BAB II

DASAR TEORI

Pada Bab II ini akan disajikan beberapa teori yang akan digunakan untuk membahas tentang penerapan skema tanda tangan *Schnorr* pada pembuatan tanda tangan digital, yang meliputi: keterbagian, faktor persekutuan terbesar, algoritma Euclid, kekongruenan, fungsi Euler, akar primitif, grup, grup siklik, Algoritma Euclid yang diperluas, uji bilangan prima, kriptografi, tanda tangan digital dan fungsi *hash*.

A. Keterbagian

Keterbagian merupakan salah satu pokok bahasan dari Teori Bilangan yang berkaitan dengan sifat pembagian dalam matematika. Penjelasan mengenai definisi dan teorema yang berkaitan dengan keterbagian telah diberikan oleh banyak buku dengan berbagai bahasa yang berbeda. Berikut beberapa definisi dan teorema yang menjelaskan tentang keterbagian.

Teorema 2.1 berikut menjelaskan tentang sisa hasil bagi yang diberikan oleh Keng (1982: 2).

Teorema 2.1 (Keng, 1982: 2). *Jika a dan b bilangan-bilangan bulat dengan $b > 0$, maka terdapat bilangan-bilangan bulat q dan r yang memenuhi:*

$$a = qb + r, \text{ dengan } 0 \leq r < b.$$

Selanjutnya, r disebut sisa dari a jika dibagi oleh b.

Selanjutnya, Definisi 2.1 berikut menjelaskan mengenai keterbagian.

Definisi 2.1 (Keng, 1982: 2). *Misal a, b merupakan bilangan bulat. Jika sisa dari a ketika dibagi oleh b adalah nol, dan jika terdapat bilangan bulat c sedemikian sehingga $a = bc$, maka a merupakan kelipatan dari b dan dituliskan $b|a$, dapat dikatakan juga bahwa b membagi habis a.*

Selanjutnya b disebut dengan pembagi a. Jika b tidak membagi a, maka dituliskan $b \nmid a$. Jelas bahwa $1|a$, $b|0$ dan untuk setiap $a \neq 0$, $a|a$. Selanjutnya, jika $b|a$, $b \neq a$ dan $b \neq 1$, maka b disebut pembagi sejati dari a. Berikut ini diberikan beberapa contoh keterbagian suatu bilangan berdasarkan Definisi 2.1.

Contoh 2.1.

(i) Bilangan 5 membagi 30 atau ditulis sebagai $5|30$, karena ada bilangan bulat, yaitu 6, sedemikian sehingga $5.6 = 30$.

(ii) Bilangan 7 membagi -21 atau ditulis sebagai $7|-21$, karena ada bilangan bulat, yaitu -3, sedemikian sehingga berlaku $7.\ -3\ = -21$.

(iii) Bilangan 8 tidak membagi 27 atau ditulis sebagai $8 \nmid 27$, karena tidak ada bilangan bulat k yang memenuhi $8k = 27$. □

Teorema berikut menjelaskan tentang sifat-sifat keterbagian yang telah didefinisikan pada Definisi 2.1.

Teorema 2.2 (Keng, 1982: 2). *Misalkan a, b, c, d, e merupakan bilangan bulat, dan $b, c \neq 0$, sehingga berlaku:*
(i) Jika $b|a$ dan $c|b$ maka $c|a$;
(ii) Jika $b|a$ maka $bc|ac$;
(iii) Jika $c|d$ dan $c|e$ maka untuk suatu bilangan bulat m dan n, $c|dm + en$;
(iv) Jika b merupakan pembagi sejati dari a , maka $1 < b < |a|$.

Bukti:

(i) Diketahui bahwa $b|a$ dan $c|b$, sehingga berdasarkan definisi, terdapat bilangan bulat d dan e sedemikian sehingga

$$a = bd \text{ dan } b = ce$$

dan didapat

$\Leftrightarrow \quad a = bd$

$\Leftrightarrow \quad a = c(ed)$,

sehingga $c|a$. Jadi, sifat *(i)* terbukti.

(ii) Diketahui bahwa $b|a$, sehingga terdapat bilangan bulat d sedemikian sehingga $a = bd$

$\Leftrightarrow \quad ac = bdc$

$\Leftrightarrow \quad ac = d(bc)$

sehingga $bc|ac$. Jadi, sifat *(ii)* terbukti.

(iii) Diketahui bahwa $c|d$ dan $c|e$, sehingga terdapat bilangan bulat k dan l sedemikian sehingga $d = ck$ dan $e = cl$

$$dm + en = ckm + cln$$
$$= c(km + ln),$$

$dm + en = c(km + ln)$, sehingga $c|dm + en$. Jadi, sifat *(iii)* terbukti.

(iv) Diketahui bahwa b pembagi dari a sehingga $b > 0$ dan $b \leq a$, dapat dituliskan : $0 < b \leq a$.

Diketahui juga bahwa b pembagi sejati dari a, sehingga

$\Leftrightarrow \quad 0 < 1 < b < a$

$\Leftrightarrow \quad 1 < b < a$

$\Leftrightarrow \quad 1 < b < a$

$\Leftrightarrow \quad 1 < b < a$

Jadi, sifat (*iv*) terbukti. Jika b merupakan pembagi sejati dari a , maka $1 < b < |a|$. ■

B. Faktor Persekutuan Terbesar/FPB (*Great Common Divisor/gcd*)

Jika terdapat bilangan bulat a dan b dengan $a = b = 0$, maka himpunan faktor persekutuan (pembagi) dari a dan b adalah semua bilangan bulat tak nol. Jika a dan b keduanya tak nol, maka terdapat himpunan bilangan bulat yang anggotanya merupakan pembagi-pembagi dari a dan b, dengan bilangan 1 selalu menjadi anggotanya, dan di antaranya pasti terdapat anggota terbesar dalam himpunan yang merupakan bilangan positif.

Definisi 2.2 (Stark, 1998: 16). *Misalkan a dan b bilangan-bilangan bulat yang tidak sama dengan nol. Jika d adalah bilangan terbesar dari faktor persekutuan a dan b, maka d disebut dengan Faktor Persekutuan Terbesar (Great Common Divisor) dari a dan b, selanjutnya dinotasikan dengan $d = gcd(a, b)$. Jika $d = gcd\ a, b\ = 1$, maka dikatakan a relatif prima dengan b.*

Setelah mengetahui definisi mengenai FPB/*gcd*, selanjutnya akan diberikan sifat-sifat dari FPB melalui dua teorema berikut.

Teorema 2.3 (Stark, 1998: 23). *Misalkan $gcd\ a, b\ = d$ dan k adalah sebarang bilangan bulat, maka:*
(a) $gcd\ a, b + ka\ = gcd(a, b)$
(b) $gcd\ ak, bk\ =\ k\ gcd(a, b)\ , k \neq 0$
(c) $gcd\ \frac{a}{d}, \frac{b}{d}\ = 1$

Teorema yang berkaitan dengan sifat FPB selanjutnya diberikan oleh Keng (1982: 5) sebagai berikut.

Teorema 2.4 (Keng, 1982: 5). *gcd (a,b) memiliki sifat-sifat sebagai berikut:*
(i) Terdapat bilangan bulat x, y sedemikian sehingga $ax + by = gcd(a, b)$
(ii) Jika $e|a$ dan $e|b$, maka $e|gcd(a, b)$

Berikut ini diberikan beberapa contoh dalam mencari faktor persekutuan dan FPB dari suatu bilangan.

Contoh 2.2.

Pembagi dari 3 adalah {1, 3}, sedangkan pembagi dari 6 adalah {1, 2, 3, 6}. Faktor persekutuan dari 3 dan 6 adalah {1, 3}.

Jadi, $gcd\ 3,6\ = 3$. □

Setelah mengetahui Contoh 2.2, selanjutnya diberikan contoh lain dalam mencari faktor persekutuan dan gcd dari dua bilangan yang disajikan pada Contoh 2.3. berikut.

Contoh 2.3.

Pembagi dari 18 adalah {1, 2, 3, 6, 9, 18}, sedangkan pembagi dari 24 adalah {1, 2, 3, 4, 6, 8, 12, 24}. Faktor persekutuan dari 18 dan 24 adalah {1, 2, 3, 6}. Jadi, $gcd\ 18,24\ = 6$. □

C. Algoritma Euclid

Algoritma Euclid biasa digunakan untuk menghitung FPB (*gcd*) dari dua bilangan yang besar. Algoritma ini memudahkan dalam perhitungan FPB dari sembarang bilangan bulat, meskipun bilangan-bilangan bulat tersebut cukup besar.

Everest dan Ward (2006: 36) menjelaskan algoritma Euclid sebagai berikut:

Misalkan diberikan bilangan bulat $a > b > 0$, proses algoritmanya adalah

$$a = q_1 b + r_1 \quad , 0 < r_1 < b$$

$$b = q_2 r_1 + r_2 \ , \ 0 < r_2 < r_1$$

.

.

.

$$r_{n-2} = q_n r_{n-1} + r_n \ , \ 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n \ ,$$

berdasarkan algoritma ini yang disebut sebagai $gcd\ a, b$ adalah r_n,

jadi $gcd\ a, b = r_n$.

Memperjelas algoritma tersebut, berikut ini diberikan contoh penggunaan algoritma Euclid dalam menghitung FPB dari dua bilangan.

Contoh 2.4.

Carilah *gcd* (5767, 4453) !

Penyelesaian:

$5767 = 1 \cdot 4453 + 1314$, maka $gcd\ 5767, 4453 = gcd(4453, 1314)$.

$4453 = 3 \cdot 1314 + 511$, maka $gcd\ 4453, 1314 = gcd(1314, 511)$.

$1314 = 2 \cdot 511 + 292$, maka $gcd\ 1314, 511 = gcd\ 511, 292$.

$511 = 1 \cdot 292 + 219$, maka $gcd\ 511, 292 = gcd\ 292, 219$.

$292 = 1 \cdot 219 + 73$, maka $gcd\ 292, 219 = gcd\ 219, 73$.

$219 = 3 \cdot 73 + 0$, maka $gcd\ 219, 73 = gcd\ 73,0 = 73$.

Jadi, $gcd(5767, 4453) = 73$. □

D. Kekongruenan

Gagasan mengenai kongruensi/kekongruenan sering ditemui dan terjadi dalam kehidupan sehari-hari. Contohnya dalam hitungan hari dalam

seminggu yang merupakan masalah kongruensi dengan modulus 7. Keng (1982: 22) menjelaskan kekongruenan melalui Definisi 2.3 berikut:

Definisi 2.3 (Keng, 1982: 22). *Misalkan k dan m suatu bilangan bulat. Jika $a - b = km$, maka a dan b kongruen modulo m, dan ditulis $a - b \equiv 0 \ (mod\ m)$ atau $a \equiv b \ (mod\ m)$. Jika a dan b tidak kongruen modulo m dituliskan $a \not\equiv b (mod\ m)$.*

Berikut ini diberikan contoh mengenai kekongruenan untuk memperjelas Definisi 2.3 .

Contoh 2.5.

(i) $25 \equiv 1 \ (\text{mod } 4)$, sebab $25 - 1 \ = 24 = 4 \times 6$

(ii) $31 \not\equiv 5 (mod\ 6)$, sebab $31 - 5 \ = 26$ bukan merupakan hasil perkalian dari 6. □

Berikut adalah sifat-sifat fundamental dari kongruensi yang dijelaskan oleh Keng (1982) .

Teorema 2.3 (Keng, 1982: 22). *Misalkan $a, b, c,$ dan m merupakan bilangan bulat.*
(a) $a \equiv a \ (mod\ m)$
(b) Jika $a \equiv b \ (mod\ m)$, maka $b \equiv a \ (mod\ m)$
(c) $a \equiv b, \ b \equiv c \ (mod\ m)$, maka $a \equiv c \ (mod\ m)$

Bukti:

Untuk suatu x, y bilangan bulat

(a) Dari bentuk $a - a = 0$

$\Leftrightarrow$ $a - a = 0 \cdot m$

jadi, terbukti $a \equiv a \ (mod\ m)$.

(b) Diketahui $a \equiv b \ (mod\ m)$ berarti

$$a - b = xm$$

$\Leftrightarrow \quad -a + a - b + b = -a + xm + b$

$\Leftrightarrow \quad 0 - xm = b - a + xm - xm$

$\Leftrightarrow \quad -xm = b - a$

$\Leftrightarrow \quad b - a = (-x)m$

Jadi, terbukti $b \equiv a \ (mod\ m)$.

(c) Jika $a \equiv b \mod m$, $b \equiv c \mod m$, *maka* $a \equiv c \mod m$

$a \equiv b \ (mod\ m)$, berarti $a - b = xm$

$b \equiv c \ (mod\ m)$, berarti $b - c = ym$

$$a - b = xm$$

$\Leftrightarrow \quad a - (c + ym) = xm$

$\Leftrightarrow \quad a - c - ym = xm$

$\Leftrightarrow \quad a - c = ym + xm$

$\Leftrightarrow \quad a - c = (x + y)m$

Jadi, terbukti $a \equiv c \mod m$. ■

Teorema selanjutnya untuk sifat fundamental dari kongruensi adalah sebagai berikut:

Teorema 2.4 (Keng, 1982: 23). *a, b, a_1, b_1 bilangan bulat. Jika $a \equiv b \ (mod\ m)$, $a_1 \equiv b_1 \ (mod\ m)$, maka:*
(i) $a + a_1 \equiv b + b_1$,
(ii) $a - a_1 \equiv b - b_1$,
(iii) $aa_1 \equiv bb_1 \ (mod\ m)$.

Bukti:

$a \equiv b \ (mod\ m)$ berarti $a - b = xm$, x bilangan bulat

$a_1 \equiv b_1 \ (mod\ m)$ berarti $a_1 - b_1 = ym$, y bilangan bulat

Sehingga:

(i) $a - b = xm$

$\Leftrightarrow \quad a_1 + a - b - b_1 = a_1 + xm - b_1$

$\Leftrightarrow \quad a + a_1 - \ b + b_1 \ = a_1 + xm - b_1$

$\Leftrightarrow \quad a + a_1 - \ b + b_1 \ = b_1 + ym + xm - b_1$

$\Leftrightarrow \quad a + a_1 - \ b + b_1 \ = b_1 - b_1 + \ y + x \ m$

$\Leftrightarrow \quad a + a_1 - \ b + b_1 \ = \ y + x \ m$

Jadi, $a + a_1 \equiv b + b_1 (mod\ m)$.

(ii) $a - b = xm$

$a = b + xm$

$\Leftrightarrow \quad a - a_1 = b + xm - a_1$

$\Leftrightarrow \quad a - a_1 = b + xm - (b_1 + ym)$

$\Leftrightarrow \quad a - a_1 = b - b_1 + \ x - y \ m$

$\Leftrightarrow \quad (\ a - a_1) - (b - b_1) = (x - y)m$

Jadi, $a - a_1 \equiv b - b_1 (mod\ m)$.

(iii) $a = b + xm$

$\Leftrightarrow \quad aa_1 = (b + xm)a_1$

$\Leftrightarrow \quad aa_1 = \ b + xm \ (b_1 + ym)$

$\Leftrightarrow \quad aa_1 = bb_1 + ymb + xmb_1 + xmym$

$\Leftrightarrow \quad aa_1 = bb_1 + (ymb + xmb_1 + \ xy \ m)$

$\Leftrightarrow \quad aa_1 - bb_1 = (yb + xb_1 + xy)m$

Jadi, $aa_1 \equiv bb_1 (mod\ m)$. ■

Teorema untuk sifat fundamental dari kongruensi yang terakhir adalah sebagai berikut:

Teorema 2.5 (Keng, 1982: 23). *Misalkan* a, b, c, d *bilangan bulat. Jika* $ac \equiv bd$, $c \equiv d \pmod{m}$ *dan* $gcd\ c, m = 1$, *maka* $a \equiv b \pmod{m}$.

Bukti:

$ac \equiv bd \pmod{m}$ berarti $ac - bd \equiv 0 \pmod{m}$,

$c \equiv d \pmod{m}$ berarti $c - d = 0 \pmod{m}$ dan $gcd\ c, m = 1$,

dari bentuk $a - b\ c + b\ c - d = ac - bd$

$\Leftrightarrow$ $a - b\ c + b\ c - d = ac - bd \equiv 0 \pmod{m}$

$\Leftrightarrow$ $a - b\ c + b\ c - d \equiv 0 \pmod{m}$

$\Leftrightarrow$ $a - b\ c \equiv 0 \pmod{m}$.

Hal ini menunjukkan bahwa $m \mid a - b\ c$. Tetapi karena $gcd\ c, m = 1$ maka $m \mid a - b$, yang berarti $(a - b)$ merupakan kelipatan dari m atau dapat ditulis $a \equiv b \pmod{m}$. ■

E. Fungsi Euler

Fungsi Euler atau disebut juga fungsi phi Euler merupakan fungsi aritmetik. Fungsi Euler berkaitan dengan himpunan residu sederhana modulo *m.* Selanjutnya akan dibahas terlebih dahulu mengenai himpunan residu (sistem residu).

Definisi 2.4 (Stark, 1998: 77). *Misalkan S adalah himpunan residu lengkap* $\pmod{m}$. *Himpunan* S' *yang memuat anggota S yang relatif prima dengan m disebut sistem residu sederhana* $\pmod{m}$.

Contoh berikut merupakan contoh mengenai residu sederhana untuk memperjelas Definisi 2.4.

Contoh 2.6.

Himpunan $\{1, 3, 5, 7\}$ adalah himpunan semua residu sederhana modulo 8, sebab 1, 3, 5, dan 7 masing-masing relatif prima dengan 8. □

Contoh yang diberikan berikut ini masih mengenai residu sederhana.

Contoh 2.7.

Himpunan $\{1, 5\}$ adalah himpunan semua residu sederhana modulo 6, sebab 1 dan 5 relatif prima dengan 6. □

Selanjutnya, diberikan definisi mengenai fungsi Euler sebagai berikut.

Definisi 2.5 (Stark, 1998: 78) Fungsi ϕ Euler. *Untuk $m \geq 1$, misalkan $\phi(m)$ menotasikan banyaknya bilangan bulat dari suatu sistem residu sederhana $(mod\ m)$, maka fungsi dari m ini disebut fungsi ϕ Euler.*

Berikut diberikan contoh mengenai fungsi ϕ Euler, untuk lebih memahami Definisi 2.5.

Contoh 2.8.

(i) Himpunan $\{1, 3, 5, 7\}$ adalah himpunan semua residu sederhana modulo 8, sehingga $\phi\ 8\ = 4$.

*(ii)*Himpunan $\{1, 5\}$ adalah himpunan semua residu sederhana modulo 6, sehingga $\phi\ 6\ = 2$. □

Salah satu sifat fungsi Euler yang berkaitan dengan banyaknya bilangan bulat dari suatu sistem residu sederhana, dijelaskan dalam Teorema 2.6 berikut.

Teorema 2.6 (Stark, 1998: 78). *Jika $m \geq 1$, maka banyaknya bilangan bulat positif yang kurang dari atau sama dengan m dan relatif prima dengan m adalah $\phi(m)$.*

Berikut adalah contoh yang menjelaskan mengenai Teorema 2.6.

Contoh 2.9.

Himpunan residu sederhana modulo 30 adalah $\{1, 7, 11, 13, 17, 19, 23, 29\}$, sebab $1, 7, 11, 13, 17, 19, 23, 29$ relatif prima dengan 30. Banyaknya elemen dari himpunan ini adalah 8, maka dikatakan bahwa $\phi\ 30\ = 8$.

Dapat diperiksa bahwa $\phi\ 1\ = 1,\ \phi\ 3\ = 2,\ \phi\ 4\ = 2,\ \phi\ 5\ = 4,\ \phi\ 7\ = 6$. □

F. Akar Primitif

Suatu bilangan bulat positif m dikatakan memiliki akar primitif a, apabila $a^{\phi\ m}\ \equiv 1(mod\ m)$, dan $a^k \neq 1(mod\ m)$, untuk semua bilangan bulat positif $k < \phi\ m$. Lebih jelasnya, akar primitif didefinisikan sebagai berikut:

Definisi 2.6 (Stark, 1998: 98). *Jika* $gcd\ a, m\ = 1$ *dan* $ord_m(a) = \phi\ m$ *, maka* a *disebut akar primitif dari* m*.*

Lebih jelasnya mengenai akar primitif diberikan beberapa contoh sebagai berikut.

Contoh 2.10.

Akar-akar primitif dari 9 adalah 2 dan 5, karena $\phi\ 9\ = 6$ dan order-order dari 2 dan 5 modulo 9 masing-masing adalah 6 serta $gcd\ 2,9\ = 1\ mod\ 9$ dan $gcd\ 5,9\ = 1\ mod\ 9$. □

Contoh 2.11 berikut akan memperlihatkan suatu bilangan yang tidak memiliki akar primitif.

Contoh 2.11.

Bilangan 8 tidak mempunyai akar primitif, sebab $\phi\ 8\ = 4$ yaitu $\{1, 3, 5, 7\}$ dengan $3^2 \equiv 1(mod\ 8)$, $5^2 \equiv 1(mod\ 8)$ dan $7 \equiv 1(mod\ 8)$. □

G. Grup

Suatu relasi $\Re$ antara himpunan A dan himpunan B adalah subhimpunan dari $A \times B = \ a, b\ \ a \in A, b \in B\}$ atau dapat dituliskan dengan $\Re \subseteq A \times B$. Untuk setiap $a \in A$ dan $b \in B$, a dikatakan berelasi $\Re$ dengan b atau dapat dituliskan $a\,\Re\,b$, jika $(a, b) \in \Re$ (Fraleigh, 2001: 4). Suatu relasi dapat berupa fungsi dan juga bukan fungsi. Relasi $\Re$ antara himpunan A dan himpunan B merupakan fungsi hanya jika, setiap elemen himpunan A berelasi dengan tepat satu elemen himpunan B. Sedangkan relasi $\Re$ bukan merupakan fungsi jika untuk suatu $a \in A$ dan $b, b_1 \in B$ maka terdapat $(a, b) \in \Re$ dan $(a, b_1) \in \Re$.

Misalkan '$*$' adalah relasi antara himpunan $S \times S$ dan himpunan S. Jika relasi $*$ ini merupakan fungsi yang membawa setiap $(a, b) \in S \times S$ untuk dipasangkan dengan suatu elemen dari S, maka relasi ini dapat disebut sebagai operasi biner yang didefinisikan oleh Fraleigh sebagai berikut:

Definisi 2.7 (Fraleigh, 2001: 20). *Suatu operasi biner $*$ pada himpunan S adalah fungsi yang memetakan dari $S \times S$ ke S. Untuk setiap $(a, b) \in S \times S$, elemen $*\ (a, b)$ dari S dinotasikan sebagai $a * b$.*

Selanjutnya diberikan contoh suatu operasi biner yang disajikan pada Contoh 2. 12 berikut ini.

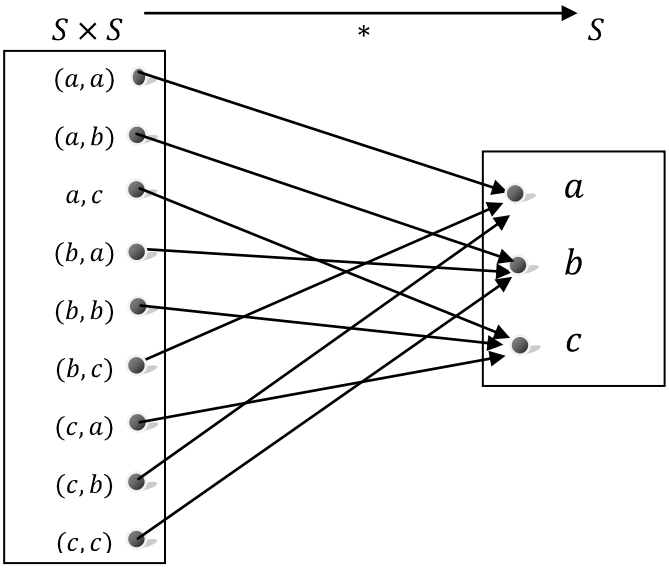
Contoh 2. 12.

Relasi '$*$' yang didefinisikan pada himpunan $S = \{a, b, c\}$ yang disajikan dalam bentuk tabel Cayley berikut:

Tabel 2. 1. Relasi '$*$' pada $S = \{a, b, c\}$

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

merupakan operasi biner, sebab:



Gambar 2. 1. Relasi '$*$' dari $S \times S$ ke S

Berdasarkan Gambar 2.1, terlihat bahwa setiap elemen dari $S \times S$ masing-masing dipetakan ke tepat satu elemen dari S. Sehingga, relasi '$*$' merupakan fungsi.

Relasi '$*$' juga bersifat tertutup, karena dapat dilihat bahwa untuk setiap $a, b \in S$, maka $a * b \in S$. □

Istilah grup pertama kali digunakan oleh Galois sekitar tahun 1830 untuk mendiskripsikan fungsi satu-satu dari himpunan hingga ke himpunan hingga yang dapat dikelompokkan dan membentuk himpunan yang tertutup terhadap komposisi (Gallian, 2013: 2).

Suatu grup adalah suatu himpunan dengan satu operasi biner yang asosiatif, terdapat suatu elemen identitas, setiap elemennnya mempunyai invers (Gallian, 2013: 43). Secara lengkap, definisi grup yang diberikan oleh Gallian sebagai berikut:

Definisi 2.8 (Gallian, 2013: 43). *Misalkan G adalah himpunan dengan operasi biner $*$. Himpunan G disebut grup dengan operasi biner ini jika memenuhi:*

(i) Bersifat asosiatif, yaitu jika $a * b * c = a * (b * c)$ untuk setiap a, b, c di G.

(ii) Terdapat elemen identitas, yaitu terdapat $e \in G$ sedemikian sehingga $a * e = e * a = a$ untuk setiap $a \in G$.

(iii) Setiap $a \in G$ mempunyai invers, yaitu jika terdapat $b \in G$ sedemikian sehingga memenuhi $a * b = b * a = e$

Memperjelas Definisi 2.8 tentang grup, diberikan beberapa contoh grup sebagai berikut (Gallian, 2013:43).

Contoh 2.13.

Himpunan bilangan bulat $\mathbb{Z}$, himpunan bilangan rasional $\mathbb{Q}$ dan himpunan bilangan real $\mathbb{R}$ merupakan grup dengan operasi biner penjumlahan, karena operasi penjumlahan antar elemen di $\mathbb{Z}, \mathbb{Q}$ dan $\mathbb{R}$ bersifat asosiatif, memiliki elemen identitas yaitu 0 dan invers dari a elemen $\mathbb{Z}, \mathbb{Q}$ dan $\mathbb{R}$ adalah $-a$. □

Selanjutnya diberikan Contoh 2.14.

Contoh 2.14.

Himpunan $M = \begin{matrix} a & b \\ c & d \end{matrix} \mid a, b, c, d \in \mathbb{Z}$ dengan operasi penjumlahan matriks merupakan grup. Operasi penjumlahan antar elemen bersifat asosiatif, memiliki elemen identitas yaitu $\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}$ dan invers dari $\begin{matrix} a & b \\ c & d \end{matrix} \in M$ adalah $\begin{matrix} -a & -b \\ -c & -d \end{matrix}$. □

Contoh lain suatu grup dari himpunan bilangan bulat diberikan pada Contoh 2.15.

Contoh 2.15.

Himpunan $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ untuk $n \geq 1$ merupakan grup dengan operasi penjumlahan modulo n. Operasi penjumlahan modulo n antar elemen di $\mathbb{Z}_n$ bersifat asosiatif, memiliki elemen identitas 0 dan untuk setiap $j > 0$ di $\mathbb{Z}_n$, invers dari j adalah $n - j$. □

Selanjutnya, Contoh 2.16 berikut ini akan menunjukkan bahwa himpunan $\mathbb{Z}_p{}^*$ merupakan grup.

Contoh 2.16.

Himpunan $\mathbb{Z}_p{}^* = \{a \in \mathbb{Z}_p \mid a \neq 0, gcd\ a, p = 1\}$ dan p bilangan prima, dengan operasi perkalian modulo p merupakan grup.

Bukti:

$\forall\ a \in \mathbb{Z}_p{}^*$, $a \neq 0$ dan p bilangan prima, sehingga $\mathbb{Z}_p{}^* = \{0 < a < p \mid a \in \mathbb{Z}_p\}$.

$\forall\ a, b \in \mathbb{Z}_p{}^*,\ a \times b = a \times b \mod p \in \mathbb{Z}_p{}^*$ (tertutup)

$\forall\, a, b, c \in \mathbb{Z}_p{}^*$ memenuhi $a \times b \times c = a \times b \bmod p \times c \bmod p$

$= a \bmod p \times (b \bmod p \times c \bmod p)$

$= a \bmod p \times b \times c \bmod p$

$= a \times b \times c$ (asosiatif)

$\exists\, 1 \in \mathbb{Z}_p{}^*$ sedemikian sehingga $\forall\, a \in \mathbb{Z}_p{}^*$, $a \times 1 = a$. Jadi, elemen identitas di $\mathbb{Z}_p{}^*$ adalah bilangan 1. (memiliki elemen identitas)

$\forall\, a \in \mathbb{Z}_p{}^*$ invers dari a adalah a^{-1} dengan $a \times a^{-1} = 1 \bmod p$.

(memiliki invers) ■

Setiap grup pasti mempunyai sub-subhimpunan. Di antara sub-subhimpunan dari suatu grup G, terdapat suatu subhimpunan yang memenuhi aksioma-aksioma grup dan grup yang demikian disebut sebagai subgrup dari G. Definisi 2.9 berikut menjelaskan mengenai subgrup dari grup G.

Definisi 2.9 (Gallian, 2013: 61). *Jika subhimpunan H dari grup G merupakan grup dengan operasi yang sama pada G, maka H disebut subgrup dari G.*

Memperjelas Definisi 2.9, diberikan beberapa contoh subgrup sebagai berikut.

Contoh 2.17.

Grup $(\mathbb{Z}, +)$ merupakan subgrup dari grup $(\mathbb{Z}, +)$ itu sendiri. Grup $(\mathbb{Q}, +)$ merupakan subgrup dari grup $(\mathbb{Q}, +)$. □

Berikut contoh lain suatu subgrup dari grup dengan operasi modulo.

Contoh 2.18.

Grup $U\ 10\ = \{a \in \mathbb{Z}_{10} | \ gcd\ a, 10\ = 1\} = \{1,3,7,9\}$ memiliki subgrup $3\ = \{3^n, n \in \mathbb{Z}\}$.

$3^1 = 3,\ 3^2 = 9,\ 3^3 = 7,\ 3^4 = 1,\ 3^5 = \ 3^4 \cdot 3 = 1.3 = 3,\ 3^6 = 3^4 \cdot 3^2 = 9,$ dan seterusnya. Oleh karena itu $3\ =\ 1,3,7,9\ = U(10)$, sehingga $3 \subseteq U(10)$ dan 3 memenuhi aksioma-aksioma sebagai grup yaitu operasi antar elemennya bersifat asosiatif, memiliki elemen identitas bilangan 1 dan invers dari setiap elemennya yaitu, $1^{-1} = 1, 3^{-1} = 7,\ 7^{-1} = 3,$ dan $9^{-1} = 9$. □

Selanjutnya, contoh berikut ini menunjukkan suatu subgrup dari grup $\mathbb{Z}_p{}^*$.

Contoh 2.19.

Himpunan $\mathbb{Z}_q{}^*$ dengan operasi perkalian modulo q dan $\mathbb{Z}_q{}^* \subset \mathbb{Z}_p{}^*$, merupakan subgrup dari $\mathbb{Z}_p{}^*$, karena $\mathbb{Z}_q{}^* \subset \mathbb{Z}_p{}^*$ dan $\mathbb{Z}_q{}^*$ dengan operasi perkalian modulo q memenuhi aksioma-aksioma dari grup. □

H. Grup Siklik

Berdasarkan Contoh 2.18, dapat dituliskan secara umum bahwa, jika G adalah grup, maka grup $a\ =\ a^n\ n \in \mathbb{Z}\}$ dengan $a \in G$ merupakan subgrup dari G (Gallian, 2013: 65). Subgrup dari grup G yang demikian disebut sebagai subgrup siklik. Subgrup juga merupakan grup, oleh karena itu subgrup siklik juga dapat disebut sebagai grup siklik yang didefinisikan sebagai berikut.

Definisi 2.9 (Gallian, 2013: 77). *Suatu grup G disebut siklik jika terdapat elemen a di G yang memenuhi $G = \{a^n \,|n \in \mathbb{Z}\}$. Selanjutnya, elemen a disebut generator dari G.*

Grup G juga dapat disebut sebagai grup yang dibangkitkan oleh a dan dituliskan dengan $G = \langle a \rangle$. Berikut ini diberikan beberapa contoh grup siklik.

Contoh 2. 20.

Grup $\mathbb{Z}_7^*$={1, 2, 3, 4, 5, 6} dengan perkalian adalah grup siklik dengan generator 3 atau 5. Dikarenakan $1 = 3^6$, $2 = 3^2$, $3 = 3^1$, $4 = 3^4$, $5 = 3^5$, $6 = 3^3$ atau $1 = 5^6$, $2 = 5^4$, $3 = 5^5$, $4 = 5^2$, $5 = 5^1$, $6 = 5^3$. □

Contoh 2. 21 berikut sedikit menjelaskan mengenai generator dari suatu grup siklik.

Contoh 2. 21.

Diberikan suatu grup G={1, a, a^2, a^3,..., a^n}. Generator dari grup tersebut adalah elemen yang memiliki pangkat yang saling prima dengan order G. Misalnya G = {1 , a, a^2, a^3,..., a^{17}}. Order G adalah 18, maka generator dari G adalah a, a^5, a^7, a^{11}, a^{13}, a^{17}. □

Selanjutnya, Teorema 2.7 berikut memberikan beberapa sifat-sifat dasar dari grup siklik.

Teorema 2.7 (Gallian, 2013: 82) *Suatu grup siklik memiliki beberapa sifat-sifat dasar sebagai berikut:*

(i) Setiap grup siklik pasti Abelian
(ii) Subgrup dari grup siklik pasti siklik
(iii) Jika $|a| = n$, maka banyaknya elemen subgrup dari a adalah pembagi dari n
(iv) Untuk suatu pembagi positif k dari n, grup a memiliki tepat satu subgrup yang memiliki banyak elemen k yaitu $a^{n/k}$.

I. Algoritma Euclid yang Diperluas

Algoritma Euclid yang diperluas (*Extended Euclidean Algorithm*) merupakan perluasan dari Algoritma Euclid. Algoritma ini biasanya dipergunakan dalam menentukan invers suatu anggota dalam grup dengan operasi perkalian modulo. Ingat kembali Algoritma Euclid berikut ini untuk menentukan $gcd(a,b)$ misalkan diberikan bilangan bulat $a > b > 0$, Algoritma Euclidnya sebagai berikut:

$$a = q_1 b + r_1 \quad , 0 < r_1 < b$$

$$b = q_2 r_1 + r_2 \, , \; 0 < r_2 < r_1$$

$$\cdot$$

$$\cdot$$

$$r_{n-2} = q_n r_{n-1} + r_n \, , \; 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n$$

dengan $r_n = gcd(a,b)$.

Selanjutnya, jika ditanyakan invers dari $b \bmod a$ dengan Algoritma Euclid yang Diperluas, maka invers ditentukan melalui penjelasan dan teorema berikut ini (Mirnawati, 2013: 16).

Menggunakan nilai q_j dengan $j = 1, 2, \ldots, n$ seperti pada Algoritma Euclid, didefinisikan:

$$t_j = \begin{cases} 0 & j = 0 \\ 1 & j = 1 \\ t_{j-2} - q_j t_{j-1} & j \geq 2 \end{cases}$$

dan

$$s_j = \begin{cases} 0 & j = 0 \\ 1 & j = 1 \\ s_{j-2} - q_j s_{j-1} & j \geq 2. \end{cases}$$

Berdasarkan pada q_j hasil algoritma Euclid dan pendefinisian t_j dan s_j diperoleh hubungan r_j, t_j dan s_j yang diberikan oleh:

Teorema 2.8. *Jika $j = 0,1, \dots, n$ maka $r_j = s_j a - t_j b$ dengan t_j dan s_j seperti yang didefinisikan dan r_j diperoleh di Algoritma Euclid, mengakibatkan:*

$$\textit{Jika } gcd\ (a, b) = 1 \textit{ maka } b^{-1} = t_j.$$

Berikut contoh penerapan Algoritma Euclid yang diperluas dalam mencari invers dari suatu elemen grup modulo.

Contoh 2. 22.

Diberikan $b = 4567$ elemen dari grup $\mathbb{Z}_{7879}{}^{*}$. Tentukan invers dari 4567 di $\mathbb{Z}_{7879}{}^{*}$!

Penyelesaian:

Langkah pertama adalah mencari j dengan menggunakan algoritma Euclid

$7879 = 1 \times 4567 + 3312, \quad j = 1$

$4567 = 1 \times 3312 + 1255, \quad j = 2$

$3312 = 2 \times 1255 + 802, \quad j = 3$

$1255 = 1 \times 802 + 453, \quad j = 4$

$802 = 1 \times 453 + 349, \quad j = 5$

$453 = 1 \times 349 + 104, \quad j = 6$

$349 = 3 \times 104 + 37, \quad j = 7$

$104 = 2 \times 37 + 30, \quad j = 8$

$37 = 1 \times 30 + 7, \quad j = 9$

$30 = 4 \times 7 + 2, \qquad j = 10$

$7 = 3 \times 2 + 1, \qquad j = 11$

$2 = 2 \times 1 + 0, \qquad j = 12$

Berdasarkan algoritma Euclid tersebut diketahui bahwa $gcd\ 7879, 4567 = 1$, dan $j = 12$ oleh karena itu:

$t_0 = 0$

$t_1 = 1$

$t_2 = t_0 - q_1 t_1 = 0 - 1 \times 1 = -1$

$t_3 = t_1 - q_2 t_2 = 1 - 1 \times (-1) = 2$

$t_4 = t_2 - q_3 t_3 = -1 - 2 \times 2 = -5$

$t_5 = t_3 - q_3 t_3 = 2 - 1 \times \ -5 \ = 7$

$t_6 = t_4 - q_5 t_5 = -5 - 1 \times 7 = -12$

$t_7 = t_5 - q_6 t_6 = 7 - 1 \times (-12) = 19$

$t_8 = t_6 - q_7 t_7 = -12 - 3 \times 19 = -69$

$t_9 = t_7 - q_8 t_8 = 19 - 2 \times -69 = 157$

$t_{10} = t_8 - q_9 t_9 = -69 - 1 \times 157 = -226$

$t_{11} = t_9 - q_{10} t_{10} = 157 - 4 \times \ -226 \ = 1061$

$t_{12} = t1_0 - q_{11} t_{11} = -226 - 3 \times 1061 = -3409$

Jadi, dapat disimpulkan bahwa invers dari $4567\ mod\ 7879$ adalah $-3409\ mod\ 7879 = 4470\ mod\ 7879$, atau dituliskan $4567^{-1} = 4470$.

J. Uji Bilangan Prima

Sebagian besar sistem kriptografi kunci publik, biasanya menggunakan bilangan prima sebagai pembentuk kunci. Salah satu cara untuk menguji suatu bilangan merupakan bilangan prima atau bukan adalah dengan menggunakan pengujian Lucas-Lehmer (Vembrina, 2013: 6) yang berdasarkan pada teorema berikut .

Teorema 2.9. *Jika ada a yang lebih kecil dari p dan lebih besar dari* 1 *sehingga:*

$$a^{p-1} \equiv 1 \ (mod\ p)$$

dan

$$a^{(p-1)/q} \not\equiv 1 \ (mod\ p)$$

untuk semua faktor prima q dari $p-1$, maka p adalah bilangan prima. Jika tidak ada a yang memenuhi kondisi tersebut, maka p bukan bilangan prima.

Bukti untuk Teorema 2.9 tersebut dapat dilihat pada jurnal penelitian yang ditulis oleh Vembrina (2013: 6).

Berikut diberikan contoh penerapan Teorema 2.8 dalam menentukan suatu bilangan adalah bilangan prima.

Contoh 2. 23.

Apakah p =103 merupakan bilangan prima?

Penyelesaian:

Misalkan diambil nilai $a = 6$ yang memenuhi $1 < 6 < 103$

$$a^{p-1} \equiv 1 \ (mod\ p)$$

$$6^{103-1} \equiv 6^{102} \equiv 1 \ (mod\ 103).$$

$$6^{103-1} \equiv 1 \ (mod\ 103).$$

$p - 1 = 102 = 2 \times 3 \times 17$, maka semua faktor prima dari $p - 1$ adalah $2, 3$ dan 17 , sehingga didapat:

$6^{(103-1)/2} = 6^{51} \equiv 102 \not\equiv 1 \ (mod\ 103\ )$

$6^{(103-1)/3} = 6^{34} \equiv 46 \not\equiv 1 \ (mod\ 103\ )$

$6^{(103-1)/17} = 6^{6} \equiv 100 \not\equiv 1 \ (mod\ 103\ ).$

Jadi, karena ada $a = 6$ yang memenuhi $6^{103-1} \equiv 1 \ (mod\ 103)$ dan $6^{(103-1)/q} \not\equiv 1 \ (mod\ 103)$ untuk semua q faktor prima dari $p - 1 = 102$, maka menurut pengujian Lucas-Lehmer, 103 merupakan bilangan prima. □

K. Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, yaitu *cryptos* yang berarti *secret* (rahasia), sedangkan *graphien* artinya *writing* (tulisan). Jadi secara asal bahasa kriptografi berarti *secret writing* (tulisan rahasia). Menurut Menezes (1997: 4) kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.

Sementara itu, tujuan dari kriptografi menurut Menezes (1997: 4) adalah sebagai berikut:

i. Kerahasiaan (*confidentiality*)

   Kerahasiaan merupakan suatu layanan yang digunakan untuk menjaga isi dari informasi dari pihak-pihak yang tak berhak untuk mendapatkannya.

ii. Integritas Data (*data integrity*)

   Integritas data merupakan suatu layanan yang menjamin bahwa pesan masih asli, dan belum dimanipulasi oleh pihak - pihak yang tidak berhak.

Realisasi layanan ini di dalam kriptografi, adalah dengan menggunakan tanda tangan digital.

iii. Otentifikasi (*authentication*)

Otentifikasi merupakan suatu layanan yang berhubungan dengan identifikasi. Misalnya, mengidentifikasi suatu kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan.

iv. Nirpenyangkalan (*non-repudiation*)

Nirpenyangkalan merupakan suatu layanan untuk mencegah pihak yang saling berkomunikasi melakukan penyangkalan. Misalkan salah satu dari pihak menyangkal telah mengirim maupun menerima pesan.

Selanjutnya, dalam kriptografi akan sering ditemukan berbagai istilah. Adapun istilah-istilah yang sering digunakan adalah sebagai berikut:

i. Enkripsi

Menurut Mao (2004: 45), enkripsi adalah proses mengubah suatu informasi ke dalam bentuk yang tidak dimengerti. Misalkan *P* adalah himpunan *plaintext*, dan *C* adalah himpunan *ciphertext*, maka fungsi enkripsi *E* memetakan *P* ke *C*, ditulis $E(P) = C$.

ii. *Plaintext*

Plaintext (clear text) adalah informasi yang dapat dibaca dan dimengerti maknanya. *Plaintext* inilah yang merupakan input dalam proses enkripsi.

iii. *Ciphertext*

Ciphertext merupakan output dari proses enkripsi yang bentuknya berupa pesan yang bersandi. Disandikannya suatu pesan adalah agar pesan tersebut tidak dapat dimengerti oleh pihak lainnya.

iv. Dekripsi

Menurut Mao (2004: 45), dekripsi merupakan proses pengembalian dari *ciphertext* manjadi *plaintext*. Misalkan *P* adalah himpunan *plaintext*, dan *C* adalah himpunan *ciphertext*, fungsi dekripsi *De* memetakan *C* ke *P*, ditulis $De(C) = P$.

v. *Chiper*

Cipher adalah metode rahasia untuk mengubah *plaintext* menjadi *ciphertext* (Elizabeth and Denning, 1982: 1). Sedangkan menurut Mao (2004: 45), *cipher* disebut juga algoritma kriptografi yang merupakan kumpulan dari algoritma enkripsi dan dekripsi.

vi. Kunci (*Key*)

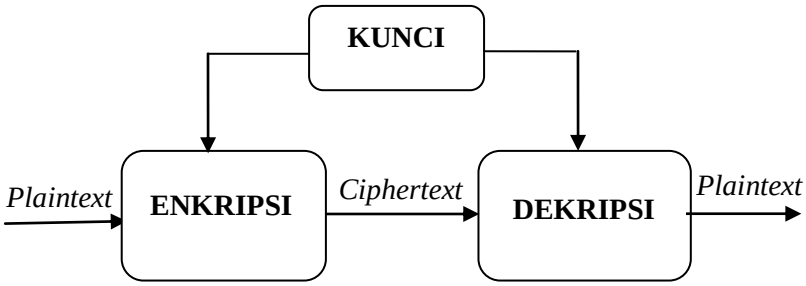
Proses enkripsi dan dekripsi memerlukan suatu kunci (*key*) yang digunakan untuk mentransformasi proses pengenkripsian dan pendekripsian pesan. Biasanya, kunci berupa deretan bilangan maupun string.

vii. Sistem Kriptografi Kunci Simetri dan Kriptografi Kunci Publik

Sistem kriptografi merupakan kumpulan yang terdiri dari *plaintext*, *ciphertext*, kunci, enkripsi serta dekripsi (Stinson, 2006 :1). Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi

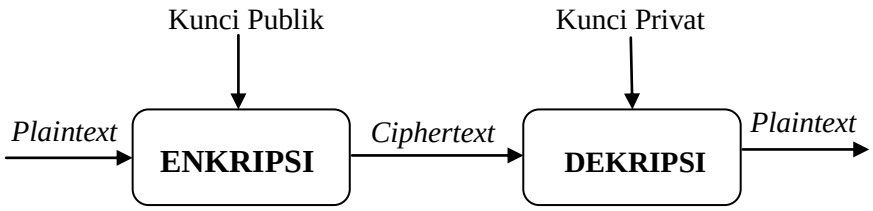
dapat dibedakan menjadi kriptografi kunci simetri dan kriptografi kunci publik.

Sistem kriptografi kunci simetri menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Oleh karena itu, sebelum saling berkomunikasi kedua belah pihak harus melakukan kesepakatan dalam menentukan kunci yang akan digunakan. Keamanan menggunakan sistem ini terletak pada kerahasiaan kunci yang akan digunakan.



Gambar 2. 2. Sistem Kriptografi Kunci Simetri

Sementara itu, pada sistem kriptografi kunci publik, kunci yang digunakan dalam proses enkripsi dan dekripsi berbeda. Sistem ini menggunakan dua buah kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk proses enkripsi, dan kunci privat digunakan untuk mendekripsikan pesan. Kunci publik bersifat tak rahasia, sedangkan kunci privat hanya boleh diketahui oleh penerima pesan.



Gambar 2. 3. Sistem Kriptografi Kunci Publik

viii. Pengirim dan Penerima

Suatu aktivitas komunikasi data, akan melibatkan pertukaran antara dua pihak, yakni pengirim dan penerima. Pengirim adalah pihak yang mengirim pesan kepada pihak lainnya. Sedangkan penerima adalah pihak yang menerima pesan (Rinaldi, 2006 : 4). Saat pengiriman pesan, pengirim tentu menginginkan pesan dapat dikirim secara aman, untuk mengamankannya, pengirim akan menyandikan pesan yang dikirimkan tersebut.

ix. Penyadap adalah orang yang mencoba mengetahui pesan selama pesan dikirim/ditransmisikan.

L. Tanda Tangan Digital

Salah satu pengembangan dari kriptografi kunci publik adalah tanda tangan digital (*digital signature*). Tanda tangan digital (*digital signature*) dapat dijadikan sebagai mekanisme autentikasi pesan yang melindungi dua pihak yang saling bertukar pesan dari pihak ketiga (penyadap). Tanda tangan digital yang valid memberikan keyakinan kepada penerima bahwa pesan yang diterima benar-benar dibuat oleh pengirim asli (Stallings, 2005:378).

Tanda tangan digital di sini bukan merupakan tanda tangan manual yang discan (didigitalisasi). Tanda tangan digital ini berupa deretan bilangan yang dapat diolah dengan perhitungan matematika sedemikian sehingga menghasilkan suatu kesimpulan yang dapat meyakinkan penerima pesan

bahwa pesan masih asli atau tidak. Menurut Jain (2011: 7), syarat suatu tanda tangan digital, yaitu:

a. Bergantung pada pesan yang ditandatangani.
b. Menggunakan informasi tunggal untuk pengirim, untuk mencegah pemalsuan dan kebohongan.
c. Secara relatif mudah dibuat.
d. Secara relatif mudah dikenali dan dibuktikan.
e. Secara perhitungan, sulit untuk dipalsukan dengan pesan baru untuk tanda tangan yang telah dibuat, dan dengan tanda tangan yang dicurangi untuk pesan yang diberikan.

Ada banyak skema pembentukan tanda tangan digital, diantaranya RSA *signature scheme*, ElGamal *signature scheme*, Schnorr *signature scheme*, DSA (*Digital Signature Algorithm*), dan ECDSA (*Elliptic Curve Digital Signature Algorithm*). Diantara skema-skema tersebut tentu masing-masing memiliki kelebihan dan kekurangan, karena itu sampai saat ini masih terus dikembangkan berbagai skema tanda tangan digital.

M. Fungsi *Hash*

Salah satu hal pokok dalam kriptografi modern adalah *hashing*. Inti dari *hashing* ini adalah penggunaan fungsi *hash* atau yang biasa disebut fungsi *hash* satu arah untuk mereduksi pesan asli menjadi suatu *message digest*. Suatu fungsi *hash* menggunakan input berupa pesan/ dokumen yang panjangnya sembarang dan mengeluarkannya menjadi string pendek dengan

panjang tetap (Hoffstein, 2008: 466). Jika suatu pesan yang akan dikirimkan adalah D dengan panjang sembarang, maka pesan tersebut direduksi dengan fungsi *hash* melalui persamaan:

$$H = h(D)$$

string pendek H selanjutnya disebut sebagai nilai *hash* dari D atau *message digest*.

Menurut Hoffstein (2008:466), beberapa kriteria yang harus dipenuhi fungsi *hash* adalah sebagai berikut:

a. Perhitungan nilai *hash* dari D harus cepat dan mudah.
b. Pengembalian nilai *hash* harus sulit. Misalnya, jika diberikan suatu nilai *hash* H, harus sulit ditemukan suatu pesan D yang memenuhi $h(D) = H$.
c. Untuk banyak aplikasi, fungsi *hash* seharusnya tidak bertumbukan (*collision resistant*). Maksudnya, harus sulit untuk menemukan dua pesan berbeda yang nilai *hash*nya sama.

Saat ini sudah banyak berkembang fungsi *hash* yang dapat digunakan untuk menghitung nilai *hash* dari suatu pesan/ dokumen. Beberapa fungsi *hash* satu arah yang cukup sering digunakan saat ini antara lain fungsi *hash* MD5, SHA-1, SHA-256 dan SHA-512. Meski begitu, beberapa metode sederhana untuk menghitung nilai *hash* juga tetap dapat digunakan, seperti dengan metode pembagian dengan sisa hasil bagi (modulo), metode penjumlahan digit, dan juga perpangkatan. Hanya saja, jika dibandingkan dengan fungsi *hash* MD5 maupun SHA metode ini jelas kalah dalam hal keamanan dan kecepatan perhitungan.