BAB II

LANDASAN TEORI

Pada bab ini akan diberikan beberapa definisi, penjelasan, dan teorema yang mendasari pembahasan pada bab-bab berikutnya. Beberapa definisi yang diberikan diantaranya adalah definisi keterbagian, faktor persekutuan terbesar, kekongruenan, grup, dan kriptografi.

A. Keterbagian

Salah satu teorema yang melandasi dalam keterbagian adalah Algoritma Pembagian. Algoritma ini menegaskan bahwa bilangan bulat a dapat "dibagi" oleh bilangan bulat positif b sedemikian sehingga sisanya lebih kecil dari b.

Untuk lebih jelasnya, diberikan teorema dan definisi dari keterbagian berikut.

Teorema 2. 1. (Burton, 1980: hal. 20). *Diberikan* $a, b \in Z$ *dengan* $b > 0$. *Maka terdapat bilangan bulat tunggal* q, $r \in Z$ *sedemikian sehingga* $a = bq + r$ *dan* $0 \leq r < b$.

Berikut ini merupakan contoh dari algoritma pembagian.

Contoh 2. 1.

a) 1987 dibagi dengan 97 memberikan hasil bagi 20 dan sisa 47;

$1987 = 97 \cdot 20 + 47$

b) -22 dibagi dengan 3 memberikan hasil bagi -8 dan sisa 2;

$-22 = 3(-8) + 2$

tetapi $-22 = 3(-7) - 1$ salah karena $r = -1$ tidak memenuhi syarat $0 \leq r < b$.

Definisi 2. 1. (Clark, 2002: hal. 15). *Bilangan d membagi bilangan n jika ada k sedemikian sehingga $n = dk$. (Istilah lainnya adalah: d pembagi dari n, atau d faktor dari n, atau n merupakan kelipatan dari d). Hubungan antara d dan n dinotasikan $d|n$. Notasi $d \nmid n$ berarti d tidak membagi n.*

Berikut merupakan contoh dari Definisi 2. 1 tentang keterbagian.

Contoh 2. 2.

a) $5|30$, karena ada bilangan bulat, yaitu 6, sedemikian hingga $30 = 5 \cdot 6$.

b) $-6|24$, karena ada bilangan bulat, yaitu -4, sedemikian hingga $24 = (-6)(-4)$.

c) $8 \nmid 27$, karena tidak ada bilangan bulat k, sedemikian hingga $27 = 8k$.

Teorema 2.2 berikut menjelaskan tentang sifat keterbagian yang diberikan oleh W. Edwin Clark (2002: hal. 15).

Teorema 2. 2. (Clark, 2002: hal. 15). *Jika n, m, dan d adalah bilangan bulat maka berlaku:*

(1) $d|0$
(2) $0|n \Longrightarrow n = 0$
(3) $1|n$
(4) *(sifat refleksif)* $n|n$
(5) $n|1 \Longrightarrow n = 1 \; atau \; n = -1$
(6) *(sifat transitif)* $d|n \; dan \; n|m \Longrightarrow d|m$
(7) *(sifat perkalian)* $d|n \Longrightarrow ad|an$
(8) *(sifat kanselasi)* $ad|an$ *dan* $a \neq 0 \Longrightarrow d|n$
(9) *(sifat linearitas)* $d|n$ *dan* $d|m \Longrightarrow d|an + bm$ *untuk sebarang bilangan bulat* a *dan* b
(10) *(sifat komparasi) Jika* d *dan* n *positif dan* $d|n$ *maka* $d \leq n$

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

Faktor Persekutuan Terbesar (FPB)/*gcd* dalam pembahasan ini mempunyai makna khusus sebagai suatu kasus dimana sisa dalam Algoritma Pembagian ini adalah nol (0). Untuk lebih jelasnya, dijelaskan melalui definisi dan contoh sebagai berikut.

Definisi 2. 2. (Burton, 1980: hal. 25) *Diberikan bilangan bulat a dan b, dengan salah satunya tidak sama dengan nol. Faktor Persekutuan Terbesar (FPB) dari a dan b, dilambangkan dengan FPB(a,b), adalah bilangan bulat positif d sedemikian hingga berlaku:*
(1) $d \mid a$ dan $d \mid b$,
(2) jika $c \mid a$ dan $c \mid b$, maka $c \leq d$.

Berikut merupakan contoh dari Definisi 2. 2.

Contoh 2. 3. Akan dicari FPB dari -12 dan 30. Pembagi positif dari -12 adalah $1, 2, 3, 4, 6, 12$, sedangkan dari 30 adalah $1, 2, 3, 5, 6, 10, 15, 30$; karenanya, faktor persekutuan dari -12 dan 30 adalah $1, 2, 3, 6$. Karena 6 adalah bilangan bulat terbesar, itu berarti $FPB(-12, 30) = 6$. Sehingga $6| -12$ dan $6|30$, dan $3|12$ dan $3|30$, maka $3 \leq 6$.

Teorema berikut menunjukkan bahwa $FPB(a, b)$ dapat direpresentasikan sebagai kombinasi linear dari a dan b.

Teorema 2. 3. (Burton, 1980: hal. 25) *Diberikan bilangan bulat a dan b, dengan keduanya tidak nol, maka terdapat bilangan bulat x dan y sedemikian sehingga*

$$FPB(a, b) = ax + by.$$

Untuk memperjelas Teorema 2. 3, akan diberikan contoh sebagai berikut.

Contoh 2. 4. Diberikan bilangan bulat yaitu -12 dan 30, maka $FPB(-12, 30)$ dapat direpresentasikan sebagai kombinasi linear:

$$FPB(-12, 30) = 6 = (-12)2 + 30 \cdot 1$$

Definisi 2. 3 berikut menjelaskan mengenai bilangan bulat relatif prima.

Definisi 2. 3. (Burton, 1980: hal. 27) *Dua bilangan bulat a dan b, dengan keduanya tidak sama dengan nol, dapat dikatakan relatif prima jika* $FPB(a,b) = 1$.

Teorema berikut menjelaskan bilangan bulat relatif prima dalam bentuk kombinasi linear.

Teorema 2. 4. (Burton, 1980: hal. 27) *Diberikan a dan b bilangan bulat, dengan keduanya tak nol. Maka a dan b relatif prima jika dan jika terdapat bilangan bulat x dan y sedemikian sehingga* $1 = ax + by$.

Teorema berikut menjelaskan mengenai bilangan relatif prima lebih lanjut.

Teorema 2. 5. (Burton, 1980: hal. 28) *Jika a | bc, dengan* $FPB(a,b) = 1$, *maka a | c.*

Untuk memperjelas Teorema 2. 5, akan diberikan contoh sebagai berikut.

Contoh 2. 5. Diberikan bilangan bulat 3 dan 5 relatif prima, dan bilangan bulat 9 yang merupakan kelipatan dari 3, maka Teorema 2. 5 berlaku. Sebagai contohnya: $3 \mid 5 \cdot 9$, sehingga $3 \mid 9$.

Teorema berikut digunakan untuk menjelaskan definisi dari $FPB(a,b)$.

Teorema 2. 6. (Burton, 1980: hal. 29) *Diberikan a, b bilangan bulat yang keduanya tak nol. Untuk bilangan bulat positif d,* $d = FPB(a,b)$ *jika dan hanya jika*
(1) d | a dan d |b,
(2) jika c | a dan c | b, maka c | d.

C. Algoritma Euclidean

Faktor Persekutuan Terbesar (FPB) dari dua bilangan bulat dapat diperoleh dengan mendata semua pembagi positif dan memilih salah satu faktor terbesarnya. Namun hal ini akan sulit jika bilangan bulat tersebut

sangat besar. Ada langkah yang lebih efisien untuk menentukan Faktor Persekutuan Terbesar (FPB) tersebut, yaitu dengan menggunakan Algoritma Pembagian secara berulang. Metode ini disebut Algoritma Euclidean.

David M. Burton (1980: hal. 31) menjelaskan Algoritma Euclidean sebagai berikut:

Misalkan a dan b dua bilangan bulat yang akan dicari Faktor Persekutuan Terbesarnya (FPB). Karena $FPB(|a|,|b|) = FPB(a,b)$, maka dapat diasumsikan bahwa $0 < b \leq a$. Langkah pertama adalah menerapkan Algoritma Pembagian pada a dan b untuk mendapatkan

$$a = q_1 b + r_1, \qquad 0 \leq r_1 < b$$

Jika $r_1 = 0$, maka $b \mid a$ dan $FPB(a,b) = b$. Ketika $r_1 \neq 0$, b dibagi r_1 untuk memperoleh bilangan bulat q_2 dan r_2 yang memenuhi

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

Jika $r_2 = 0$, maka selesai; jika tidak, lanjutkan seperti sebelumnya untuk mendapatkan

$$r_1 = q_3 r_2 + r_3, \qquad 0 \leq r_3 < r_2$$

Proses pembagian ini berlanjut sampai beberapa kali hingga muncul dengan sisa nol, pada tahap ke $n+1$ dimana r_{n-1} dibagi dengan r_n (sisa nol dapat diperoleh secara cepat atau lambat berdasar $b > r_1 > r_2 > \cdots \geq 0$).

Berikut merupakan sistem persamaannya:

$$a = q_1 b + r_1, \qquad 0 \leq r_1 < b$$

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

$$r_1 = q_3 r_2 + r_3, \qquad 0 \leq r_3 < r_2$$

$$\vdots$$

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

$$r_{n-1} = q_{n+1} r_n + 0.$$

Berdasar algoritma ini $FPB(a, b) = r_n$.

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

Contoh 2. 6. Carilah $FPB(12378, 3054)$!

Penyelesaian:

$12378 = 4 \cdot 3054 + 162$

$3054 = 18 \cdot 162 + 138$

$162 = 1 \cdot 138 + 24$

$138 = 5 \cdot 24 + 18$

$24 = 1 \cdot 18 + 6$

$18 = 3 \cdot 6 + 0$

Jadi, $FPB(12378, 3054) = 6$.

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. Berikut ini merupakan definisi kekongruenan menurut Clark (2002: hal. 31).

Definisi 2. 4. (Burton, 1980: hal. 70) *Misalkan m bilangan bulat positif. Bilangan bulat a dan b dikatakan kongruen modulo m, yang disimbolkan dengan*

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

jika m membagi $a - b$; yang dibuktikan dengan $a - b = kn$, untuk k bilangan bulat.

Untuk memperjelas Definisi 2. 4, akan diberikan contoh sebagai berikut.

Contoh 2. 7.

a) $25 \equiv 1 \pmod 4$, sebab $25 - 1 = 6 \times 4$

b) $1 \equiv -3\ (mod\ 4)$, sebab $1 - (-3) = 4 = 4 \times 1$

c) $3 \equiv 24\ (mod\ 7)$ sebab $3 - 24 = -21 = 7 \times (-3)$

d) $-31 \equiv 11\ (mod\ 7)$ sebab $-31 - 11 = -42 = 7 \times (-6)$

Berikut adalah sifat-sifat fundamental dari kongruensi yang dijelaskan oleh Clark (2002).

Teorema 2. 7. (Clark, 2002: hal. 32) *Kekongruenan merupakan relasi ekuivalen: untuk semua $a, b, c, dan\ m > 0$*
(1) (sifat refleksif) $a \equiv a\ (mod\ m)$
(2) (sifat simetris) $a \equiv b\ (mod\ m) \Longrightarrow b \equiv a(mod\ m)$
(3) (sifat transitif) $a \equiv b\ (mod\ m)$ dan $b \equiv c\ (mod\ m) \Longrightarrow a \equiv c\ (mod\ m)$

Bukti :

Untuk suatu x, y bilangan bulat

(1) Dari bentuk $a - a = 0 \Leftrightarrow a - a = 0 \cdot m$

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

(2) Jika $a \equiv b\ (mod\ m)$ 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 $b \equiv a \ (mod\ m)$.

(3) 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 $b - c = ym$

$$a - b = xm$$

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

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

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

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

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

Teorema 2. 8. (Clark, 2002: hal. 33) *Jika* $a \equiv b \ (mod\ m)$ *dan* $c \equiv d \ (mod\ m)$*, maka*

(1) $a + c \equiv b + d \ (mod\ m)$ *dan* $a - c \equiv b - d \ (mod\ m)$
(2) $ac \equiv bd \ (mod\ m)$
(3) $a^n \equiv b^n \ (mod\ m)$ *untuk semua* $n \geq 1$
(4) $f(a) \equiv f(b) (mod\ m)$ *untuk semua polinomial* $f(x)$ *dengan koefisien bilangan bulat*

Bukti:

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

$c \equiv d \ (mod\ m)$ berarti $c - d = ym$, y bilangan bulat

Sehingga:

(1)

a. $a - b = xm$

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

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

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

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

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

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

b. $a - b = xm$

$a = b + xm$

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

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

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

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

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

(2) $a - b = xm$

$a = b + xm$

$\Leftrightarrow \quad ac = (b + xm)c$

$\Leftrightarrow \quad ac = (b + xm)(d + ym)$

$\Leftrightarrow \quad ac = bd + ymb + xmd + xmym$

$\Leftrightarrow \quad ac = bd + (ymb + xmd + xy \cdot m)$

$\Leftrightarrow \quad ac - bd = (yb + xd + xy)m$

Jadi, terbukti $ac \equiv bd \ (mod\ m)$.

(3) Akan dibuktikan $a^n \equiv b^n \ (mod\ m)$ dengan induksi pada n.

Jika $n = 1$, hasilnya benar dengan asumsi bahwa $a \equiv b \ (mod\ m)$.

Diasumsikan benar untuk $n = k$. Maka $a^k \equiv b^k \ (mod\ m)$. Kemudian akan dibuktikan benar untuk $n = k + 1$, dengan menggunakan $a \equiv b \ (mod\ m)$ dan $ac \equiv bd \ (mod\ m)$, diperoleh $aa^k \equiv bb^k \ (mod\ m)$. Oleh karena itu $a^{k+1} \equiv b^{k+1} \ (mod\ m)$

Jadi terbukti $a^n \equiv b^n \ (mod\ m)$ untuk semua $n \geq 1$.

(4) Dimisalkan $f(x) = c_n x^n + \cdots + c_1 x + c_0$. Akan dibuktikan dengan menggunakan induksi pada n bahwa jika $a \equiv b \ (mod\ m)$ maka

$$c_n a^n + \cdots + c_0 = c_n b^n + \cdots + c_0 \ (mod\ m).$$

Jika $n = 0$, diperoleh $c_0 \equiv c_0 \ (mod\ m)$ dari Teorema 2.7 (1). Diasumsikan benar untuk $n = k$. Maka diperoleh

(*) $$c_k a^k + \cdots + c_1 a + c_0 = c_k b^k + \cdots + c_1 b + c_0 \ (mod\ m).$$

Kemudian akan dibuktikan benar untuk $n = k + 1$, yaitu ditunjukkan $a^{k+1} \equiv b^{k+1} \ (mod\ m)$. Berdasarkan $c_{k+1} \equiv c_{k+1} \ (mod\ m)$ dengan menggunakan $ac \equiv bd \ (mod\ m)$ maka diperoleh

(**) $$c_{k+1} a^{k+1} \equiv c_{k+1} b^{k+1} \ (mod\ m).$$

Kemudian dengan mengaplikasikan $a + c \equiv b + d \ (mod\ m)$ ke (*) dan (**), didapatkan

$$c_{k+1} a^{k+1} + c_k a^k + \cdots + c_0 = c_{k+1} b^{k+1} + c_k b^k + \cdots + c_0 \ (mod\ m).$$

Sehingga terbukti $f(a) \equiv f(b) (mod\ m)$ untik semua polinomial $f(x)$ dengan koefisien bilangan bulat.

E. Fungsi Euler

Bagian ini menjelaskan tentang diperolehnya Generalisasi Euler dari Teorema Fermat. Euler memperluas teorema Ferrmat, yang fokus pada kekongruenan dengan modulo prima, untuk sebarang modulo. Euler memperkenalkan suatu konsep teori bilangan yang penting, yang dideskripsikan sebagai berikut:

Definisi 2. 5. (Burton, 1980: hal. 136) *Untuk* $n \geq 1$, $\phi(n)$ *merupakan banyaknya bilangan bulat positif yang tidak lebih dari n dan relatif prima dengan n.*

Contoh 2. 8. $\phi(30) = 8$; karena bilangan bulat positif yang tidak lebih dari 30 dan relatif prima dengan 30, ada 8 yaitu:

$$1, 7, 11, 13, 17, 19, 23, 29.$$

Teorema 2. 9. (Burton, 1980: hal. 137) *Jika p adalah prima dan* $k > 0$, *maka*

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Contoh 2. 9. Sebagai contoh dari Teorema 2. 9, didapatkan

$$\phi(9) = \phi(3^2) = 3^2 - 3 = 6;$$

enam bilangan bulat yang relatif prima dengan 9 adalah $1, 2, 4, 5, 7, 8$.

Teorema 2. 10. (Burton, 1980: hal. 139) *Jika bilangan bulat* $n > 1$ *mempunyai faktorisasi prima* $n = {p_1}^{k_1} {p_2}^{k_2} \dots {p_r}^{k_r}, maka$

$$\begin{aligned}\phi(n) &= ({p_1}^{k_1} - {p_1}^{k_1 - 1})({p_2}^{k_2} - {p_2}^{k_2 - 1}) \dots ({p_r}^{k_r} - {p_r}^{k_r - 1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

Contoh 2. 11. Dimisalkan menghitung nilai $\phi(360)$. Dekomposisi pangkat prima dari 360 adalah $2^3 \cdot 3^2 \cdot 5$. Dengan menerapkan Teorema 2. 10 diperoleh

$$\phi(360) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96.$$

F. Akar Primitif

Sebelum membahas mengenai akar primitif akan dibahas terlebih dahulu mengenai order. Order sebuah elemen g dari grup G adalah bilangan bulat positif terkecil m sedemikian hingga $g^m = e$, dimana e adalah elemen identitas dari grup G. Jika tidak ada bilangan bulat terkecil seperti m, maka dikatakan bahwa g berorder tak hingga.

Selanjutnya dijelaskan mengenai akar primitif yaitu suatu bilangan bulat positif n dikatakan memiliki akar primitif a, apabila $a^{\phi(n)} \equiv 1\ (mod\ n)$, dan $a^k \not\equiv 1\ (mod\ n)$ untuk semua bilangan bulat positif $k < \phi(n)$. Lebih jelasnya, akar primitif didefinisikan sebagai berikut:

Definisi 2. 5. (Burton, 1980: hal. 159) *Jika $FPB(a,n) = 1$ dan a merupakan order $\phi(n)$ modulo n, maka a adalah akar primitif dari n.*

Lebih jelasnya mengenai akar primitif diberikan beberapa contoh sebagai berikut.

Contoh 2. 12. Akar-akar primitif dari 7 adalah 3 dan 5, karena $\phi\ (7) = 6$ dan order-order dari 3 dan 5 modulo 7 masing-masing adalah 6 serta $FPB(3,7) = 1\ mod\ 7$ dan $FPB(5,7) = 1\ mod\ 7$

G. Uji Bilangan Prima

Biasanya sistem kriptografi kunci publik, sebagian besar 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: hal. 6) yang berdasarkan pada teorema berikut.

Teorema 2. 12. *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.

Berikut diberikan contoh penerapan Teorema 2. 12 dalam menentukan suatu bilangan adalah bilangan prima.

Contoh 2. 13. Misalkan $p = 347$ dan $a = 2$,

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

$2^{347-1} \equiv 2^{346} \equiv 1(mod\ 347)$

$2^{347-1} \equiv 1(mod\ 347)$

Karena $p - 1 = 2 \cdot 173$, maka semua faktor prima dari $p - 1$ adalah 2 dan 173, kemudian dilakukan perhitungan berikut :

$2^{346/2} = 2^{173} \equiv 346 \not\equiv 1(mod\ 347)$

$2^{346/137} = 2^{2} \equiv 4 \not\equiv 1\ (mod\ 347)$

Jadi, karena ada $a = 2$ yang memenuhi $2^{347-1} \equiv 1(mod\ 347)$ dan $2^{(347-1)/q} \not\equiv 1(mod\ 347)$ untuk semua q faktor prima dari $p - 1 = 346$, maka menurut pengujian Lucas-Lehmer, 347 merupakan bilangan prima.

H. Grup

Istilah grup pertama kali dikenalkan oleh Galois sekitar tahun 1840 untuk mendeskripsikan himpunan dari fungsi satu-satu pada himpunan berhingga yang dapat dikelompokkan dalam himpunan tertutup dengan operasi komposisi (Gallian, 2013: hal. 42). Sebelum membahas mengenai grup akan dibahas terlebih dahulu mengenai operasi biner. Operasi biner pada himpunan tidak kosong S adalah pemetaan dari $S \times S$ ke S. Notasi yang digunakan untuk menyatakan operasi biner adalah $+, \times, *, \circ, \otimes$, dan lain sebagainya. Hasil dari sebuah operasi, misalnya $*$, pada elemen a dan b akan ditulis sebagai $a * b$. Selanjutnya akan dijelaskan mengenai operasi biner berdasarkan definisi berikut.

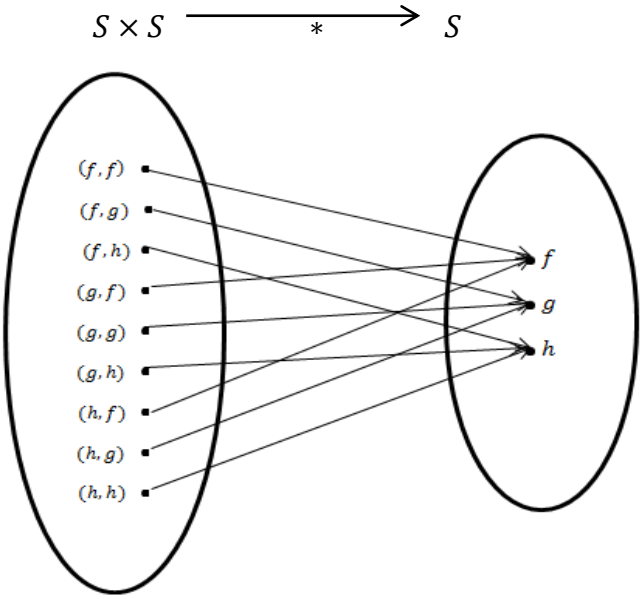
Definisi 2. 6.(Gallian, 2013: hal. 42) *Misalkan G adalah suatu himpunan. Operasi biner pada G adalah suatu fungsi yang memetakan $G \times G$ ke G .*

Contoh 2. 13. Relasi " $*$ " merupakan operasi biner pada himpunan $S = \{f, g, h\}$ yang didefinisikan dalam tabel Caley berikut:

Tabel 2.1. Relasi " $*$ " pada $\boldsymbol{S = \{f, g, h\}}$

$*$	f	g	h
f	f	h	g
g	h	g	f
h	g	f	h

merupakan operasi biner. Hal tersebut dapat dijelaskan sebagai berikut:



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

Berdasarkan Gambar 2. 1 tersebut dapat dilihat bahwa setiap anggota $S \times S$ mempunyai tepat satu pasangan dengan anggota S, sehingga dapat disimpulkan bahwa relasi " $*$ " merupakan fungsi. Relasi " $*$ " juga bersifat tertutup, karena untuk setiap $f, g \in S$, maka $f * g \in S$.

Selanjutnya akan dijelaskan mengenai grup berdasarkan definisi berikut.

Definisi 2. 7. (Gallian, 2013: hal. 43) *Misalkan G adalah himpunan dengan operasi biner *. Himpunan G disebut grup dengan operasi biner ini jika memenuhi:*

(i) Bersifat asosiatif, yaitu $(a * b) * c = a * (b * c)$ *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 terdapat* $b \in G$ *sedemikan sehingga memenuhi* $a * b = b * a = e$

Untuk memperjelas Definisi 2.7 tentang grup, akan diberikan contoh sebagai berikut.

Contoh 2. 14. $G = \{0, 1, 2\}$ dengan operasi biner penjumlahan dalam modulo 3 adalah sebuah grup. Operasi biner penjumlahan modulo 3 didefinisikan sebagai tabel Cayley

berikut :

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

G adalah suatu grup, karena memenuhi Definisi 2. 7.

(i) Tertutup, karena semua hasil operasi penjumlahan selalu menghasilkan nilai yang terdapat di dalam G.

(ii) Asosiatif, operasi penjumlahan modulo 3 bersifat asosiatif yang berarti bahwa $(a + b) + c = a + (b + c)$, untuk semua $a, b, c \in G$.

(iii) Memiliki elemen identitas. Elemen 0 adalah elemen identitas dan memiliki sifat bahwa $a + 0 = 0 + a = a$.

(iv) Untuk semua elemen a didalam G, elemen 0^{-1} adalah 0, elemen 1^{-1} adalah 2, dan untuk elemen 2^{-1} adalah 1, sehingga $0 + 0 = 0$, $1 + 2 = 0$, dan $2 + 1 = 0$.

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. Untuk lebih jelasnya, diberikan definisi berikut.

Definisi 2. 8. (Gallian, 2013: hal. 61) *Jika subhimpunan H dari grup G merupakan grup dengan operasi yang sama pada G, maka H disebut subgrup dari G.*

Untuk memperjelas definisi tentang subgrup, akan diberikan contoh sebagai berikut.

Contoh 2. 15. (Isnaini, 2016: hal. 25) Grup $U\ (9) = \{a \in \mathbb{Z}_9 | FPB\ (a, 9) = 1\} = \{1,2,4,5,7,8\}$ memiliki subgrup $< 2 >= \{2^n, n \in \mathbb{Z}\}$.

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 7,\ 2^5 = 5,\ 2^6 = 1,\ 2^7 = 2^3 \cdot 2^4 = 8 \cdot 7 = 2$, dan seterusnya. Oleh karena itu $< 2 >= \{1,2,4,5,7,8\} = U(9)$, sehingga $< 2 > \subseteq U(9)$ dan $< 2 >$ memenuhi aksioma-aksioma sebagai grup yaitu operasi antar elemennya bersifat asosiatif, memiliki elemen identitas bilangan 1, dan invers dari setiap elemennya yaitu, $1^{-1} = 1,\ 2^{-1} = 5,\ 4^{-1} = 7,\ 5^{-1} = 2,\ 7^{-1} = 4, 8^{-1} = 8$.

I. Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* berarti menyembunyikan, sedangkan *graphia* berarti tulisan. Jadi, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes, 1996: hal. 4).

Sementara itu, tujuan dari kriptografi menurut Menezes (1996: hal. 4) adalah sebagai berikut:

i. Kerahasiaan (*confidelity*).

   Layanan kerahasiaan harus menjadikan pesan yang dikirim menjadi tetap rahasia dan tidak diketahui oleh pihak lain kecuali pihak penerima pesan atau pihak yang memiliki ijin. Biasanya hal tersebut dilakukan dengan menggunakan suatu algoritma matematis yang mampu mengubah data yang ada menjadi sulit dibaca dan dipahami.

ii. Keutuhan data (*data integrity*).

   Merupakan layanan yang dapat mendeteksi atau mengenali jika terjadi perubahan data (penambahan, perubahan, penghapusan) yang dilakuan oleh pihak lain.

iii. Otentikasi (*authentication*).

   Layanan ini berhubungan dengan proses identifikasi keaslian data/informasi serta identifikasi pihak-pihak yang terlibat dalam pengiriman data/informasi.

iv. Anti penyangkalan (*non-repudiation*). Layanan ini mencegah suatu pihak menyangkal aksi yang telah dilakukan sebelumnya.

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

i. Enkripsi

   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. Dekripsi

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 $De(C) = P$.

iii. *Plaintext*

Plaintext merupakan nama lain dari pesan. Pesan adalah data ataupun suatu informasi yang dapat dibaca dan dimengerti maknanya.

iv. *Ciphertext*

Ciphertext adalah suatu bentuk pesan yang bersandi. Disandikannya suatu pesan adalah agar pesan tersebut tidak dapat dimengerti oleh pihak lainnya.

v. *Cipher*

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.

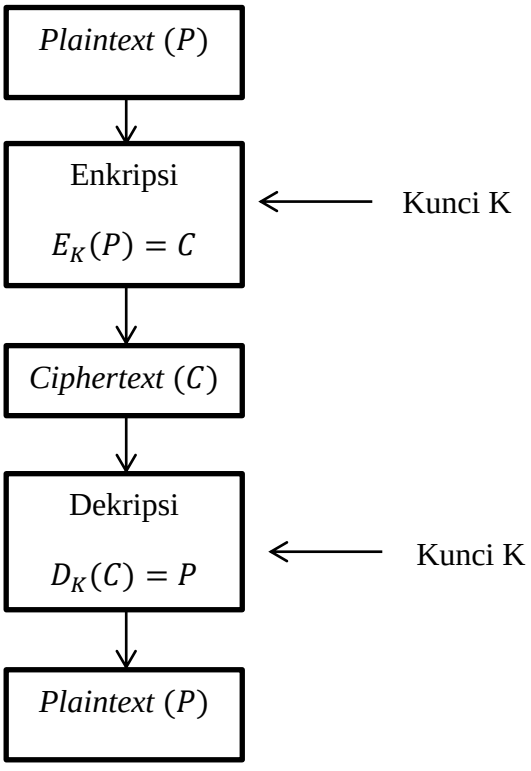
vii. Sistem Kriptografi Kunci Simetri dan Kriptografi Kunci Publik

Sistem kriptografi merupakan kumpulan yang terdiri dari *plaintext, ciphertext*, kunci, enkripsi serta dekripsi.(Stinson, 2006 : hal. 1)

Berdasarkan kunci yang digunakan dalam proses enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetri dan kriptografi kunci publik.

Kriptografi simetris merupakan kriptografi yang menggunakan kunci yang sama dalam 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. Contoh algoritma simetris adalah *Caesar Cipher, Shift Cipher, Substitution Cipher, Affine Cipher*, *Hill Cipher,* dan *Vigenere Cipher*.

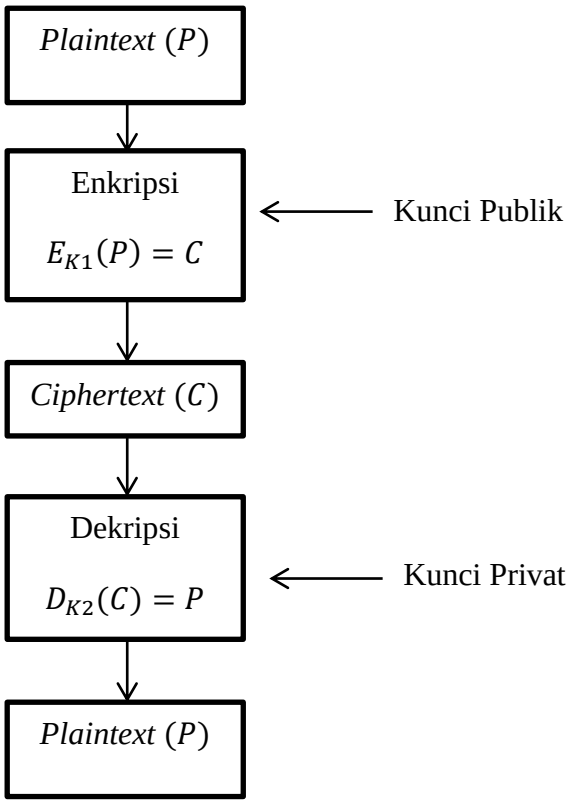
Dibawah ini diberikan skema kriptografi simetri



Gambar 2. 2. Skema Kriptografi Simetri

Sementara kriptografi kunci publik yaitu kunci yang digunakan dalam proses enkripsi dan dekripsi berbeda. Sistem ini terdapat 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. Contoh algoritma asimetris adalah RSA *(Rivest-Shamir-Adleman), ElGamal,* dan DSA *(Digital Signature Algorithm).*

Dibawah ini diberikan skema kriptografi kunci publik



Gambar 2. 3. Skema Kriptografi Kunci Publik

viii. Pengirim dan Penerima

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

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