BAB II
TINJAUAN PUSTAKA

Pada Bab II ini dibahas materi-materi yang mendukung bagian pembahasan masalah. Materi-materi yang dimaksud meliputi operasi uner dan biner, *latin rectangle* dan *latin square*, *groupoid*, *quasi-group*, *system of distinct representative* (SDR), dan kriptografi.

2.1 Operasi Uner dan Biner

Suatu sistem aljabar terdiri dari himpunan obyek dengan satu atau lebih operasi yang didefinisikan di dalamnya. Berdasarkan banyaknya elemen sebarang yang terlibat dalam himpunan, operasi pada aljabar dibagi menjadi beberapa bagian salah satunya adalah operasi uner dan biner. Operasi uner merupakan operasi yang hanya melibatkan satu elemen sebarang dalam himpunan, sedangkan operasi biner adalah operasi yang melibatkan dua elemen sebarang dalam himpunan. Berikut definisi lain dari operasi uner dan biner.

Definisi 2.1.1

Misalkan L adalah sebarang himpunan tak kosong. Suatu fungsi θ dari L ke L disebut operasi uner pada L. Jika θ adalah operasi uner pada himpunan L, maka $\theta(l)$ adalah elemen tunggal di dalam L untuk semua $l \in L$.

(Gupta, 2012)

Contoh 2.1.2

Diketahui $\mathbb{N}$ adalah himpunan semua bilangan asli. Misalkan θ adalah fungsi dari $\mathbb{N}$ ke $\mathbb{N}$ yang didefinisikan oleh $\theta(n) = -n$ untuk semua $n \in \mathbb{N}$. Maka θ adalah operasi uner pada $\mathbb{N}$. ■

Definisi 2.1.3

Misalkan L adalah sebarang himpunan tak kosong. Suatu pemetaan,

$$*: L \times L \to L$$

disebut operasi biner dalam himpunan L. Operasi biner pada himpunan L memetakan tiap-tiap pasangan terurut dalam L ke tepat satu elemen dalam L.

(Bhattacharya, dkk., 1990)

Contoh 2.1.4

Diketahui $\mathbb{Z}$ adalah himpunan semua bilangan bulat. Didefinisikan operasi $*$ pada $\mathbb{Z}$ dengan syarat untuk setiap $a, b \in \mathbb{Z}$ maka $a * b = a + b$. Dapat dilihat dari sifat bilangan bulat bahwa penjumlahan dua bilangan bulat akan selalu menghasilkan bilangan bulat dan tunggal, sehingga dapat dipastikan $a * b = a + b \in \mathbb{Z}$. Dari sini diketahui bahwa operasi $*$ merupakan operasi biner pada $\mathbb{Z}$. ■

2.2 *Latin Rectangle* dan *Latin Square*

Nama "*latin square*" terinspirasi dari makalah matematika yang ditulis oleh Leonhard Euler yang menggunakan karakter latin sebagai simbol. Tentu saja simbol dengan karakter latin ini dapat diubah dengan karakter lain seperti angka. *Latin square* memiliki hubungan yang erat dengan *latin rectangle*, yang mana *latin rectangle* dapat dilengkapkan menjadi *latin square*. dan *latin square* dapat direduksi barisnya menjadi *latin rectangle*. Berikut diberikan definisi mengenai *latin rectangle* dan *latin square*.

Definisi 2.2.1

$W_{k\times n}$ adalah notasi untuk *latin rectangle* berukuran $k \times n$ dengan $k, n \in \mathbb{N}$ dan $k < n$. *Latin rectangle* adalah matriks dengan k buah baris dan n buah kolom yang berisi elemen-elemen $w_1, \dots, w_n$, sedemikian sehingga tiap-tiap elemen disebutkan sekali dalam tiap baris dan kolom (Al-Turky, 2007).

Contoh 2.2.2

Misal diberikan W adalah himpunan bilangan asli kurang dari 6. Dinotasikan $W = \{1, 2, 3, 4, 5\}$.

$$W_{2\times 5} = \begin{bmatrix} 3 & 2 & 5 & 1 & 4 \\ 1 & 4 & 3 & 2 & 5 \end{bmatrix}$$

$W_{2\times 5}$ adalah sebuah *latin rectangle* berukuran 2×5 atas himpunan $W = \{1, 2, 3, 4, 5\}$. ■

Definisi 2.2.3

Latin rectangle berukuran $k \times n$ disebut *latin square* orde n yang dinotasikan $W_{n\times n}$ jika $k = n$ dengan $k, n \in \mathbb{N}$ (Markovski, dkk., 1997). *Latin square* orde n adalah matriks berukuran

$n \times n$ dengan n^2 elemen yang diambil dari suatu himpunan tak kosong W. Elemen-elemen tersebut ditata sedemikian rupa sehingga masing-masing disebutkan sekali dalam tiap kolom dan baris.

(Koscienly, 2002)

Contoh 2.2.4

Misal diberikan W adalah himpunan bilangan asli kurang dari 6. Dinotasikan $W = \{1, 2, 3, 4, 5\}$.

$$W_{5\times5} = \begin{bmatrix} 3 & 2 & 5 & 1 & 4 \\ 1 & 4 & 3 & 2 & 5 \\ 4 & 1 & 2 & 5 & 3 \\ 5 & 3 & 1 & 4 & 2 \\ 2 & 5 & 4 & 3 & 1 \end{bmatrix}$$

$W_{5\times5}$ adalah sebuah *latin square* berukuran 5×5 atas himpunan $W = \{1, 2, 3, 4,5\}$. ■

2.3 *Groupoid*

Groupoid merupakan salah satu bagian dari sistem aljabar yang paling sederhana dan menjadi dasar bagi sistem aljabar lain yang lebih kompleks seperti *quasigroup*, grup, ring dan sebagainya. Berikut diberikan definisi yang lebih jelas mengenai *groupoid*.

Definisi 2.3.1

Groupoid adalah himpunan berhingga P yang di dalamnya didefinisikan sebuah operasi biner $*$ yang memenuhi $a * b \in P$ untuk semua $a, b \in P$ (Yuliawan, 2012).

Hasil operasi biner pada *groupoid* yang memiliki n anggota dapat dinyatakan dalam sebuah matriks berukuran $n \times n$ yang seluruh anggotanya merupakan anggota *groupoid* tersebut baik sebagian maupun keseluruhan (Yuliawan, 2012).

Contoh 2.3.2

Berikut adalah *groupoid* $P = \{1, 2, 3, 4\}$ yang hasil operasi biner anggota-anggotanya dinyatakan sebagai matriks M,

$$M = \begin{bmatrix} 1 & 3 & 2 & 4 \\ 2 & 1 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{bmatrix}.$$

Dari matriks M dapat diketahui bahwa *groupoid* di atas memenuhi operasi biner $*$ sebagai berikut:

$$\begin{array}{llll} 1*1=1, & 1*2=3, & 1*3=2, & 1*4=4, \\ 2*1=2, & 2*2=1, & 2*3=3, & 2*4=4, \\ 3*1=3, & 3*2=4, & 3*3=1, & 3*4=2, \\ 4*1=1, & 4*2=2, & 4*3=3, & 4*4=4. \blacksquare \end{array}$$

(Yuliawan, 2012)

Contoh 2.3.3

Seperti halnya pada Contoh 2.3.2, berikut adalah *groupoid* $P=\{1,2,3,4\}$ yang hasil operasi binernya dinyatakan sebagai matriks N,

$$N=\begin{bmatrix} 1 & 2 & 2 & 1 \\ 2 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 1 & 1 \end{bmatrix}.$$

Dari matriks N dapat diketahui bahwa *groupoid* di atas memenuhi operasi biner * sebagai berikut:

$$\begin{array}{llll} 1*1=1, & 1*2=2, & 1*3=2, & 1*4=1, \\ 2*1=2, & 2*2=1, & 2*3=1, & 2*4=1, \\ 3*1=2, & 3*2=2, & 3*3=2, & 3*4=2, \\ 4*1=1, & 4*2=2, & 4*3=1, & 4*4=1. \end{array}$$

Matriks N menyatakan *groupoid* dengan anggota 1, 2, 3, dan 4 meskipun matriks tersebut tidak memuat elemen 3 dan 4. ■

(Yuliawan, 2012)

2.4 *Quasigroup*

Definisi 2.4.1

Menurut Ochodcova dan Snasel (2001), sebuah *groupoid* $(Q,*)$ disebut *quasigroup* jika untuk setiap $u,v\in Q$ terdapat dengan tunggal $x,y\in Q$ sedemikian sehingga berlaku $u*x=v$ dan $y*u=v$.

Contoh 2.4.2

Diberikan suatu *quasigroup* $(Q,*)$ dengan $Q=\{3,4,5,6,7\}$ dan operasi biner $*$. Operasi biner pada *quasigroup* $(Q,*)$ didefinisikan sebagai berikut:

$$3*3=7, \quad 3*4=6, \quad 3*5=5, \quad 3*6=4,$$

$3 * 7 = 3$, $4 * 3 = 4$, $4 * 4 = 3$, $4 * 5 = 7$,
$4 * 6 = 6$, $4 * 7 = 5$, $5 * 3 = 6$, $5 * 4 = 5$,
$5 * 5 = 4$, $5 * 6 = 3$, $5 * 7 = 7$, $6 * 3 = 3$,
$6 * 4 = 7$, $6 * 5 = 6$, $6 * 6 = 5$, $6 * 7 = 4$,
$7 * 3 = 5$, $7 * 4 = 4$, $7 * 5 = 3$, $7 * 6 = 7$,
$7 * 7 = 6$. ■

Tabel Cayley adalah teknik untuk mempresentasikan operasi biner pada suatu himpunan yang jumlah elemennya berhingga dengan menempatkan semua hasil operasinya ke dalam sebuah *array* berbentuk persegi (Wavrik, 2001). Tabel Cayley ini disebut juga sebagai tabel operasi. Dengan menghilangkan *headline* dan *sideline* pada tabel operasi, diperoleh sebuah *latin square* berukuran $n \times n$ dengan n adalah banyaknya elemen pada suatu himpunan dalam sistem aljabar. Mengingat *quasi-group* adalah bagian dari sistem aljabar, maka tabel Cayley ini dapat diaplikasikan pada *quasigroup*. Oleh karena itu *quasi-group* bisa dikonstruksi dengan menggunakan *latin square.* Berikut adalah teorema yang membahas tentang keterkaitan *groupoid*, *quasigroup*, dan *latin square*.

Teorema 2.4.3

Suatu *groupoid* $Q = \{q_1, \dots, q_n\}$ adalah sebuah *quasigroup* jika dan hanya jika tabel operasinya berupa *latin square*.

(Bell, 2005)

Bukti:

Misal diberikan sebuah *quasigroup* $Q = \{q_1, \dots, q_n\}$ dengan n buah elemen. Berdasarkan sifat *quasigroup*, untuk setiap pasangan q_i dan q_j di dalam Q, dapat ditemukan dua elemen tunggal yakni q_k dan q_l di dalam Q sedemikian sehingga berlaku $q_i q_k = q_j$ dan $q_l q_i = q_j$, dengan $i, j, k, l \in \{1, \dots, n\}$. Dari sini dapat diketahui bahwa untuk tiap-tiap i dan j terdapat k dan l yang tunggal sedemikian sehingga $ik = j$, dan $li = j$. Hal ini ekuivalen dengan pernyataan bahwa untuk setiap baris dan kolom yang saling berpotongan diperoleh suatu entri yang tunggal, sehingga bisa dikonstruksikan sebuah *latin square* dari tabel operasi *quasigroup* Q.

Misal diberikan sebuah *latin square* $B = (b_{ij})$ yang berukuran $n \times n$ dengan $i = 1, \dots, n$ dan $j = 1, \dots, n$, yang mana penomoran pada baris ke-1 sampai ke-n dimulai dari atas ke bawah, dan penomoran pada kolom ke-1 sampai kolom ke-n dimulai dari kiri ke kanan. Didefinisikan $ij = b_{ij}$. Karena B adalah sebuah *latin square*, maka jelas untuk setiap pemilihan baris $\alpha \in \{1, \dots, n\}$ dan sebuah entri pada baris tersebut $\beta \in \{1, \dots, n\}$, selalu dapat ditemukan kolom tunggal $i \in \{1, \dots, n\}$ sedemikian sehingga $\alpha i = \beta$. Hal yang sama juga terjadi dengan memandang α sebagai kolom, akan selalu dapat ditemukan baris tunggal j sedemikian sehingga $j\alpha = \beta$. Hal ini sesuai dengan sifat *quasigroup*, yang mana untuk setiap α dan β elemen *quasigroup* dapat ditemukan i dan j sedemikian sehingga berlaku $\alpha i = \beta$ dan $j\alpha = \beta$, oleh karena itu suatu *quasigroup* dapat dikonstruksikan dari *latin square*.

Karena pembuktian dari kanan dan kiri terpenuhi, maka Teorema 2.4.3 terbukti benar.■

(Bell, 2005)

Contoh 2.4.4

Diberikan *quasigroup* $(Q,*)$ dengan $Q = \{3, 4, 5, 6, 7\}$. Operasi biner pada *quasigroup* ini didefinisikan sebagaimana yang ada pada Contoh 2.4.2. Operasi biner pada *quasigroup* $(Q,*)$ dapat disajikan dalam bentuk tabel operasi berikut:

Tabel 1. *Quasigroup* $(Q,*)$

$*$	3	4	5	6	7
3	7	6	5	4	3
4	4	3	7	6	5
5	6	5	4	3	7
6	3	7	6	5	4
7	5	4	3	7	6

Dengan menghilangkan *headline* dan *sideline* pada Tabel 1 di atas diperoleh *latin square*,

$$Q_{5\times5} = \begin{bmatrix} 7 & 6 & 5 & 4 & 3 \\ 4 & 3 & 7 & 6 & 5 \\ 6 & 5 & 4 & 3 & 7 \\ 3 & 7 & 6 & 5 & 4 \\ 5 & 4 & 3 & 7 & 6 \end{bmatrix}. \blacksquare$$

2.5 *System of Distinct Representative* (SDR)

Sebagaimana yang telah dijelaskan di awal mengenai definisi *latin rectangle* dan *latin square*, dapat diketahui bahwa *latin square* dapat dikonstruksikan dengan menambahkan baris pada *latin rectangle*. Penambahan sebuah baris pada *latin rectangle* sama halnya dengan menemukan SDR untuk himpunan kolom-kolom dalam *latin rectangle*. Berikut diberikan definisi, teorema dan contoh mengenai SDR.

Definisi 2.5.1

Misalkan D himpunan sebarang, $n \in \mathbb{N}$ dan $S_1, S_2, \dots, S_n$ adalah himpunan-himpunan berhingga serta subset dari D. Jika $i = 1, \dots, n$, maka SDR (*system of distinct representative*) dari S_i adalah himpunan $\mathfrak{H} = \{s_1, \dots, s_n\}$ yang memenuhi syarat $s_i \in S_i$ untuk semua i dan $s_1 \neq s_2 \neq \cdots \neq s_n$. Dalam hal ini s_i disebut wakil dari S_i.

(Burton, 1996)

Contoh 2.5.2

Diberikan koleksi himpunan berikut:

$$S_1 = \{5\},\ S_2 = \{1,5\} \text{ dan } S_3 = \{1,4\}.$$

Dengan mengambil satu wakil dari masing-masing himpunan diperoleh SDR dari S_i dengan $i = 1, 2, 3$ adalah $\mathfrak{H} = \{5, 1, 4\}$.

Contoh 2.5.3

Diberikan koleksi himpunan berikut:

$$S_1 = \{4\},\ S_2 = \{2\},\ S_3 = \{2, 3, 4\} \text{ dan } S_4 = \{4,2\}.$$

Ambil 4 sebagai wakil dari S_1 dan 2 sebagai wakil dari S_2, karena wakil dari masing-masing himpunan harus berbeda maka wakil dari S_3 haruslah 3, sedangkan untuk S_4 tidak ditemukan wakil yang memenuhi sehingga tidak ada SDR untuk koleksi himpunan ini.■

Jika $0 \leq j \leq n$, $S = \{S_1, S_2, \dots, S_n\}$ dan $\mathfrak{H}$ eksis, maka gabungan j buah himpunan di dalam S memiliki sedikitnya j elemen yang berbeda, karena setiap S_i memiliki wakil yakni $s_i \in \mathfrak{H}$. Pada tahun 1935, Philip Hall berhasil mencetuskan teorema yang dikenal dengan nama *Hall's Theorem*. Teorema ini menunjukkan bahwa kebalikan dari pernyataan di atas adalah benar, yakni jika gabungan j buah himpunan dari S memiliki sedikitnya j elemen yang berbeda maka SDR untuk S_i ada.

Teorema 2.5.4 (Teorema Philip Hall, 1935)

Misalkan D himpunan sebarang, $S = \{S_1, S_2, \dots, S_n\}$ adalah koleksi n himpunan berhingga dan subset dari D. Dinotasikan $|T(J)| = \left|\cup_{j\in J} S_j\right|$ dengan $J \subseteq \{0,1, \dots, n\}$. SDR di S dikatakan eksis jika dan hanya jika untuk semua J berlaku, $|T(J)| \geq |J|$.

(Donovan, 1999)

Sebelum dilakukan pembuktian, terlebih dahulu diberikan definisi mengenai J kritis. J dikatakan kritis jika $|T(J)| = |J|$, hal ini menunjukkan bahwa setiap elemen di dalam gabungan himpunan berindeks J harus menjadi wakil dari himpunan.

Bukti:

Pembuktian ke kanan pada bagian ini dianggap sudah jelas. Jika $\mathfrak{H}$ adalah SDR dari j buah himpunan sedemikian sehingga $|\mathfrak{H}| = j$, maka terdapat sedikitnya j elemen yang dimiliki oleh gabungan himpunan tersebut, karena jika $s_i \in \mathfrak{H}$ maka $s_i \in S_i$.

Untuk pembuktian ke kiri, dilakukan induksi pada n yang dalam hal ini adalah jumlah himpunan di dalam S. Untuk $n = 1$, diperoleh $S = \{S_1\}$, jika $|J| = 0$ maka jelas bahwa gabungan dari nol himpunan di S memiliki sedikitnya nol elemen, jika $|J| = 1$, dengan mengasumsikan $|T(J)| \geq 1$, maka terdapat sedikitnya satu elemen di dalam gabungan satu himpunan S_1 dalam S, ini berarti bahwa $s_i \in \mathfrak{H}$ sehingga terdapat SDR untuk S. Kemudian diberikan asumsi induksi untuk $|S| = k$ dengan $k \in \mathbb{N}$ dan $k < n$, terdapat SDR untuk S sehingga Teorema 2.5.4 terpenuhi. Pembuktian selanjutnya akan dilakukan dalam dua kasus berbeda sebagai berikut.

Kasus 1

Diberikan koleksi himpunan S sedemikian sehingga J tidak kritis kecuali $J = \{1, \dots, n\}$ dan $J = \emptyset$. Misal dipilih $s \in S_n$, dan $S_i' = S_i \backslash s$ yakni himpunan yang tidak memuat s untuk setiap $1 \leq i \leq n$. Misalkan $J \subseteq \{1, \dots, n-1\}$, maka $|T'(J)| \geq |T(J)| - 1$, sebab maksimum elemen yang dapat diambil dari $T'(J)$ adalah satu. Karena J tidak kritis, maka $|T'(J)| > |J| - 1$, sehingga $|T'(J)| \geq |J|$, dengan menggunakan asumsi induksi terdapat SDR untuk $\{S_1', \dots, S_{n-1}'\}$. Karena s bukan anggota dari himpunan ini maka $s = s_n$ adalah wakil dari S_n, dan diperoleh $\mathfrak{H} = \{s_1, \dots, s_n\}$ adalah SDR dari S.

Kasus 2

Diberikan koleksi himpunan S sedemikian sehingga J kritis kecuali $J = \{1, \dots, n\}$ dan $J = \emptyset$ serta diasumsikan J minimal. Misalkan $K = \{1, \dots, n\} \setminus J$, untuk semua $k \in K$, berlaku $S'_k = S_k \setminus T(J)$, yakni himpunan yang meniadakan semua elemen di $T(J)$. Diperoleh $|T'(K)| = |T(J \cup K)| - |T(J)|$, sehingga S'_k terpisah dari S_j. Dari asumsi diperoleh hasil $|T'(K)| \geq |J \cup K| - |T(J)|$, karena J kritis maka $|T'(K)| \geq |J \cup K| - |J|$. J terpisah dari K sehingga $|T'(K)| \geq |K|$. Dengan asumsi induksi terdapat SDR untuk koleksi himpunan S'_k yang berindeks K. Karena $T'(K)$ terpisah dari $T(J)$, maka SDR-nya terpisah dari SDR milik koleksi himpunan yang berindeks J. Hal ini terjadi karena SDR milik koleksi himpunan yang berindeks J adalah subset dari $T(J)$. Dengan mengkombinasikan kedua SDR diperoleh SDR untuk S. Karena pembuktian dari kanan dan kiri terpenuhi, maka Teorema 2.5.4 terbukti benar. ■

(Bell, 2005)

Contoh 2.5.5

Diberikan koleksi himpunan $S_1 = \{8, 10\}$, $S_2 = \{8, 10, 11\}$ dan $S_3 = \{8, 9\}$. Jika $T(3) = S_1 \cup S_2 \cup S_3$, maka diperoleh $T(3) = \{8, 9, 10, 11\}$, sehingga $|T(3)| = 4$. Berdasarkan Teorema 2.5.4, terdapat SDR untuk S yakni $\mathfrak{H} = \{10, 11, 8\}$, $\mathfrak{H} = \{8, 10, 9\}$, $\mathfrak{H} = \{8, 11, 9\}$, $\mathfrak{H} = \{10, 11, 9\}$ dan $\mathfrak{H} = \{10, 8, 9\}$.

Akibat 2.5.6

Misalkan D adalah himpunan sebarang dan $n \in \mathbb{N}$. $S = \{S_1, S_2, \dots, S_n\}$ adalah koleksi n himpunan berhingga dan subset dari D. Jika terdapat sebuah SDR untuk $n - 1$ buah himpunan di dalam S, maka SDR tersebut dapat diperluas menjadi SDR untuk S dengan syarat Teorema 2.5.4 terpenuhi.

(Bell, 2005)

Contoh 2.5.7

Diberikan koleksi himpunan $S_1 = \{8, 10\}$, $S_2 = \{8, 10, 11\}$ $S_3 = \{8,9\}$ dan $S_4 = \{12\}$. Untuk $J = 3$, diperoleh $T(3) = \{8,9,10,11\}$, sehingga $|T(3)| = 4$. Berdasarkan Teorema 2.5.4, terdapat SDR untuk S yakni $\mathfrak{H} = \{10,11,8\}$, $\mathfrak{H} = \{8,10,9\}$, $\mathfrak{H} = \{8,11,9\}$, $\mathfrak{H} = \{10, 11, 9\}$ dan $\mathfrak{H} = \{10, 8, 9\}$ sebagaimana keterangan pada Contoh 2.5.5. Untuk $J = 4$, diperoleh $T(4) =$

$\{8, 9, 10, 11, 12\}$, sehingga $|T(4)| = 5$. Karena Teorema 2.5.4 terpenuhi maka SDR untuk koleksi himpunan $S = \{S_1, S_2, S_3\}$ dapat diperluas menjadi SDR untuk koleksi himpunan $S = \{S_1, S_2, S_3, S_4\}$ yaitu $\mathfrak{H} = \{10, 11, 8, 12\}$, $\mathfrak{H} = \{8,10,9,12\}$, $\mathfrak{H} = \{8,11,9,12\}$, $\mathfrak{H} = \{10,11,9,12\}$, dan $\mathfrak{H} = \{10,8,9,12\}$.

Teorema 2.5.8

Misalkan D adalah himpunan sebarang dan $n, k \in \mathbb{N}$. $S = \{S_1, S_2, \dots, S_n\}$ adalah koleksi n himpunan berhingga dan subset dari D sedemikian sehingga untuk semua $J \in \{1, \dots, n\}$ berlaku $|T(J)| = |J|$. Misalkan untuk $i \in \{1, \dots, n\}$ berlaku $|S_i| \geq k$, maka jumlah minimal SDR yang berbeda untuk S adalah $k!$ jika $k \leq n$ dan $k(k-1) \dots (k-n+1)$ jika $k > n$.

(Bell, 2005)

Bukti:

Untuk membuktikan teorema ini, digunakan langkah-langkah pembuktian pada Teorema 2.5.4 dengan melakukan modifikasi asumsi induksi pada k, dimulai dari $k = 1$ sampai ke bentuk umumnya. Pembuktian selanjutnya akan dilakukan dalam dua kasus berbeda sebagai berikut:

Kasus 1

Dengan mengasumsikan $|S_n| \geq k$, diperoleh sedikitnya k buah pilihan s_n dari SDR untuk koleksi himpunan S. Untuk setiap $1 \leq i \leq n-1$ dikonstruksikan himpunan $S_i' = S_i \setminus s_n$. Dari asumsi induksi diperoleh $(k-1)!$ buah SDR untuk koleksi himpunan S jika $k \leq n$ dan $(k-1) \dots (k-n+1)$ buah jika $k > n$. Jelas bahwa SDR ini terpisah dari s_n, sehingga dengan menggunakan prinsip perkalian diperoleh $k(k-1) \dots (k-n+1)$ atau $k!$ buah SDR yang berbeda untuk S.

Kasus 2

Pada kasus 2 ini himpunan berindeks J yang merupakan subset dari S adalah kritis, dan diasumsikan minimal. Asumsikan pula $J \neq \{1, \dots, n\}$, karena J kritis maka $k \leq n$. Dari asumsi induksi untuk $|J| \leq n-1$, diperoleh $k!$ buah SDR untuk koleksi himpunan berindeks J. Dengan menggunakan Akibat 2.5.6, SDR untuk koleksi himpunan berindeks J ini dapat diperluas menjadi SDR bagi S. ■

(Bell, 2005)

Contoh 2.5.9

Diberikan koleksi himpunan $S_1 = \{1,2\}$, $S_2 = \{1,2,3\}$ dan $S_3 = \{1,3\}$. Diperoleh $T(3) = \{1,2,3\}$ sehingga $|T(3)| = 3$ dan berlaku $|S_i| \geq 2$ untuk $i = 1,2,3$. Berdasarkan Teorema 2.5.8, terdapat sedikitnya 2! buah SDR berbeda untuk S. Dengan mengambil satu perwakilan dari masing-masing himpunan diperoleh tiga buah SDR untuk S sebagai berikut, $\mathfrak{H} = \{1,2,3\}$, $\mathfrak{H} = \{2,1,3\}$ dan $\mathfrak{H} = \{2,3,1\}$.

2.6 Kriptografi

Definisi 2.6.1

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

(Riyanto, 2007)

Contoh kriptografi dalam kehidupan sehari-hari diantaranya adalah transaksi melalui ATM, *pay television*, komunikasi dengan menggunakan telepon seluler, *barcode* dan sebagainya (Munir, 2004).

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu (Menezes, dkk., 1996).

1. Kerahasiaan, adalah aspek yang digunakan untuk menjaga isi informasi dari siapapun kecuali orang yang memiliki wewenang untuk mengetahuinya. Terdapat banyak sekali pendekatan yang dapat digunakan untuk merahasiakan data, termasuk membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
2. Integritas data, adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjamin integritas data, seseorang atau sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak memiliki wewenang. Bentuk dari manipulasi data antara lain menyisipkan, menghapus,

dan mensubstitusikan data lain ke dalam data yang sebenarnya.

3. Autentikasi, adalah aspek yang berhubungan dengan identifikasi, baik autentikasi pihak-pihak yang terlibat dalam pengiriman data maupun autentikasi keaslian data. Kedua pihak yang terlibat dalam komunikasi harus mengenalkan diri satu sama lain. Informasi yang dikirim harus terbukti keasliannya meliputi asal-usulnya, tanggal asal, isi informasi, tanggal pengiriman dan sebagainya.
4. *Non-repudiation*, adalah usaha untuk mencegah terjadinya penyangkalan terhadap tanggung jawab atau tindakan pengiriman suatu informasi, dengan kata lain jika pihak pengirim menyangkal telah mengirim suatu pesan, maka harus bisa dibuktikan bahwa pesan yang dikirim berasal dari pengirim tersebut.

Definisi 2.6.2

Enkripsi atau dalam bahasa Inggrisnya *encryption* adalah proses yang dilakukan untuk mengamankan sebuah pesan (disebut *plaintext*) menjadi pesan yang tersembunyi dan tidak dapat dibaca (disebut *ciphertext*). Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah *encipher*.

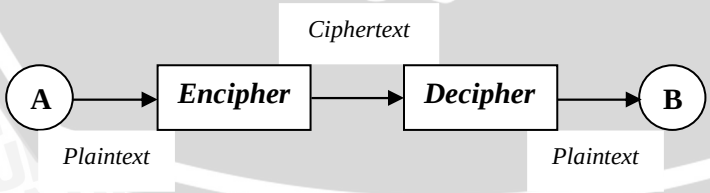
(Sasongko, 2005)

Definisi 2.6.3

Dekripsi atau dalam bahasa Inggrisnya *decryption* adalah proses untuk mengubah *ciphertext* menjadi *plaintext*. Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah *decipher*.

(Sasongko, 2005)

Misalkan A adalah pihak yang mengirimkan pesan dan B adalah pihak yang menerima pesan, alur kriptografi secara umum dapat dijelaskan dalam skema berikut:



Definisi 2.6.4

Parameter yang digunakan dalam proses *encipher* dan *decipher* disebut kunci (Yuliawan, 2012).

Definisi 2.6.5

Algoritma kriptografi atau yang sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan *encipher* dan *decipher* (Riyanto, 2007). Secara umum algoritma kriptografi dibagi menjadi dua jenis yaitu algoritma kunci rahasia dan algoritma kunci publik (Markovski, dkk., 1997).

Algoritma kriptografi modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci (Budiyono, 2004). *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula.

Definisi 2.6.6

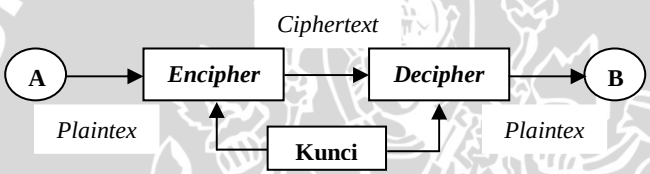
Algoritma kunci rahasia atau biasa disebut algoritma simetris adalah algoritma kriptografi yang menggunakan kunci yang sama untuk proses *encipher* dan *decipher*-nya (Riyanto, 2007). Istilah lain dari algoritma ini adalah algoritma kriptografi konvensional (Andri, 2009).

Keamanan algoritma konvensional tergantung pada kunci (Riyanto, 2007). Membocorkan kunci sama artinya dengan memberikan kesempatan bagi pihak tak berwenang untuk melakukan *encipher* dan *decipher* pada *plaintext* (Ochodcova, 2012). Algoritma kriptografi yang termasuk dalam algoritma konvesional diantaranya adalah (Namiesyva, 2012):

1. *Subtitution Cipher*
   Subtitution cipher adalah algoritma yang mengganti setiap karakter dari *plaintext* dengan karakter lain dalam susunan abjad tanpa adanya perubahan pada susunan abjad asli. Contoh algoritma ini diantaranya *caesar cipher* dan *vigenere cipher*.
2. *Transposition Cipher*
   Transposition cipher adalah algoritma yang mengubah susunan karakter dari *plaintext* tanpa mengganti karakter yang ada dengan karakter yang lain. Contoh algoritma ini adalah *rail fence*.

3. *Block Cipher*
   Block cipher adalah algoritma yang membagi karakter pada *plaintext* menjadi blok dengan ukuran tertentu yang mana setiap blok dikodekan dengan menggunakan kunci yang sama. Empat mode operasi yang lazim diterapkan pada algotitma ini adalah *Electronic Code Book* (*ECB*), *Cipher Block Chaining* (*CBC*), *Cipher Feedback* (*CFC*) dan *Output Feedback* (*OFB*).
4. *Stream Cipher*
   Stream cipher adalah algoritma yang mengkodekan karakter persatuan karakter seperti bit, byte, nible, dan sebagainya. Pada tiap pengkodean satu satuan karakter digunakan kunci yang dibangkitkan dari kunci sebelumnya.

Secara umum, alur algoritma kriptografi konvensional dapat dijelaskan dalam skema berikut:

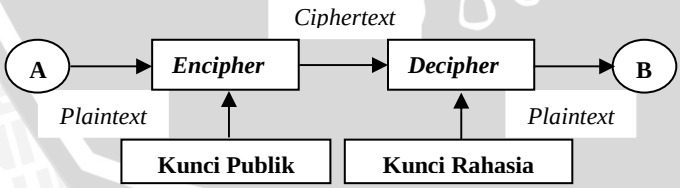


(Riyanto, 2007)

Definisi 2.6.7

Algoritma kunci publik atau yang biasa disebut dengan algoritma kunci asimetris adalah algoritma kriptografi dengan menggunakan kunci yang berbeda untuk proses *encipher* dan *decipher*-nya, yang mana kunci untuk *encipher* dapat diketahui oleh publik tetapi untuk proses *decipher*-nya hanya diketahui oleh pihak yang berwenang (Namiesyva, 2012).

Contoh algoritma kunci publik adalah RSA, ElGamal, McEliece, LUC dan DSA (Riyanto, 2007). Secara umum, alur algoritma kunci publik dapat dijelaskan dalam skema berikut:



(Riyanto, 2007)