan basis b_2 tidak lulus uji persamaan (2), maka untuk basis $b_1 b_2$ akan tidak lulus uji. Jika persamaan (2) berlaku untuk b_1 dan $b_1 b_2$ maka basis $b_1 b_2$ akan tidak lulus uji. Jika persamaan (1) berlaku untuk b_1 dan $b_1 b_2$ maka

$$b_1^{(n-1)/2} \equiv \left(\frac{b_1}{n}\right) (\mathrm{mod}\, n)$$
$$(b_1 b_2)^{(n-1)/2} \equiv \left(\frac{b_1 b_2}{n}\right) (\mathrm{mod}\, n)$$
$$(b_1 b_2)^{(n-1)/2} = b_1^{(n-1)/2} b_2^{(n-1)/2}$$
$$\left(\frac{b_1 b_2}{n}\right) = \left(\frac{b_1}{n}\right)\left(\frac{b_2}{n}\right)$$

Sehingga didapat, $b_2^{(n-1)/2} \equiv \left(\frac{b_2}{n}\right) (\mathrm{mod}\, n)$, jadi jika $b_2^{(n-1)/2} \not\equiv \left(\frac{b_2}{n}\right) (\mathrm{mod}\, n)$ maka, $(b_1 b_2)^{(n-1)/2} \not\equiv \left(\frac{b_1 b_2}{n}\right) (\mathrm{mod}\, n)$. Akan ditunjukkan jika bilangan n komposit dan ganjil, maka terdapat basis b yang gagal uji pada persamaan (1). Jika suatu bilangan komposit dan ganjil n lulus uji persamaan (1) untuk semua basis, maka $\left(\frac{b}{n}\right)^2 \equiv b^{n-1} \equiv 1 (\mathrm{mod}\, n)$. Untuk semua basis b, jadi berdasarkan definisi *Carmichael n* merupakan bilangan *Carmichael n* bebas kuadrat (suatu bilangan dikatakan bebas kuadrat jika bilangan tersebut tidak bisa dibagi oleh kuadrat suatu bilangan $p > 1$). Maka didapat $n = pr$ dengan p adalah bilangan prima dan $\gcd(p, r) = 1$, ambil satu *quadratic non-residue* g dalam $(\mathbb{Z}/p\mathbb{Z})^*$ dan pilih a, maka

$$a \equiv g (\mathrm{mod}\, p)$$
$$a \equiv 1 (\mathrm{mod}\, r)$$

Sehingga berdasarkan *Chines Remainder Theorem* dapat dipilih,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{pr}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{r}\right) = \left(\frac{g}{p}\right)\left(\frac{1}{r}\right) = (-1)(1) = -1$$

Maka untuk semua basis yang lulus persamaan (1), akan didapatkan

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \equiv -1 (\mathrm{mod}\, n)$$

Karena $r|n$ maka $a^{(n-1)/2} \equiv -1 (\mathrm{mod}\, r)$, terjadi kontradiksi dengan $a \equiv 1 (\mathrm{mod}\, r)$, sehingga tidak mungkin semua basis lulus uji persamaan (1), jadi terdapat basis b yang tidak lulus uji. Akan ditunjukkan bahwa jika ada basis b yang tidak lulus uji persamaan (1), maka paling sedikit 50%

basis $b \in (\mathbb{Z}/p\mathbb{Z})^*$ tidak lulus uji, jika $\{b_1, b_2, \dots, b_s\}$ merupakan himpunan semua basis yang lulus uji persamaan (1), maka $\{bb_1, bb_2, \dots, bb_s\}$ merupakan himpunan yang tidak lulus uji persamaan (1) dan besarnya sama dengan besar himpunan $\{b_1, b_2, \dots, b_s\}$, jadi sedikitnya 50% dari semua basis akan tidak lulus uji persamaan (1).

Dengan demikian langkah-langkah untuk menguji suatu bilangan mungkin prima atau komposit pada metode Solovay-Strassen adalah sebagai berikut [3];

1. Menentukan bilangan yang diuji yaitu n (bilangan bulat ganjil yang memiliki minimal dua faktor prima.
2. Memilih suatu bilangan b secara acak sebagai basis, dengan cara mengambil sebarang bilangan bulat ganjil positif yang beradapa pada interval $0 < b < n$.
   Mencari $d = \gcd(b, n)$ dengan menggunakan algoritma Euclid. Algoritma Euclid menggunakan algoritma pembagian pada b dan n. Adapun algoritma pembagian yaitu $n = bq + r$, dimana q disebut hasil bagi dan r disebut sisa. Kemudian algoritma pembagian diulangi untuk hasil bagi dan sisa yang baru, sampai diperoleh sisa nol. Hasil bagi yang tak nol adalah $d = \gcd(b, n)$.
3. Jika $d > 1$ maka n adalah bilangan komposit dan d merupakan faktor yang dapat membagi n, dengan demikian pengujian selesai.
4. Jika $d = 1$ maka n akan diuji dengan menggunakan persamaan (1) terhadap basis b. Jika tidak lulus uji dengan menggunakan persamaan (1) maka n adalah bilangan komposit, pengujian selesai. Namun jika lulus uji dengan menggunakan persamaan (1) maka n bilangan prima, pengujian selesai.

Contoh 17:

Misalkan bilangan yang diuji adalah $n = 524289$ (pada aplikasi metode *Solovay-Strassen* menggunakan bilangan yang berdigit 200). Ambil sebarang basis b misalkan b yang dipilih adalah 4. Setelah menentukan basis, dilanjutkan mencari $d = \gcd(b, n)$ dengan menggunakan algoritma Euclid,

$524289 = 131072\ (4) + 1$

$4 = 4(1) + 0$

Dengan demikian $d = \gcd(4,524289) = 1$. Dari algoritma Euclid $n = 524289$ dan $b = 4$ dapat dibentuk kedalam kombinasi linear yaitu,

$1 = 524289 - 131072(4)$

$0 = 4 - 4(1)$

Didapat,

$0 = 4 - 4(1) = 4 - 4[524289 - 131071(4)] = 4 - 4(524289) + 524288(4)$

$= 524289(4) - 4(524289).$

selanjutnya menguji 524289 terhadap basis 4 dengan menggunakan persamaan

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

Didapatlah nila simbol Jacobi dari $\left(\frac{4}{524289}\right)$ sebagai berikut,

$\left(\frac{4}{524289}\right) = \left(\frac{2}{524289}\right)\left(\frac{2}{524289}\right) = 1$

Dan nilai dari

$4^{(524289-1)/2} (\text{mod } 524289) = 4^{(524288)/2} (\text{mod } 524289) = 4^{393216} (\text{mod } 524289) = 1$

Dengan demikian,

$\left(\frac{4}{524289}\right) \equiv 4^{(524289-1)/2} (\text{mod } 524289) = 1$

Dapat disimpulkan bahwa $n = 524289$ merupakan bilangan prima.

Dikarenakan metode *Solovay-Strassen* digunakan pada bilangan yang jumlah digitnya 200, sehingga kemungkinan tidak lulus uji dapat terjadi, sebagaimana dijelaskan pada teorema berikut,

Teorema 18 [6] *Jika n adalah bilangan ganjil yang memiliki minimal dua faktor prima dan $b = \{1,2,\dots,n-1\}$ maka peluang algoritma Solovay-Strassen menyimpulkan n mungkin prima adalah $\leq \frac{1}{2}$.*

Bukti:

Misal $G(n) = \left\{b \,\middle|\, b \in (\mathbb{Z}/n\mathbb{Z})^* \left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod n\right\}$, pertama akan ditunjukkan bahwa $G(n)$ adalah subgrup $(\mathbb{Z}/n\mathbb{Z})^*$.

i. Jelas bahwa $G(n) \in (\mathbb{Z}/n\mathbb{Z})^*$.

ii. Akan ditunjukkan untuk setiap $a, b \in G(n)$ maka $ab \in G(n)$. Karena $a, b \in G(n)$ maka $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \bmod n$ dan $\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod n$, berdasarkan teorema maka diperoleh,

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \equiv a^{(n-1)/2} b^{(n-1)/2} \pmod n = (ab)^{(n-1)/2} \pmod n.$$

Jadi terbukti bahwa $ab \in G(n)$, yang berarti bahwa $G(n)$ memenuhi sifat tertutup terhadap operasi perkalian.

iii. Jelas bahwa 1 merupakan identitas perkalian pada $(\mathbb{Z}/n\mathbb{Z})^*$, karena $\left(\frac{1}{n}\right) \equiv 1^{(n-1)/2} \pmod n$.

iv. Akan ditunjukkan untuk setiap $b \in G(n)$ terdapat $b^{-1} \in G(n)$ sedemikian sehingga $bb^{-1} = 1$, karena $b \in (\mathbb{Z}/n\mathbb{Z})^*$ maka pasti ada $b^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$. Kemudian akan ditunjukkan bahwa $b^{-1} \in G(n)$, dengan menggunakan teorema 12 poin i, diperoleh.

$$\left(\frac{bb^{-1}}{n}\right) = \left(\frac{b}{n}\right)\left(\frac{b^{-1}}{n}\right)$$

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

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

Kedua ruas dibagi dengan $b^{(n-1)/2}$ maka diperoleh,

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

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

atau

$$\left(\frac{b^{-1}}{n}\right) \equiv (b^{-1})^{(n-1)/2} \pmod n.$$

Yang berarti bahwa $b^{-1} \in G(n)$

Dari pembuktian (i), (ii), (iii) dan (iv) terbukti bahwa $G(n)$ merupakan subgrup dari $(\mathbb{Z}/n\mathbb{Z})^*$. Selanjutnya akan dibuktikan bahwa $|G(n)| \leq \frac{|(\mathbb{Z}/n\mathbb{Z})^*|}{2}$. Berdasarkan Teorema 10 diketahui bahwa subgrup $|G(n)|$ membagi grup $|(\mathbb{Z}/n\mathbb{Z})^*|$, jadi ada dua kemungkinan yang terjadi $|G(n)| = |(\mathbb{Z}/n\mathbb{Z})^*|$ atau $|G(n)| < \frac{|(\mathbb{Z}/n\mathbb{Z})^*|}{2}$.

Akan ditunjukkan bahwa terdapat $b \in (\mathbb{Z}/n\mathbb{Z})^*$, tetapi $b \notin G(n)$. Misalkan $n = p^k q$, dengan p adalah bilangan prima ganjil dan q adalah bilangan bulat ganjil, $k \geq 2$ dan $\gcd(p, q) = 1$. Akan dipilih $b = 1 + p^{k-1}q$, sehingga diperoleh

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p^k q}\right) = \left(\frac{b}{p}\right)^k \left(\frac{b}{q}\right) = 1.$$

Berdasarkan Teorema 4 diperoleh,

$$b^{(n-1)/2} = \left(1 + p^{k-1}q\right)^{(n-1)/2}$$
$$\equiv 1 + \frac{n-1}{2} p^{k-1} q \pmod n$$

Jika $\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod n$, maka diperoleh

$$1 \equiv 1 + \frac{n-1}{2} p^{k-1} q \pmod n$$

$$0 \equiv \frac{n-1}{2} p^{k-1} q \pmod n$$

Artinya $\frac{n-1}{2}p^{k-1}q$ adalah kelipatan n, sehingga dapat ditulis

$n\left|\frac{n-1}{2}p^{k-1}q\right. = p^k q\left|\frac{n-1}{2}p^{k-1}q\right. = p\left|\frac{n-1}{2}\right. = p \equiv 1(\mathrm{mod}\, n)$

Hal ini kontradiksi dengan pernyataa awal bahwa $p \equiv 0(\mathrm{mod}\, n)$, jadi dapat dinyatakan bahwa $\left(\frac{b}{n}\right) \not\equiv b^{(n-1)/2} \,(\mathrm{mod}\, n)$, sehingga $b \in (\mathbb{Z}/n\mathbb{Z})^*$ tetapi $b \notin G(n)$. Dengan demikian disimpulkan bahwa $|G(n)| \leq \frac{|(\mathbb{Z}/n\mathbb{Z})^*|}{2}$. Jadi probabilitas algoritma menyimpulkan kesimpulan yang salah adalah $|G(n)| \leq \frac{|(\mathbb{Z}/n\mathbb{Z})^*|}{2} \leq \frac{|(\mathbb{Z}/n\mathbb{Z})^*|}{2|(\mathbb{Z}/n\mathbb{Z})^*|} \leq \frac{1}{2} = 0{,}5$.

PENUTUP

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa:

Metode *Solovay-Strassen* merupakan metode yang menggunakan percobaan acak. Pada metode ini dibahas teori-teori yang digunakan untuk memperjelas metode *Solovay-Strassen* seperti, definisi dari simbol Legendre (disimbolkan dengan $\left(\frac{a}{p}\right)$) yang juga berkaitan dengan simbol Jacobi (disimbolkan dengan $\left(\frac{b}{n}\right)$). Metode *Solovay-Strassen* menguji bilangan bulat ganjil yang memiliki minimal dua faktor prima yang dinyatakan dengan n, kemudian menentukan basis b yang dipilih secara acak dengan cara mengambil sebarang bilangan bulat positif yang berada pada interval $0 < b < n$. Setelah itu menentukan faktor persekutuan terbesarnya atau $d = \gcd(b, n)$. Jika didapatkan bahwa $d > 1$ maka n komposit. Namun jika didapatkan $d = 1$ maka pengujian dilanjutkan dengan menguji b dan n dengan menggunakan persamaan $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) (\mathrm{mod}\, n)$. Dari persamaan tersebut dicari nilai kesamaan dari persamaan kiri dan kanan. Jika $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) (\mathrm{mod}\, n)$ maka n mungkin prima. Namun jika $\left(\frac{b}{n}\right) \not\equiv b^{(n-1)/2} (\mathrm{mod}\, n)$ maka n komposit.. Jika dalam pengambilan basis secara acak didapatkan bahwa n komposit, maka pengambilan basis secara acak dapat diulangi lagi sampai ditemukan bilangan mungkin prima. Dengan demikian kesimpulan dari hasil uji bilangan bulat positif ada dua kemungkinan yang terjadi yaitu bilangan mungkin prima atau bilangan komposit. Karena terdapat pengulangan yang dilakukan pada metode *Solovay-Strassen* maka peluang kemungkinan salah yang terjadi pada pengujian adalah kurang dari atau sama dengan 0,5. Karena penulis hanya mengkaji metode dari *Solovay-Strassen*, sehingga disarankan bagi pembaca untuk membahas aplikasi metode *Solovay-Strassen*. Dapat juga membahas metode uji bilangan prima yang lain seperti metode *Miller-Rabin*.

DAFTAR PUSTAKA

[1]. Muftie A. *Matematika Alam Semesta Kodetifikasi Bilangan Prima dalam Al-Qur'an*. Bandung: PT. Kiblat Utama; 2014.
[2]. Munir R. *Matematika Diskret*. Bandung: Informatika Bandung; 2012.
[3]. Kromodimoeljo S. *Teori dan Aplikasi Kriptografi*. Jakarta: SPK IT Consulting; 2010.
[4]. Niven, Zuckerman, *and Montgomery*. *An Introduction to the Theory of Number*. Canada: Jhon Wiley & Sons, Inc;1991.
[5]. Judson. *Abstrat Algebra*. Stephen F. Austin State University; 2010.
[6]. Scoof R. Four Primalty testing Algorithm. *Algorithmic Number Theory*. 2008;4:102-104.

SARI PUSPITA : FMIPA UNTAN, Pontianak, MySelfSari@gmail.com
EVI NOVIANI : FMIPA UNTAN, Pontianak, evi_noviani@math.untan.ac.id
BAYU PRIHANDONO : FMIPA UNTAN, Pontianak, beiprihandono@gmail.com