BAB III
HASIL DAN PEMBAHASAN

3.1 Mengkonstruksi *Quasigroup* dengan Menggunakan *Latin Square*

Subbab ini membahas tentang salah satu fungsi *latin square* sebagai media untuk membentuk *quasigroup*. Sebagaimana yang telah dijelaskan dalam Teorema 2.4.3 pada bab sebelumnya, terdapat hubungan yang erat antara *groupoid*, *quasigroup*, dan *latin square*. Teorema ini secara implisit memberikan penjelasan bahwa *quasigroup* dapat dinyatakan sebagai *latin square* dan sebaliknya. Secara umum, *quasigroup* tidak memiliki beberapa dari sifat aljabar seperti assosiatif, komutatif, distributif, memuat elemen identitas dan lain-lain. Dari sini dapat ditunjukkan bahwa tabel operasi *quasigroup* adalah sebuah *latin square*.

Kesesuaian inilah yang mendasari ide pengkonstruksian *quasigroup* dengan menggunakan *latin square*. Diantara dasar metode pengkonstruksian yang dapat digunakan adalah modifikasi teorema Marshal Hall. Teorema yang dicetuskan pada tahun 1945 ini menyatakan bahwa setiap *latin rectangle* berukuran $k \times n$ dapat diperluas menjadi *latin rectangle* berukuran $(k+1) \times n$ dengan $k = 0, 1, \dots, n-1$ dan dilengkapkan hingga menjadi *latin square*.

Teorema 3.1.1 (Teorema Marshal Hall, 1945)

Setiap *latin rectangle* W berukuran $k \times n$ dengan $0 \leq k \leq n$, dapat dilengkapkan menjadi sebuah *latin square* berorde n.

(Donovan, 1999)

Bukti:

Untuk kasus $k = 0$ diperoleh hasil yang trivial, begitu juga dengan $k = n$. Oleh karena itu, dalam pembuktian ini diasumsikan bahwa W adalah *latin rectangle* berukuran $k \times n$ dengan $0 < k < n$.

Untuk $1 \leq j \leq n$, misalkan S_j adalah himpunan dari semua $x \in \{1, 2, \dots, n\}$ sedemikian sehingga x tidak muncul di kolom j dalam W. Perhatikan bahwa $|S_j| = n - k$, karena W adalah *latin rectangle* maka setiap elemen akan muncul sekali dalam tiap

baris dan kolom sehingga untuk semua $x \in \{1, 2, \dots, n\}$ dari koleksi himpunan $S_1, S_2, \dots, S_n$ masing-masing akan muncul sebanyak $(n-k)$ kali. Dari sini akan ditunjukkan bahwa terdapat sebuah SDR $\mathfrak{H} = \{s_1, s_2, \dots, s_n\}$ untuk koleksi himpunan $S_1, S_2, \dots, S_n$ dan sebagai akibatnya, *latin rectangle* $W \cup \{(k+1,1,s_1), (k+1,2,s_2), \dots, (k+1,n,s_n)\}$ berukuran $(k+1) \times n$ adalah hasil perluasan dari *latin rectangle* W.

Asumsikan bahwa SDR tidak ada, sehingga terdapat $z \in \{1, 2, \dots, n\}$ dan beberapa wakil dari koleksi himpunan $S_{j1}, S_{j2}, \dots, S_{jz}$ sedemikian sehingga $|S_{j1} \cup S_{j2} \cup \dots \cup S_{jz}| < z$. Akan tetapi persamaan $|S_{j1}| + |S_{j2}| + \cdots + |S_{jz}| = z(n-k)$ mengimplikasikan bahwa terdapat $x \in \{1, 2, \dots, n\}$ dari koleksi himpunan $S_{j1}, S_{j2}, \dots, S_{jz}$ yang muncul lebih dari $(n-k)$ kali. Terjadi kontradiksi yang mana seharusnya untuk semua $x \in \{1, 2, \dots, n\}$ dari koleksi himpunan $S_1, S_2, \dots, S_n$ masing-masing muncul sebanyak $(n-k)$ kali. Oleh karena itu SDR harus ada sehingga *latin rectangle* W yang berukuran $k \times n$ dapat diperluas menjadi *latin rectangle* $W \cup \{(k+1, 1, s_1), (k+1, 2, s_2), \dots, (k+1, n, s_n)\}$. Jika $W \cup \{(k+1, 1, s_1), (k+1, 2, s_2), \dots, (k+1, n, s_n)\}$ adalah *latin square* dengan orde n maka pembuktian selesai, jika tidak maka proses di atas diulang dan $W \cup \{(k+1,1,s_1), (k+1,2,s_2), \dots, (k+1,n,s_n)\}$ diperluas menjadi *latin rectangle* berukuran $(k+2) \times n$. Proses ini dilakukan terus-menerus sampai akhirnya diperoleh sebuah *latin square*.■

(Donovan, 1999)

Contoh 3.1.2

Misal diberikan sebuah *latin rectangle* $W_{3\times5}$ dengan $W = \{1, 2, 3, 4, 5\}$ sebagai berikut:

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

Latin rectangle di atas dapat diperluas menjadi sebuah *latin rectangle* berukuran 4×5 dengan menambahkan sebuah baris berisi elemen-elemen 1, 2, 3, 4, dan 5 yang ditata sedemikian

hingga masing-masing kolom memuat elemen yang berbeda. Diperoleh *latin rectangle*,

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

Latin rectangle di atas dapat dilengkapkan menjadi sebuah *latin square* berukuran 5×5 dengan menambahkan sebuah baris berisi elemen-elemen 1, 2, 3, 4, dan 5 yang belum termuat di masing-masing kolom. Diperoleh *latin square*,

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

Untuk mengetahui jumlah kemungkinan *latin square* yang akan dihasilkan dari proses pengkonstruksian, Jordan Bell (2005) memberikan teorema beserta pembuktian yang terkait dengan hal ini sebagai berikut:

Teorema 3.1.3

Misalkan W adalah *latin rectangle* berukuran $k \times n$, terdapat sedikitnya $(n-k)!$ cara untuk menambahkan satu baris pada W sehingga diperoleh suatu *latin rectangle* berukuran $(k+1) \times n$.

Bukti:

Representasikan komplemen dari entri-entri pada kolom ke-i *latin rectangle* $W_{k\times n}$ dengan S_i. Penambahan sebuah baris pada suatu *latin rectangle* ekuivalen dengan menemukan sebuah SDR untuk $S = \{S_1, S_2, \dots, S_n\}$. Jelas bahwa $|S_i| = n-k$. Misalkan $r = n-k$. Dapat diketahui bahwa untuk setiap $x \in \{1, 2, \dots, n\}$ terdapat dengan tepat r buah kolom yang tidak memuat x. Hal ini memenuhi kondisi Teorema 2.5.4 dan masing-masing kolom memiliki r elemen yang berbeda di dalamnya. Sehingga berdasarkan Teorema 2.5.8 (dengan $k \leq n$) terdapat $r! = (n-k)!$ cara untuk menambahkan sebuah baris agar diperoleh suatu *latin rectangle* berukuran $(k+1) \times n$. ■

(Bell, 2005)

Dalam teorema di atas, Jordan Bell secara tidak langsung memberikan penjelasan bahwa proses pembentukan sebuah *latin square* berukuran $n \times n$ atas himpunan yang memiliki n buah elemen akan menghasilkan sedikitnya $n!\,(n-1)!\,(n-2)!\ldots 2!\,1!$ buah *latin square* yang berbeda. Sehingga akan ada minimal $n!\,(n-1)!\,(n-2)!\ldots 2!\,1!$ buah *quasigroup* berbeda yang dapat dikonstruksikan.

Contoh 3.1.4

Misal diberikan himpunan $W = \{1, 2, 3\}$. Dari himpunan tersebut akan dikonstruksikan sebuah *latin rectangle*. Langkah pertama yang harus dilakukan adalah menyusun baris pertama *latin rectangle* dengan menggunakan elemen-elemen W. Banyaknya cara yang dapat dilakukan adalah sebanyak permutasi jumlah elemen W yakni $3! = 6$ buah cara. Dari hasil permutasi diperoleh enam buah *latin rectangle* berukuran 1×3 sebagai berikut:

$$W_{1\times3}^{1} = [1 \quad 2 \quad 3];\ W_{1\times3}^{2} = [1 \quad 3 \quad 2];\ W_{1\times3}^{3} = [2 \quad 1 \quad 3]$$

$$W_{1\times3}^{4} = [2 \quad 3 \quad 1];\ W_{1\times3}^{5} = [3 \quad 2 \quad 1];\ W_{1\times3}^{6} = [3 \quad 1 \quad 2].$$

Berdasarkan Teorema 3.1.1, masing-masing *latin rectangle* di atas dapat dilengkapkan menjadi *latin square* dengan menambahkan baris secara bertahap. Menurut Teorema 3.1.3, terdapat $(3-1)! = 2!$ banyaknya cara yang dapat dilakukan untuk menambahkan sebuah baris pada $W_{1\times3}$. Sehingga diperoleh:

$$W_{2\times3}^{1,1} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix};\quad W_{2\times3}^{1,2} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix};$$

$$W_{2\times3}^{2,1} = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix};\quad W_{2\times3}^{2,2} = \begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{bmatrix};$$

$$W_{2\times3}^{3,1} = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{bmatrix};\quad W_{2\times3}^{3,2} = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix};$$

$$W_{2\times3}^{4,1} = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix};\quad W_{2\times3}^{4,2} = \begin{bmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix};$$

$$W_{2\times3}^{5,1} = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix};\quad W_{2\times3}^{5,2} = \begin{bmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix};$$

$$W_{2\times3}^{6,1}=\begin{bmatrix}3&1&2\\2&3&1\end{bmatrix};\ W_{2\times3}^{6,2}=\begin{bmatrix}3&1&2\\1&2&3\end{bmatrix}.$$

Selanjutnya, masing-masing *latin rectangle* di atas akan dilengkapkan menjadi sebuah *latin square*. Menurut Teorema 3.1.3, terdapat $(3-2)!=1!$ banyaknya cara yang dapat dilakukan untuk menambahkan sebuah baris pada $W_{2\times3}$. Sehingga,

$$W_{3\times3}^{1,1}=\begin{bmatrix}1&2&3\\2&3&1\\3&1&2\end{bmatrix};\ W_{3\times3}^{1,2}=\begin{bmatrix}1&2&3\\3&1&2\\2&3&1\end{bmatrix};$$

$$W_{3\times3}^{2,1}=\begin{bmatrix}1&3&2\\2&1&3\\3&2&1\end{bmatrix};\ W_{3\times3}^{2,2}=\begin{bmatrix}1&3&2\\3&2&1\\2&1&3\end{bmatrix};$$

$$W_{3\times3}^{3,1}=\begin{bmatrix}2&1&3\\1&3&2\\3&2&1\end{bmatrix};\ W_{3\times3}^{3,2}=\begin{bmatrix}2&1&3\\3&2&1\\1&3&2\end{bmatrix};$$

$$W_{3\times3}^{4,1}=\begin{bmatrix}2&3&1\\1&2&3\\3&1&2\end{bmatrix};\ W_{3\times3}^{4,2}=\begin{bmatrix}2&3&1\\3&1&2\\1&2&3\end{bmatrix};$$

$$W_{3\times3}^{5,1}=\begin{bmatrix}3&2&1\\1&3&2\\2&1&3\end{bmatrix};\ W_{3\times3}^{5,2}=\begin{bmatrix}3&2&1\\2&1&3\\1&3&2\end{bmatrix};$$

$$W_{3\times3}^{6,1}=\begin{bmatrix}3&1&2\\2&3&1\\1&2&3\end{bmatrix};\ W_{3\times3}^{6,2}=\begin{bmatrix}3&1&2\\1&2&3\\2&3&1\end{bmatrix}.$$

Dua belas buah *latin square* di atas merepresentasikan tabel operasi untuk dua belas buah *quasigroup* atas himpunan yang sama dengan operasi biner yang berbeda sebagai berikut:

Tabel 2. *Quasigroup* $(W^{1,1},*)$

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

Tabel 3. *Quasigroup* $(W^{1,2},*)$

$*$	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

Tabel 4. *Quasigroup* $(W^{2,1},*)$

$*$	1	2	3
1	1	3	2
2	2	1	3
3	3	2	1

Tabel 5. *Quasigroup* $(W^{2,2},*)$

$*$	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

Tabel 6. *Quasigroup* $(W^{3,1},*)$

$*$	1	2	3
1	2	1	3
2	1	3	2
3	3	2	1

Tabel 7. *Quasigroup* $(W^{3,2},*)$

$*$	1	2	3
1	2	1	3
2	3	2	1
3	1	3	2

Tabel 8. *Quasigroup* $(W^{4,1},*)$

$*$	1	2	3
1	2	3	1
2	1	2	3
3	3	1	2

Tabel 9. *Quasigroup* $(W^{4,2},*)$

$*$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

Tabel 10. *Quasigroup* $(W^{5,1},*)$

$*$	1	2	3
1	3	2	1
2	1	3	2
3	2	1	3

Tabel 11.*Quasigroup* $(W^{5,2},*)$

$*$	1	2	3
1	3	2	1
2	2	1	3
3	1	3	2

Tabel 12.*Quasigroup* $(W^{6,1},*)$

$*$	1	2	3
1	3	1	2
2	2	3	1
3	1	2	3

Tabel 13.*Quasigroup* $(W^{6,2},*)$

$*$	1	2	3
1	3	1	2
2	1	2	3
3	2	3	1

Pada *quasigroup* $(W^{1,1},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 1;$ $1 * 2 = 2;$ $1 * 3 = 3;$
$2 * 1 = 2;$ $2 * 2 = 3;$ $2 * 3 = 1;$
$3 * 1 = 3;$ $3 * 2 = 1;$ $3 * 3 = 2.$

Pada *quasigroup* $(W^{1,2},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 1;$ $1 * 2 = 2;$ $1 * 3 = 3;$

$2 * 1 = 3;$ $2 * 2 = 1;$ $2 * 3 = 2;$
$3 * 1 = 2;$ $3 * 2 = 3;$ $3 * 3 = 1.$

Pada *quasigroup* $(W^{2,1},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 1;$ $1 * 2 = 3;$ $1 * 3 = 2;$
$2 * 1 = 2;$ $2 * 2 = 1;$ $2 * 3 = 3;$
$3 * 1 = 3;$ $3 * 2 = 2;$ $3 * 3 = 1.$

Pada *quasigroup* $(W^{2,2},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 1;$ $1 * 2 = 3;$ $1 * 3 = 2;$
$2 * 1 = 3;$ $2 * 2 = 2;$ $2 * 3 = 1;$
$3 * 1 = 2;$ $3 * 2 = 1;$ $3 * 3 = 3.$

Pada *quasigroup* $(W^{3,1},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 2;$ $1 * 2 = 1;$ $1 * 3 = 3;$
$2 * 1 = 1;$ $2 * 2 = 3;$ $2 * 3 = 2;$
$3 * 1 = 3;$ $3 * 2 = 2;$ $3 * 3 = 1.$

Pada *quasigroup* $(W^{3,2},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 2;$ $1 * 2 = 1;$ $1 * 3 = 3;$
$2 * 1 = 3;$ $2 * 2 = 2;$ $2 * 3 = 1;$
$3 * 1 = 1;$ $3 * 2 = 3;$ $3 * 3 = 2.$

Pada *quasigroup* $(W^{4,1},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 2;$ $1 * 2 = 3;$ $1 * 3 = 1;$
$2 * 1 = 1;$ $2 * 2 = 2;$ $2 * 3 = 3;$
$3 * 1 = 3;$ $3 * 2 = 1;$ $3 * 3 = 2.$

Pada *quasigroup* $(W^{4,2},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 2;$ $1 * 2 = 3;$ $1 * 3 = 1;$
$2 * 1 = 3;$ $2 * 2 = 1;$ $2 * 3 = 2;$
$3 * 1 = 1;$ $3 * 2 = 2;$ $3 * 3 = 3.$

Pada *quasigroup* $(W^{5,1},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 3;$ $1 * 2 = 2;$ $1 * 3 = 1;$
$2 * 1 = 1;$ $2 * 2 = 3;$ $2 * 3 = 2;$
$3 * 1 = 2;$ $3 * 2 = 1;$ $3 * 3 = 3.$

Pada *quasigroup* $(W^{5,2},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 3;$ $1 * 2 = 2;$ $1 * 3 = 1;$
$2 * 1 = 2;$ $2 * 2 = 1;$ $2 * 3 = 3;$
$3 * 1 = 1;$ $3 * 2 = 3;$ $3 * 3 = 2.$

Pada *quasigroup* $(W^{6,1},*)$ didefinisikan operasi biner berikut:

$1 * 1 = 3;$ $1 * 2 = 1;$ $1 * 3 = 2;$
$2 * 1 = 2;$ $2 * 2 = 3;$ $2 * 3 = 1;$
$3 * 1 = 1;$ $3 * 2 = 2;$ $3 * 3 = 3.$

Pada *quasigroup* $(W^{6,2},*)$ didefinisikan operasi biner berikut:

$1*1=3;\quad 1*2=1;\quad 1*3=2;$
$2*1=1;\quad 2*2=2;\quad 2*3=3;$
$3*1=2;\quad 3*2=3;\quad 3*3=1.$ ■

3.2 Mengkonstruksi Kunci Rahasia dalam Bentuk *Quasigroup Cipher*

Pada era modern seperti sekarang ini, manusia dituntut untuk bisa membangun suatu sistem komunikasi dan informasi yang cepat dan aman. Salah satu hal penting untuk menjamin keamanan informasi dalam komunikasi yang dilakukan dengan menggunakan komputer dan jaringan komputer adalah kode atau *cipher* (Budiyono, 2004). *Cipher* menggunakan suatu algoritma kriptografi untuk mengkodekan *plaintext* menjadi *ciphertext*. Proses mengubah *plaintext* menjadi *ciphertext* dan sebaliknya, dilakukan dengan menggunakan suatu parameter yang disebut kunci. Kunci dalam algoritma kriptografi dapat dikonstruksikan dan direpresentasikan dalam bentuk grup, ring, matriks, pemfaktoran bilangan prima dan sebagainya.

Pada subbab ini akan dibahas suatu metode pembentukan kunci rahasia yang direpresentasikan dalam bentuk *quasigroup cipher*. Hal ini dilakukan mengingat salah satu dari sifat *quasigroup* yang dapat dimanfaatkan untuk mengkonstruksi fungsi *encipher* dan *decipher* (Markovski, 1997). Berdasarkan Contoh 3.1.4, jika $A=\{a_1,\dots,a_n\}$ adalah himpunan alfabet yang membentuk *quasigroup* $(A,*)$ maka tabel operasinya dapat dipandang sebagai *latin square* dengan ukuran $n\times n$, dan sebaliknya. Sebelum jauh pembahasan mengenai bagaimana *quasigroup* $(A,*)$ dikonstruksikan menjadi *quasigroup cipher*, terlebih dahulu diberikan teorema dan definisi berikut:

Teorema 3.2.1

Misalkan $(A,*)$ adalah *quasigroup* yang menetapkan sebuah operasi biner $\backslash$ pada A sedemikian sehingga untuk semua $x,y\in A$ berlaku,

$$x\backslash y=z \leftrightarrow x*z=y,$$

maka *groupoid* $(A,\backslash)$ adalah *quasigroup*.

(Markovski, dkk., 1997)

Bukti:

Groupoid $(A,\backslash)$ adalah sebuah *quasigroup* jika untuk setiap $x, z \in A$ selalu dapat ditemukan $y, w \in A$ sedemikian sehingga berlaku:

$$w \backslash x = z \text{ dan } x \backslash y = z.$$

$w \backslash x = z$ dan $x \backslash y = z$ akan terpenuhi jika dan hanya jika $w * z = x$ dan $x * z = y$ terdefinisi di $(A,*)$. Karena $(A,*)$ adalah *quasigroup* maka berlaku sifat tertutup sehingga $w * z = x$ dan $x * z = y$ selalu terpenuhi dalam *quasigroup* $(A,*)$. Hal ini mengimplikasikan bahwa $w \backslash x = z$ dan $x \backslash y = z$ berlaku di $(A,\backslash)$, dengan demikian terbukti $(A,\backslash)$ adalah *quasigroup*. ■

Contoh 3.2.2

Misalkan $A = (r, s, t)$ dan *quasigroup* $(A,*)$ didefinisikan oleh Tabel 14 berikut:

Tabel 14. *Quasigroup* $(A,*)$

$*$	r	s	t
r	t	r	s
s	s	t	r
t	r	s	t

Dari Tabel 14 diketahui bahwa *quasigroup* $(A,*)$ memenuhi operasi biner berikut:

$r * r = t;$ $s * r = s;$ $t * r = r;$
$r * s = r;$ $s * s = t;$ $t * s = s;$
$r * t = s;$ $s * t = r;$ $t * t = t.$

Jika z mewakili elemen pada kolom dan x mewakili elemen-elemen pada baris sedemikian sehingga $x * z = y$, maka untuk membentuk *quasigroup* $(A,\backslash)$, harus dipenuhi

$$x \backslash y = z \leftrightarrow x * z = y,$$

sehingga,

$r * r = t \leftrightarrow r \backslash t = r;$ $r * s = r \leftrightarrow r \backslash r = s;$
$r * t = s \leftrightarrow r \backslash s = t;$ $s * r = s \leftrightarrow s \backslash s = r;$
$s * s = t \leftrightarrow s \backslash t = s;$ $s * t = r \leftrightarrow s \backslash r = t;$
$t * r = r \leftrightarrow t \backslash r = r;$ $t * s = s \leftrightarrow t \backslash s = s;$
$t * t = t \leftrightarrow t \backslash t = t.$

Dari hasil operasi biner di atas, dapat dikonstruksikan Tabel *quasigroup* $(A,\backslash)$ sebagai berikut:

Tabel 15. *Quasigroup* $(A,\backslash)$

$\backslash$	r	s	t
r	s	t	r
s	t	r	s
t	r	s	t

Definisi 3.2.3

Operasi $\backslash$ adalah *dual* dari $*$ sehingga *quasigroup* $(A,\backslash)$ adalah *dual* dari *quasigroup* $(A,*)$. $(A,*,\backslash)$ adalah *quasigroup* yang diperoleh dari hasil perluasan *quasigroup* $(A,*)$.

(Markovski, dkk., 1997)

Teorema 3.2.4

Quasigroup $(A,*,\backslash)$ memenuhi persamaan identitas:

$$x \backslash (x * y) = y, \quad x * (x \backslash y) = y$$

untuk semua $x, y \in A$.

(Markovski, dkk., 1997)

Bukti:

Ambil sebarang $x, y, z \in A$. Misalkan $x * y = z$, berdasarkan Teorema 3.2.1 berlaku $x \backslash z = y$. Subtitusikan nilai $z = x * y$, diperoleh persamaan identitas, $x \backslash (x * y) = y$.

Ambil sebarang $x, y, w \in A$. Misalkan $x \backslash y = w$, berdasarkan Teorema 3.2.1 berlaku $x * w = y$. Subtitusikan nilai $w = x \backslash y$, diperoleh persamaan identitas, $x * (x \backslash y) = y$. Dengan demikian Teorema 3.2.4 terbukti. ■

Teorema 3.2.4 di atas menjelaskan tentang sifat *quasigroup* $(A,*)$ dan *quasigroup dual*-nya $(A,\backslash)$, yang mana komposisi dari dua *quasigroup* ini akan menghasilkan persamaan identitas. Sifat ini sangat berguna dalam proses *encipher* dan *decipher*. *Ciphertext* yang diperoleh dari proses *encipher* dengan menggunakan *quasigroup* $(A,*)$, akan diubah kembali menjadi *plaintext* dengan menggunakan *quasigroup* $(A,\backslash)$ pada proses *decipher*.

Contoh 3.2.5

Misalkan $A = (r, s, t)$ dan *quasigroup* $(A,*,\backslash)$ didefinisikan oleh Tabel 14 dan Tabel 15 sebagaimana pada Contoh 3.2.2.

Tabel 14. *Quasigroup* $(A,*)$

$*$	r	s	t
r	t	r	s
s	s	t	r
t	r	s	t

Tabel 15. *Quasigroup* $(A,\backslash)$

$\backslash$	r	s	t
r	s	t	r
s	t	r	s
t	r	s	t

Dengan menerapkan Teorema 3.2.4 diperoleh persamaan identitas sebagai berikut:

$$\begin{aligned} r \backslash (r * r) &= r \backslash t = r; & r * (r\backslash t) &= r * r = t;\\ r \backslash (r * s) &= r \backslash r = s; & r * (r\backslash r) &= r * s = r;\\ r \backslash (r * t) &= r \backslash s = t; & r * (r\backslash s) &= r * t = s;\\ s \backslash (s * r) &= s \backslash s = r; & s * (s\backslash s) &= s * r = s;\\ s \backslash (s * s) &= s \backslash t = s; & s * (s\backslash t) &= s * s = t;\\ s \backslash (s * t) &= s \backslash r = t; & s * (s\backslash r) &= s * t = r;\\ t \backslash (t * r) &= t \backslash r = r; & t * (t\backslash r) &= t * r = r;\\ t \backslash (t * s) &= t \backslash s = s; & t * (t\backslash s) &= t * s = s;\\ t \backslash (t * t) &= t \backslash t = t; & t * (t\backslash t) &= t * t = t. \blacksquare \end{aligned}$$

Misalkan $(A,*,\backslash)$ adalah *quasigroup* sebagaimana yang telah didefinisikan di atas. Diberikan himpunan A^+ yang merupakan himpunan tak kosong berisi *plaintext* yang dibentuk dari elemen-elemen A. Didefinisikan dua operasi uner f_* dan $f_\backslash$ pada A^+ sebagai berikut:

Definisi 3.2.6

Misalkan $u_i \in A^+,\ k \in \mathbb{N},\ k \geq 1$, dan $a_1 \in A$ maka,

$$f_*(u_1u_2 \ldots u_k) = v_1v_2 \ldots v_k$$
$$\Leftrightarrow v_1 = a_1 * u_1, \quad v_{i+1} = v_i * u_{i+1}, \quad i = 1, 2, \ldots, k-1,$$
$$f_\backslash(u_1u_2 \ldots u_k) = v_1v_2 \ldots v_k$$
$$\Leftrightarrow v_1 = a_1 \backslash u_1, \quad v_{i+1} = u_i \backslash u_{i+1}, \quad i = 1, 2, \ldots, k-1.$$

Sixtuple $(A,*,\backslash, a_1, f_*, f_\backslash)$ disebut *quasigroup cipher* atas alfabet A.

(Markovski, dkk., 1997)

Contoh 3.2.7

Misalkan $A = (a, b, c, d)$ dan $a_1 = a$. *Quasigroup* $(A,*)$ dan $(A,\backslash)$ didefinisikan oleh Tabel 16 dan Tabel 17 berikut:

Tabel 16. *Quasigroup* $(A,*)$

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

Tabel 17. *Quasigroup* $(A,\backslash)$

$\backslash$	a	b	c	d
a	d	a	b	c
b	a	b	c	d
c	b	c	d	a
d	c	d	a	b

Misal diberikan $u = adabbaca$, maka diperoleh f_*-nya sebagai berikut:

$$v_1 = a_1 * u_1 = a * a = b \qquad v_2 = v_1 * u_2 = b * d = d$$
$$v_3 = v_2 * u_3 = d * a = c \qquad v_4 = v_3 * u_4 = c * b = a$$
$$v_5 = v_4 * u_5 = a * b = c \qquad v_6 = v_5 * u_6 = c * a = d$$
$$v_7 = v_6 * u_7 = d * c = a \qquad v_8 = v_7 * u_8 = a * a = b$$

sehingga $f_*(adabbaca) = bdcacdab$. Dengan nilai u yang sama diperoleh $f_\backslash$-nya sebagai berikut:

$$v_1 = a_1 \backslash u_1 = a \backslash a = d \qquad v_2 = u_1 \backslash u_2 = a \backslash d = c$$
$$v_3 = u_2 \backslash u_3 = d \backslash a = c \qquad v_4 = u_3 \backslash u_4 = a \backslash b = a$$
$$v_5 = u_4 \backslash u_5 = b \backslash b = b \qquad v_6 = u_5 \backslash u_6 = b \backslash a = a$$
$$v_7 = u_6 \backslash u_7 = a \backslash c = b \qquad v_8 = u_7 \backslash u_8 = c \backslash a = b$$

sehingga $f_\backslash(adabbaca) = dccababb$. ■

Smith (2007) dalam makalahnya yang berjudul *Four Lectures on Quasigroup Representations* menyebutkan bahwa terdapat operasi biner lain, yakni operasi biner / yang terdefinisi di dalam *quasigroup* $(Q,*)$. Smith menyebut \ sebagai pembagi kiri (*left division*), dan / sebagai pembagi kanan (*right division*). Dalam makalahnya Smith juga menyebutkan bahwa operasi biner / ini memenuhi persamaan identitas,

$$(x * y)/y = x \text{ dan } (x/y) * y = x.$$

Karena *quasigroup* dengan operasi biner $*$ dan / memenuhi persamaan identitas, maka *quasigroup* $(Q,*,/)$ juga dapat digunakan sebagai kunci rahasia atau *quasigroup cipher*. Sebelum jauh pembahasan mengenai *quasigroup cipher* yang dibentuk dari *quasigroup* $(Q,*,/)$, terlebih dahulu akan diberikan beberapa teorema dan definisi berikut:

Teorema 3.2.7

Misalkan $(A,*)$ adalah *quasigroup* yang menetapkan sebuah operasi biner $/$ pada A sedemikian sehingga untuk semua $x, y \in A$ berlaku,

$$x/y = z \leftrightarrow z * y = x,$$

maka *groupoid* $(A,/)$ adalah *quasigroup*.

Bukti:

Groupoid $(A,/)$ adalah sebuah *quasigroup* jika untuk setiap $x, z \in A$ selalu dapat ditemukan $y, w \in A$ sedemikian sehingga berlaku:

$$w/x = z \text{ dan } x/y = z.$$

$w/x = z$ dan $x/y = z$ akan terpenuhi jika dan hanya jika $z * x = w$ dan $z * y = x$ terdefinisi di $(A,*)$. Karena $(A,*)$ adalah *quasigroup* maka berlaku sifat tertutup sehingga $z * x = w$ dan $z * y = x$ selalu terpenuhi dalam *quasigroup* $(A,*)$. Hal ini mengimplikasikan bahwa $w/x = z$ dan $x/y = z$ berlaku di $(A,/)$, dengan demikian terbukti $(A,/)$ adalah *quasigroup*. ■

Contoh 3.2.8

Misalkan $A = (m, n, o)$ dan *quasigroup* $(A,*)$ didefinisikan oleh Tabel 18 berikut:

Tabel 18. *Quasigroup* $(A,*)$

$*$	m	n	o
m	o	n	m
n	m	o	n
o	n	m	o

Dari Tabel 18 di atas diketahui bahwa *quasigroup* $(A,*)$ memenuhi operasi biner berikut:

$m * m = o;$ $n * m = m;$ $o * m = n;$
$m * n = n;$ $n * n = o;$ $o * n = m;$
$m * o = m;$ $n * o = n;$ $o * o = o.$

Misalkan z mewakili elemen-elemen pada baris dan y mewakili elemen-elemen pada kolom sedemikian sehingga $z * y = x$, maka untuk membentuk *quasigroup* $(A,/)$, harus dipenuhi,

$$x/y = z \leftrightarrow z * y = x.$$

Sehingga,

$m * m = o \leftrightarrow o/m = m;$ $\quad m * n = n \leftrightarrow n/n = m;$
$m * o = m \leftrightarrow m/o = m;$ $\quad n * m = m \leftrightarrow m/m = n;$
$n * n = o \leftrightarrow o/n = n;$ $\quad n * o = n \leftrightarrow n/o = n;$
$o * m = n \leftrightarrow n/m = o;$ $\quad o * n = m \leftrightarrow m/n = o;$
$o * o = o \leftrightarrow o/o = o.$

Dari hasil operasi biner di atas, dapat dikonstruksikan tabel operasi biner *quasigroup* $(A,/)$ sebagai berikut:

Tabel 19. *Quasigroup* $(A,/)$

$/$	m	n	o
m	n	o	m
n	o	m	n
o	m	n	o

Definisi 3.2.9

Operasi $/$ adalah *dual* dari $*$ sehingga *quasigroup* $(A,/)$ adalah *dual* dari *quasigroup* $(A,*)$. $(A,*,/)$ adalah *quasigroup* yang diperoleh dari hasil perluasan *quasigroup* $(A,*)$.

Teorema 3.2.10

Quasigroup $(A,*,/)$ memenuhi persamaan identitas:

$$(x * y)/y = x, \quad (x/y) * y = x$$

untuk semua $x, y \in A$.

Bukti:

Misalkan diambil sebarang elemen $x, y, z \in A$. Misalkan pula $x * y = z$, berdasarkan Teorema 3.2.7 berlaku $z/y = x$. Subtitusikan nilai $z = x * y$, diperoleh persamaan identitas, $(x * y)/y = x$.

Misalkan diambil sebarang elemen $x, y, w \in A$. Misalkan pula $x/y = w$, berdasarkan Teorema 3.2.7 berlaku $w * y = x$. Subtitusikan nilai $w = x/y$, diperoleh persamaan identitas, $(x/y) * y = x$. Karena dua persamaan identitas di atas terpenuhi, maka Teorema 3.2.10 terbukti benar. ■

Contoh 3.2.11

Misalkan $A = (m, n, o)$ dan *quasigroup* $(A,*,/)$ didefinisikan oleh Tabel 18 dan Tabel 19 seperti pada Contoh 3.2.8 diatas.

Tabel 18. *Quasigroup* $(A,*)$

$*$	m	n	o
m	o	n	m
n	m	o	n
o	n	m	o

Tabel 19. *Quasigroup* $(A,/)$

$/$	m	n	o
m	n	o	m
n	o	m	n
o	m	n	o

Dengan menerapkan Teorema 3.2.10 diperoleh persamaan identitas sebagai berikut:

$(m * m)/m = o/m = m;$ $(m/m) * m = n * m = m;$
$(m * n)/n = n/n = m;$ $(m/n) * n = o * n = m;$
$(m * o)/o = m/o = m;$ $(m/o) * o = m * o = m;$
$(n * m)/m = m/m = n;$ $(n/m) * m = o * m = n;$
$(n * n)/n = o/n = n;$ $(n/n) * n = m * n = n;$
$(n * o)/o = n/o = n;$ $(n/o) * o = n * o = n;$
$(o * m)/m = n/m = o;$ $(o/m) * m = m * m = o;$
$(o * n)/n = m/n = o;$ $(o/n) * n = n * n = o;$
$(o * o)/o = o/o = o;$ $(o/o) * o = o * o = o.$■

Misalkan $(A,*,/)$ adalah *quasigroup* sebagaimana yang telah didefinisikan di atas. Diberikan himpunan A^+ yang merupakan himpunan tak kosong berisi *plaintext* yang dibentuk dari elemen-elemen A. Didefinisikan dua operasi uner f_* dan $f_/$ pada A^+ sebagai berikut:

Definisi 3.2.12

Misalkan $u_i \in A^+,\ k \in \mathbb{N},\ k \geq 1$, dan $a_1 \in A$ maka,

$$f_*(u_1u_2\ \dots\ u_k) = v_1v_2 \dots v_k$$
$$\Leftrightarrow v_1 = u_1 * a_1, \quad v_{i+1} = u_{i+1} * v_i, \quad i = 1, 2, \dots, k-1$$
$$f_/(u_1u_2\ \dots\ u_k) = v_1v_2 \dots v_k$$
$$\Leftrightarrow v_1 = u_1/a_1, \quad v_{i+1} = u_{i+1}/u_i, \quad i = 1, 2, \dots, k-1$$

Sixtuple $(A,*,/,a_1,f_*,f_/)$ disebut *quasigroup cipher* atas alfabet A.

Contoh 3.2.13

Misalkan $A = (a,b,c,d)$ dan $a_1 = b$. *Quasigroup* $(A,*)$ dan $(A,/)$ didefinisikan oleh Tabel 20 dan Tabel 21 berikut:

Tabel 20. *Quasigroup* $(A,*)$

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

Tabel 21. *Quasigroup* $(A,/)$

$/$	a	b	c	d
a	b	d	c	a
b	a	b	d	c
c	c	a	b	d
d	d	c	a	b

Misal diberikan $u = bacabaca$, maka diperoleh f_* -nya sebagai berikut:

$$v_1 = u_1 * a_1 = b * b = b \qquad v_2 = u_2 * v_1 = a * b = c$$
$$v_3 = u_3 * v_2 = c * c = a \qquad v_4 = u_4 * v_3 = a * a = b$$
$$v_5 = u_5 * v_4 = b * b = b \qquad v_6 = u_6 * v_5 = a * b = c$$
$$v_7 = u_7 * v_6 = c * c = a \qquad v_8 = u_8 * v_7 = a * a = b$$

sehingga $f_*(bacabaca) = bcabbcab$. Dengan nilai u yang sama diperoleh $f_/$ -nya sebagai berikut:

$$v_1 = u_1/a_1 = b/b = b \qquad v_2 = u_2/u_1 = a/b = d$$
$$v_3 = u_3/u_2 = c/a = c \qquad v_4 = u_4/u_3 = a/c = c$$
$$v_5 = u_5/u_4 = b/a = a \qquad v_6 = u_6/u_5 = a/b = d$$
$$v_7 = u_7/u_6 = c/a = c \qquad v_8 = u_8/u_7 = a/c = c$$

sehingga $f_/(bacabaca) = bdccadcc$. ■

Karena *quasigroup cipher* $(A,*,\backslash,a_1,f_*,f_\backslash)$ dan *quasigroup cipher* $(A,*,/,a_1,f_*,f_/)$ berbeda, maka *quasigroup cipher* $(A,*,\backslash,a_1,f_*,f_\backslash)$ dinamakan sebagai *quasigroup cipher* kiri (*left quasigroup cipher*) sedangkan $(A,*,/,a_1,f_*,f_/)$ dinamakan sebagai *quasigroup cipher* kanan (*right quasigroup cipher*).

3.3 Mengkonstruksi Fungsi *Encipher* dan *Decipher* dengan Menggunakan *Quasigroup Cipher*

Algoritma kriptografi tidak bisa lepas dari proses *encipher* dan *decipher*. Masing-masing proses dilakukan dengan menggunakan sebuah fungsi yang disebut fungsi *encipher* dan *decipher*. Fungsi *encipher* berguna untuk mengubah *plaintext* menjadi *ciphertext*. Sedangkan untuk mengubah *ciphertext* menjadi *plaintext* digunakan fungsi *decipher*. Dari sini diketahui bahwa komposisi antara fungsi *encipher* dan *decipher* akan menghasilkan suatu pemetaan identitas.

Lemma 3.3.1

Jika $(A,*,\backslash,a_1,f_*,f_\backslash)$ adalah *quasigroup cipher* (kiri) atas himpunan alfabet A, maka $f_\backslash \circ f_* = 1_{A^+}$ yang mana 1_{A^+} adalah pemetaan identitas pada A^+ dan $\circ$ adalah pemetaan komposisi.

(Markovski, dkk., 1997)

Bukti:

Misalkan $u_i \in A,\ k \geq 1$ dan

$$f_*(u_1u_2 \dots u_k) = v_1v_2 \dots v_k.$$

Didefinisikan,

$$f_\backslash \circ f_*(u_1u_2 \dots u_k) = f_\backslash(v_1v_2 \dots v_k) = w_1w_2 \dots w_k.$$

Sehingga untuk $i = 1, 2, \dots, k-1$ diperoleh,

$$v_1 = a_1 * u_1,$$
$$v_{i+1} = v_i * u_{i+1},$$
$$w_1 = a_1 \backslash v_1,$$
$$w_{i+1} = v_i \backslash v_{i+1},$$

Dengan menggunakan Teorema 3.2.4 diperoleh,

$$w_1 = a_1 \backslash (a_1 * u_1) = u_1,$$
$$w_{i+1} = v_i \backslash (v_i * u_{i+1}) = u_{i+1}$$

untuk $i = 1, 2, \dots, k-1$. ■

(Markovski, dkk., 1997)

Dari Lemma 3.3.1 di atas diketahui bahwa $f_\backslash \circ f_*$ menghasilkan pemetaan identitas di A^+, sehingga untuk *quasigroup cipher* kiri diambil $f_e = f_*$ sebagai fungsi *encipher* dan $f_d = f_\backslash$ sebagai fungsi *decipher*-nya.

Lemma 3.3.2

Jika $(A,*,/,a_1,f_*,f_/)$ adalah *quasigroup cipher* kanan atas himpunan alfabet A, maka $f_/ \circ f_* = 1_{A^+}$ yang mana 1_{A^+} adalah pemetaan identitas pada A^+ dan $\circ$ adalah pemetaan komposisi.

Bukti:

Misalkan $u_i \in A,\ k \geq 1$ dan

$$f_*(u_1u_2 \dots u_k) = v_1v_2 \dots v_k.$$

Didefinisikan,

$$f_/ \circ f_*(u_1u_2 \dots u_k) = f_/(v_1v_2 \dots v_k) = w_1w_2 \dots w_k.$$

Sehingga untuk $i = 1, 2, \dots, k-1$ diperoleh,

$$v_1 = u_1 * a_1,$$

$$v_{i+1} = u_{i+1} * v_i,$$
$$w_1 = v_1/a_1,$$
$$w_{i+1} = v_{i+1}/v_i,$$

Dengan menggunakan Teorema 3.2.10 diperoleh,

$$w_1 = (u_1 * a_1)/a_1 = u_1,$$
$$w_{i+1} = (u_{i+1} * v_i)/v_i = u_{i+1}$$

untuk $i = 1, 2, \dots, k-1$. ■

Dari Lemma 3.3.2 di atas diketahui bahwa $f_/ \circ f_*$ menghasilkan pemetaan identitas di A^+, sehingga untuk *quasigroup cipher* kanan diambil $f_e = f_*$ sebagai fungsi *encipher* dan $f_d = f_/$ sebagai fungsi *decipher*-nya.

Contoh 3.3.3

Misalkan *A* adalah himpunan 26 buah huruf alfabet dengan menambahkan tanda *underscore* sebagai spasi dalam *plaintext*. Hasil operasi biner pada *quasigroup* $(A,*)$ didefinisikan oleh Tabel 22 berikut:

Tabel 22. *Quasigroup* $(A,*)$

$*$	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_
a	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m
b	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l
d	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
e	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k
f	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
g	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j
h	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i
j	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
k	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h
l	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
m	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g
n	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
o	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f
p	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
q	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e
r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
s	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d
t	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
u	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c
v	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
w	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b
x	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
y	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a
z	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n
_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_

Dari Tabel 22 di atas, dikonstruksikan tabel *quasigroup* $(A,\backslash)$ dan *quasigroup* $(A,/)$ dengan menggunakan Teorema

3.2.1 dan Teorema 3.2.7. Untuk *quasigroup cipher* kiri diperoleh tabel *quasigroup* $(A,\backslash)$ sebagai berikut:

Tabel 23. *Quasigroup* $(A,\backslash)$

\	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_
a	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a
c	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
d	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b
e	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
f	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c
g	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
h	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d
i	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
j	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e
k	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
l	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f
m	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
n	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g
o	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
p	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h
q	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
r	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i
s	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
t	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j
u	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
v	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k
w	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
x	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l
y	_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
z	n	o	p	q	r	s	t	u	v	w	x	y	z	_	a	b	c	d	e	f	g	h	i	j	k	l	m
_	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_

Misalkan dipilih e sebagai *leader* sehingga $a_1 = e$ dan diberikan *plaintext* $u = harap\_tenang\_ada\_ujian$. *Plaintext* ini akan diubah menjadi sebuah *ciphertext* dengan menggunakan fungsi *encipher* berikut:

$v_1 = a_1 * u_1 = e * h = s;$ $v_2 = v_1 * u_2 = s * a = e;$
$v_3 = v_2 * u_3 = e * r = b;$ $v_4 = v_3 * u_4 = b * a = \_;$
$v_5 = v_4 * u_5 = \_ * p = p;$ $v_6 = v_5 * u_6 = p * \_ = s;$
$v_7 = v_6 * u_7 = s * t = x;$ $v_8 = v_7 * u_8 = x * e = t;$
$v_9 = v_8 * u_9 = \_ * n = d;$ $v_{10} = v_9 * u_{10} = d * a = z;$
$v_{11} = v_{10} * u_{11} = z * n = a;$ $v_{12} = v_{11} * u_{12} = a * g = t;$
$v_{13} = v_{12} * u_{13} = t * \_ = q;$ $v_{14} = v_{13} * u_{14} = q * a = f;$
$v_{15} = v_{14} * u_{15} = f * d = a;$ $v_{16} = v_{15} * u_{16} = a * a = n;$
$v_{17} = v_{16} * u_{17} = n * \_ = t;$ $v_{18} = v_{17} * u_{18} = t * u = k;$
$v_{19} = v_{18} * u_{19} = k * j = r;$ $v_{20} = v_{19} * u_{20} = r * i = \_;$
$v_{21} = v_{20} * u_{21} = \_ * a = a;$ $v_{22} = v_{21} * u_{22} = a * n = \_.$

Dari hasil proses *encipher* di atas diperoleh *ciphertext*, $v = seb\_psxtdzatqfantkr\_a\_$. Untuk mengubah *ciphertext*

menjadi *plaintext* kembali dilakukan proses *decipher* dengan menggunakan fungsi *decipher* berikut:

$w_1 = a_1 \setminus v_1 = e \setminus s = h;$ $w_2 = v_1 \setminus v_2 = s \setminus e = a;$
$w_3 = v_2 \setminus v_3 = e \setminus b = r;$ $w_4 = v_3 \setminus v_4 = b \setminus \_ = a;$
$w_5 = v_4 \setminus v_5 = \_ \setminus p = p;$ $w_6 = v_5 \setminus v_6 = p \setminus s = \_;$
$w_7 = v_6 \setminus v_7 = s \setminus x = t;$ $w_8 = v_7 \setminus v_8 = x \setminus t = e;$
$w_9 = v_8 \setminus v_9 = t \setminus d = n;$ $w_{10} = v_9 \setminus v_{10} = d \setminus z = a;$
$w_{11} = v_{10} \setminus v_{11} = z \setminus a = n;$ $w_{12} = v_{11} \setminus v_{12} = a \setminus t = g;$
$w_{13} = v_{12} \setminus v_{13} = t \setminus q = \_;$ $w_{14} = v_{13} \setminus v_{14} = q \setminus f = a;$
$w_{15} = v_{14} \setminus v_{15} = f \setminus a = d;$ $w_{16} = v_{15} \setminus v_{16} = a \setminus n = a;$
$w_{17} = v_{16} \setminus v_{17} = n \setminus t = \_;$ $w_{18} = v_{17} \setminus v_{18} = t \setminus k = u;$
$w_{19} = v_{18} \setminus v_{19} = k \setminus r = j;$ $w_{20} = v_{19} \setminus v_{20} = r \setminus \_ = i;$
$w_{21} = v_{20} \setminus v_{21} = \_ \setminus a = a;$ $w_{22} = v_{21} \setminus v_{22} = a \setminus \_ = n;$

Dari proses *decipher* di atas diperoleh *plaintext* awal yakni $u = harap\_tenang\_ada\_ujian.$ ■

Untuk *quasigroup cipher* kanan diperoleh tabel *quasigroup* $(A,/)$ sebagai berikut:

Tabel 24. *Quasigroup* $(A,/)$

/	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	_
a	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y
b	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w
c	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u
d	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s
e	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q
f	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o
g	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m
h	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k
i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i
j	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g
k	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e
l	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c
m	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z	a
n	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x	z
o	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v	x
p	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t	v
q	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r	t
r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p	r
s	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n	p
t	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l	n
u	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j	l
v	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h	j
w	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f	h
x	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d	f
y	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b	d
z	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_	b
_	b	d	f	h	j	l	n	p	r	t	v	x	z	a	c	e	g	i	k	m	o	q	s	u	w	y	_

Misalkan dipilih e sebagai *leader* sehingga $a_1 = e$ dan diberikan *plaintext* $u = harap\_tenang\_ada\_ujian$. *Plaintext* ini akan diubah menjadi sebuah *ciphertext* dengan menggunakan fungsi *encipher* berikut:

$v_1 = u_1 * a_1 = h * e = a;$ $v_2 = u_2 * v_1 = a * a = n;$
$v_3 = u_3 * v_2 = r * n = e;$ $v_4 = u_4 * v_3 = a * e = r;$
$v_5 = u_5 * v_4 = p * r = j;$ $v_6 = u_6 * v_5 = \_ * j = j;$
$v_7 = u_7 * v_6 = t * j = \_;$ $v_8 = u_8 * v_7 = e * \_ = k;$
$v_9 = u_9 * v_8 = n * k = d;$ $v_{10} = u_{10} * v_9 = a * d = q;$
$v_{11} = u_{11} * v_{10} = n * q = j;$ $v_{12} = u_{12} * v_{11} = g * j = t;$
$v_{13} = u_{13} * v_{12} = \_ * t = t;$ $v_{14} = u_{14} * v_{13} = a * t = f;$
$v_{15} = u_{15} * v_{14} = d * f = d;$ $v_{16} = u_{16} * v_{15} = a * d = q;$
$v_{17} = u_{17} * v_{16} = \_ * q = q;$ $v_{18} = u_{18} * v_{17} = u * q = t;$
$v_{19} = u_{19} * v_{18} = j * t = o;$ $v_{20} = u_{20} * v_{19} = i * o = x;$
$v_{21} = u_{21} * v_{20} = a * x = j;$ $v_{22} = u_{22} * v_{21} = n * j = c.$

Dari hasil proses *encipher* di atas diperoleh *ciphertext* sebagai berikut, $v = anerjj\_kdqjttfdqqtoxjc$. Untuk mengubah *ciphertext* menjadi *plaintext* kembali dilakukan proses *decipher* dengan menggunakan fungsi *decipher* berikut:

$w_1 = v_1 * a_1 = a * e = h;$ $w_2 = v_2 * v_1 = n * a = a;$
$w_3 = v_3 * v_2 = e * n = r;$ $w_4 = v_4 * v_3 = r * e = a;$
$w_5 = v_5 * v_4 = j * r = p;$ $w_6 = v_6 * v_5 = j * j = \_;$
$w_7 = v_7 * v_6 = \_ * j = t;$ $w_8 = v_8 * v_7 = k * \_ = e;$
$w_9 = v_9 * v_8 = d * k = n;$ $w_{10} = v_{10} * v_9 = q * d = a;$
$w_{11} = v_{11} * v_{10} = j * q = n;$ $w_{12} = v_{12} * v_{11} = t * j = g;$
$w_{13} = v_{13} * v_{12} = t * t = \_;$ $w_{14} = v_{14} * v_{13} = f * t = a;$
$w_{15} = v_{15} * v_{14} = d * f = d;$ $w_{16} = v_{16} * v_{15} = q * d = a;$
$w_{17} = v_{17} * v_{16} = q * q = \_;$ $w_{18} = v_{18} * v_{17} = t * q = u;$
$w_{19} = v_{19} * v_{18} = o * t = j;$ $w_{20} = v_{20} * v_{19} = x * o = i;$
$w_{21} = v_{21} * v_{20} = j * x = a;$ $w_{22} = v_{22} * v_{21} = c * j = n.$

Dari proses *decipher* di atas diperoleh *plaintext* awal yakni, $u = harap\_tenang\_ada\_ujian$. ■

Secara garis besar dapat disimpulkan bahwa fungsi *encipher* dan *decipher* adalah fungsi yang komposisi keduanya menghasilkan pemetaan identitas. Dalam *quasigroup cipher* baik kanan maupun kiri, fungsi *encipher* dan *decipher*-nya tak lain adalah dua fungsi uner yang didefinisikan di dalamnya.

3.4 Kelebihan dan Kelemahan Metode Kunci Rahasia dengan Menggunakan *Quasigroup Cipher*

Komunikasi dengan kunci rahasia mengharuskan setiap pasangan atau grup yang terlibat dalam komunikasi memiliki sebuah kunci rahasia yang bisa dibangkitkan. Masalahnya akan menjadi rumit apabila komunikasi dilakukan secara bersama-sama oleh sebanyak n orang pengguna dan setiap dua pihak melakukan pertukaran kunci, maka dibutuhkan sebanyak $C_2^n = n!/(n-2)!\,2! = n(n-1)/2$ buah kunci rahasia yang bisa dipertukarkan secara aman (Riyanto, 2007).

Untuk mengatasi kelemahan ini, *quasigroup cipher* haruslah dibangun atas himpunan dengan jumlah elemen yang besar. Semakin banyak jumlah elemen himpunan pembangunnya, maka semakin banyak pula jumlah *quasigroup cipher* yang akan dihasilkan. Sebagai contoh, misalkan diambil 256 buah karakter ASCII yang akan digunakan untuk mengkonstruksi *quasigroup* $(A,*)$. Berdasarkan Teorema 3.1.3, terdapat 256!255!254!...2!1! buah *latin square* yang dapat dibentuk, dengan demikian sebanyak $256!255!...2!1! > 10^{58000}$ buah *quasigroup* dapat dikonstruksikan (Markovski, dkk., 1997).

Metode kunci rahasia dengan menggunakan *quasigroup cipher* dapat digolongkan dalam algoritma *stream cipher*. Masing-masing karakter dalam *plaintext* dikodekan oleh satu karakter, sehingga *ciphertex* yang dihasilkan sama panjang dengan *plaintext*-nya. Oleh karena itu metode ini baik untuk komunikasi *online* yang cepat (Markovski, dkk., 1997). Algoritma *stream cipher* cocok untuk mengenkripsikan aliran data yang terus menerus melalui saluran komunikasi, seperti data berupa suara digital pada jaringan telepon *mobile* GSM (Munir, 2004). Alasannya, jika *ciphertext* yang diterima mengandung kesalahan, maka hanya akan dihasilkan satu kesalahan pada waktu proses *decipher*, karena tiap karakter *plaintext* hanya bergantung pada satu karakter *ciphertext*. Hal yang hampir serupa juga terjadi dalam metode kunci rahasia dengan menggunakan *quasigroup cipher*. Sebagai ilustrasinya, diberikan teorema-teorema berikut:

Teorema 3.4.1

Misalkan $u = u_1 u_2 \dots u_k \in A^+$ adalah *plaintext*, sedangkan $v = f_*(u) = v_1 v_2 \dots v_k$ adalah *ciphertext*-nya dan $v' = v_1 v_2 \dots v_{i-1} v_i' v_{i+1} \dots v_k (v_i' \in A)$. Maka,

$$f_{\backslash}(v') = u_1 u_2 \dots u_{i-1} u_i' u_{i+1}' u_{i+2} \dots u_k,$$

untuk $u_i', u_{i+1}' \in A$.

(Markovski, dkk., 1997)

Bukti:

Diketahui $v' = v_1 v_2 \dots v_{i-1} v_i' v_{i+1} \dots v_k$. Misalkan $f_{\backslash}(v') = w'$, maka,

$$w_1 = a_1 \backslash v_1 = a_1 \backslash (a_1 * u_1) = u_1$$
$$w_i = v_{i-1} \backslash v_i' = v_{i-1} \backslash (v_{i-1} * u_i') = u_i'$$
$$w_{i+1} = v_i \backslash v_{i+1} = v_i' \backslash (v_i' * u_{i+1}') = u_{i+1}'$$

dari sini terbukti bahwa

$$f_{\backslash}(v') = u_1 u_2 \dots u_{i-1} u_i' u_{i+1}' u_{i+2} \dots u_k. \blacksquare$$

Teorema 3.4.2

Misalkan $u = u_1 u_2 \dots u_k \in A^+$ adalah *plaintext*, sedangkan $v = f_*(u) = v_1 v_2 \dots v_k$ adalah *ciphertext*-nya dan $v' = v_1 v_2 \dots v_{i-1} v_i' v_{i+1} \dots v_k (v_i' \in A)$. Maka,

$$f_{/}(v') = u_1 u_2 \dots u_{i-1} u_i' u_{i+1}' u_{i+2} \dots u_k,$$

untuk $u_i', u_{i+1}' \in A$.

Bukti:

Diketahui $v' = v_1 v_2 \dots v_{i-1} v_i' v_{i+1} \dots v_k$. Misalkan $f_{/}(v') = w'$, maka,

$$w_1 = v_1 / a_1 = (u_1 * a_1)/a_1 = u_1$$
$$w_i = v_i' / v_{i-1} = (u_i' * v_{i-1})/v_{i-1} = u_i'$$
$$w_{i+1} = v_{i+1} / v_i = (u_{i+1}' * v_i')/v_i' = u_{i+1}'$$

dari sini terbukti bahwa

$$f_{/}(v') = u_1 u_2 \dots u_{i-1} u_i' u_{i+1}' u_{i+2} \dots u_k. \blacksquare$$

Contoh 3.4.3 berikut akan memberikan ilustrasi lebih jelas mengenai error yang terjadi dalam *ciphertext* pada *quasigroup cipher* kiri. Contoh 3.4.3 ini dianggap telah mewakili ilustrasi error yang terjadi dalam *ciphertext* pada *quasigroup cipher* kanan.

Contoh 3.4.3

Misalkan $A = \{a, b, d, e, g, i, k, l, m, n, o, r, u\}$ dan hasil operasi biner pada *quasigroup* $(A,*)$ didefinisikan oleh Tabel 25 berikut:

Tabel 25. *Quasigroup* $(A,*)$

$*$	a	b	d	e	g	i	k	l	m	n	o	r	u
a	m	n	o	r	u	a	b	d	e	g	i	k	l
b	u	a	b	d	e	g	i	k	l	m	n	o	r
d	e	g	i	k	l	m	n	o	r	u	a	b	d
e	r	u	a	b	d	e	g	i	k	l	m	n	o
g	l	m	n	o	r	u	a	b	d	e	g	i	k
i	b	d	e	g	i	k	l	m	n	o	r	u	a
k	a	b	d	e	g	i	k	l	m	n	o	r	u
l	g	i	k	l	m	n	o	r	u	a	b	d	e
m	o	r	u	a	b	d	e	g	i	k	l	m	n
n	k	l	m	n	o	r	u	a	b	d	e	g	i
o	d	e	g	i	k	l	m	n	o	r	u	a	b
r	n	o	r	u	a	b	d	e	g	i	k	l	m
u	i	k	l	m	n	o	r	u	a	b	d	e	g

Dari Tabel 25 di atas diperoleh tabel *dual quasigroup* $(A,\backslash)$ sebagai berikut:

Tabel 26. *Quasigroup* $(A,\backslash)$

$\backslash$	a	b	d	e	g	i	k	l	m	n	o	r	u
a	i	k	l	m	n	o	r	u	a	b	d	e	g
b	b	d	e	g	i	k	l	m	n	o	r	u	a
d	o	r	u	a	b	d	e	g	i	k	l	m	n
e	d	e	g	i	k	l	m	n	o	r	u	a	b
g	k	l	m	n	o	r	u	a	b	d	e	g	i
i	u	a	b	d	e	g	i	k	l	m	n	o	r
k	a	b	d	e	g	i	k	l	m	n	o	r	u
l	n	o	r	u	a	b	d	e	g	i	k	l	m
m	e	g	i	k	l	m	n	o	r	u	a	b	d
n	l	m	n	o	r	u	a	b	d	e	g	i	k
o	r	u	a	b	d	e	g	i	k	l	m	n	o
r	g	i	k	l	m	n	o	r	u	a	b	d	e
u	m	n	o	r	u	a	b	d	e	g	i	k	l

Misalkan dipilih m sebagai *leader* sehingga $a_1 = m$ dan diberikan *plaintext* $u = ambiluangdiloker$. Dilakukan proses *encipher* berikut:

$v_1 = a_1 * u_1 = m * a = o;$ $\quad v_2 = v_1 * u_2 = o * m = o;$

$v_3 = v_2 * u_3 = o * b = e;$ $\quad v_4 = v_3 * u_4 = e * i = e;$

$v_5 = v_4 * u_5 = e * l = i;$ $v_6 = v_5 * u_6 = i * u = a;$
$v_7 = v_6 * u_7 = a * a = m;$ $v_8 = v_7 * u_8 = m * n = k;$
$v_9 = v_8 * u_9 = k * g = g;$ $v_{10} = v_9 * u_{10} = g * d = n;$
$v_{11} = v_{10} * u_{11} = n * i = r;$ $v_{12} = v_{11} * u_{12} = r * l = e;$
$v_{13} = v_{12} * u_{13} = e * o = m;$ $v_{14} = v_{13} * u_{14} = m * k = e;$
$v_{15} = v_{14} * u_{15} = e * e = b;$ $v_{16} = v_{15} * u_{16} = b * r = o.$

Proses *encipher* di atas menghasilkan *ciphertext* $v = ooeeiamkgnremebo$. Misalkan karena suatu hal *ciphertext* mengalami gangguan sehingga berubah menjadi $v' = ooeeiamkgnrerebo$, untuk mengetahui *plaintext* yang akan dihasilkan dilakukan proses *decipher* berikut:

$w_1 = a_1 \setminus v_1 = m \setminus o = a;$ $w_2 = v_1 \setminus v_2 = o \setminus o = m;$
$w_3 = v_2 \setminus v_3 = o \setminus e = b;$ $w_4 = v_3 \setminus v_4 = e \setminus e = i;$
$w_5 = v_4 \setminus v_5 = e \setminus i = l;$ $w_6 = v_5 \setminus v_6 = i \setminus a = u;$
$w_7 = v_6 \setminus v_7 = a \setminus m = a;$ $w_8 = v_7 \setminus v_8 = m \setminus k = n;$
$w_9 = v_8 \setminus v_9 = k \setminus g = g;$ $w_{10} = v_9 \setminus v_{10} = g \setminus n = d;$
$w_{11} = v_{10} \setminus v_{11} = n \setminus r = i;$ $w_{12} = v_{11} \setminus v_{12} = r \setminus e = l;$
$w_{13} = v_{12} \setminus v'_{13} = e \setminus r = a;$ $w_{14} = v'_{13} \setminus v_{14} = r \setminus e = l;$
$w_{15} = v_{14} \setminus v_{15} = e \setminus b = e;$ $w_{16} = v_{15} \setminus v_{16} = b \setminus o = r;$

diperoleh *plaintext* $f_\setminus(v') = u' = ambiluangdilaler$. Dari sini dapat diketahui bahwa kesalahan satu karakter dalam *ciphertext* tidak akan mengubah *plaintext* secara keseluruhan, sehingga metode ini dinilai tahan akan error. ■

Keunggulan lain dari metode ini adalah keamanan kunci rahasia yang relatif kuat (Markovski, dkk., 1997). Misalkan penyelundup mengetahui *ciphertext* $v = v_1 v_2 \dots v_k = f_*(u_1 u_2 \dots u_k)$, dengan $u_1 u_2 \dots u_k$ adalah kumpulan *plaintext* yang tidak diketahui. Sebagai contoh, untuk dapat mengetahui *quasigroup cipher* kiri $(A, *, \setminus, a_1, f_*, f_\setminus)$, dia harus bisa memecahkan sistem persamaan berikut:

$$v_1 = a_1 * u_1$$
$$v_2 = v_1 * u_2$$
$$\dots$$
$$v_k = v_{k-1} * u_k.$$

Sistem persamaan di atas memiliki banyak solusi *quasigroup*, yang artinya metode ini berhasil melawan serangan penyelundup (Markovski, dkk., 1997).

Akan tetapi jika penyelundup mengetahui *plaintext* dan *ciphertext*, maka dia bisa mengetahui *quasigroup* dengan mudah. Untuk menanggulangi kelemahan ini, digunakanlah dua buah *quasigroup* atau lebih sebagai kunci untuk proses *encipher* dan *decipher*. Misalkan $(A,*)$ dan $(A,*')$ adalah dua *quasigroup* yang berbeda dan bukan *dual* antara satu sama lain, dengan bentuk *quasigroup cipher* kiri masing-masing $(A,*,\backslash,a_1,f_*,f_\backslash)$ dan $(A,*',\backslash',a'_1,f_{*'},f_{\backslash'})$. Fungsi *encipher* dan *decipher*-nya menggunakan persamaan (Markovski, dkk., 1997):

$$f_e = f_{*'} \circ f_*, \qquad f_d = f_\backslash \circ f_{\backslash'}.$$

Untuk *quasigroup cipher* kanan, diambil *quasigroup* $(A,*)$ dan $(A,*')$ yang berbeda dan bukan *dual* antara satu sama lain, dengan bentuk *quasigroup cipher* kanan masing-masing $(A,*,/,a_1,f_*,f_/)$ dan $(A,*',/',a'_1,f_{*'},f_{/'})$. Fungsi *encipher* dan *decipher*-nya menggunakan persamaan:

$$f_e = f_{*'} \circ f_*, \qquad f_d = f_/ \circ f_{/'}.$$

Berikut diberikan contoh penerapan metode *double quasigroup cipher* dengan menggunakan *quasigroup cipher* kiri. Contoh ini dianggap telah mewakili *double quasigroup cipher* kanan.

Contoh 3.4.4

Misalkan $A = \{a,b,d,e,g,i,k,l,m,n,o,r,u\}$, hasil operasi biner pada *quasigroup* $(A,*)$ dan $(A,\backslash)$ didefinisikan oleh Tabel 25 dan Tabel 26 sebagaimana pada Contoh 3.4.3. Diberikan dua buah *quasigroup* lain yakni $(A,*')$ dan $(A,\backslash')$ yang hasil operasi binernya didefinisikan oleh Tabel 27 dan Tabel 28 berikut:

Tabel 27. *Quasigroup* $(A,*')$

$*'$	a	b	d	e	g	i	k	l	m	n	o	r	u
a	g	i	k	l	m	n	o	r	u	a	b	d	e
b	i	k	l	m	n	o	r	u	a	b	d	e	g
d	e	g	i	k	l	m	n	o	r	u	a	b	d
e	m	n	o	r	u	a	b	d	e	g	i	k	l
g	l	m	n	o	r	u	a	b	d	e	g	i	k
i	b	d	e	g	i	k	l	m	n	o	r	u	a
k	n	o	r	u	a	b	d	e	g	i	k	l	m
l	r	u	a	b	d	e	g	i	k	l	m	n	o
m	o	r	u	a	b	d	e	g	i	k	l	m	n
n	k	l	m	n	o	r	u	a	b	d	e	g	i
o	d	e	g	i	k	l	m	n	o	r	u	a	b
r	u	a	b	d	e	g	i	k	l	m	n	o	r
u	a	b	d	e	g	i	k	l	m	n	o	r	u

Tabel 28. *Quasigroup* $(A,\backslash')$

$\backslash'$	a	b	d	e	g	i	k	l	m	n	o	r	u
a	n	o	r	u	a	b	d	e	g	i	k	l	m
b	m	n	o	r	u	a	b	d	e	g	i	k	l
d	o	r	u	a	b	d	e	g	i	k	l	m	n
e	i	k	l	m	n	o	r	u	a	b	d	e	g
g	k	l	m	n	o	r	u	a	b	d	e	g	i
i	u	a	b	d	e	g	i	k	l	m	n	o	r
k	g	i	k	l	m	n	o	r	u	a	b	d	e
l	d	e	g	i	k	l	m	n	o	r	u	a	b
m	e	g	i	k	l	m	n	o	r	u	a	b	d
n	l	m	n	o	r	u	a	b	d	e	g	i	k
o	r	u	a	b	d	e	g	i	k	l	m	n	o
r	b	d	e	g	i	k	l	m	n	o	r	u	a
u	a	b	d	e	g	i	k	l	m	n	o	r	u

Sebagaimana pada Contoh 3.4.3, misalkan dipilih *m* sebagai *leader* sehingga $a_1 = m$ dan diberikan *plaintext* $u = ambiluangdiloker$. Setelah dilakukan proses *encipher* diperoleh *ciphertext* $v = ooeeiamkgnremebo$. Kemudian dilakukan proses *encipher* yang ke dua dengan menggunakan *quasigroup* $(A,*')$. Dipilih *o* sebagai *leader* sehingga $a'_1 = o$.

$w_1 = a'_1 *' v_1 = o *' o = u;$ $w_2 = w_1 *' v_2 = u *' o = o;$
$w_3 = w_2 *' v_3 = o *' e = i;$ $w_4 = w_3 *' v_4 = i *' e = g;$
$w_5 = w_4 *' v_5 = g *' i = u;$ $w_6 = w_5 *' v_6 = u *' a = a;$
$w_7 = w_6 *' v_7 = a *' m = u;$ $w_8 = w_7 *' v_8 = u *' k = k;$
$w_9 = w_8 *' v_9 = k *' g = a;$ $w_{10} = w_9 *' v_{10} = a *' n = a;$
$w_{11} = w_{10} *' v_{11} = a *' r = d;$ $w_{12} = w_{11} *' v_{12} = d *' e = k;$
$w_{13} = w_{12} *' v_{13} = k *' m = g;$ $w_{14} = w_{13} *' v_{14} = g *' e = o;$
$w_{15} = w_{14} *' v_{15} = o *' b = e;$ $w_{16} = w_{15} *' v_{16} = e *' o = i.$

Dari proses *encipher* yang ke dua, diperoleh *ciphertext* $w = uoiguaukaadkgoei$. Untuk mengembalikan *ciphertext* ini ke bentuk semula dilakukan dua kali proses *decipher*. Proses *decipher* yang pertama dengan menggunakan fungsi *decipher* pada *quasigroup* $(A,\backslash')$.

$x_1 = a'_1 \backslash' w_1 = o \backslash' u = o;$ $x_2 = w_1 \backslash' w_2 = u \backslash' o = o;$
$x_3 = w_2 \backslash' w_3 = o \backslash' i = e;$ $x_4 = w_3 \backslash' w_4 = i \backslash' g = e;$
$x_5 = w_4 \backslash' w_5 = g \backslash' u = i;$ $x_6 = w_5 \backslash' w_6 = u \backslash' a = a;$
$x_7 = w_6 \backslash' w_7 = a \backslash' u = m;$ $x_8 = w_7 \backslash' w_8 = u \backslash' k = k;$
$x_9 = w_8 \backslash' w_9 = k \backslash' a = g;$ $x_{10} = w_9 \backslash' w_{10} = a \backslash' a = n;$

$x_{11} = w_{10} \setminus' w_{11} = a \setminus' d = r;$ $x_{12} = w_{11} \setminus' w_{12} = d \setminus' k = e;$
$x_{13} = w_{12} \setminus' w_{13} = k \setminus' g = m;$ $x_{14} = w_{13} \setminus' w_{14} = g \setminus' o = e;$
$x_{15} = w_{14} \setminus' w_{15} = o \setminus' e = b;$ $x_{16} = w_{15} \setminus' w_{16} = e \setminus' i = o;$

Diperoleh *plaintext* sementaranya $x = ooeeiamkgnremebo$ yang mana $x = v$. Proses *decipher* yang ke dua dilakukan dengan menggunakan fungsi *decipher* pada *quasigroup* $(A,\setminus)$.

$y_1 = a_1 \setminus x_1 = m \setminus o = a;$ $y_2 = x_1 \setminus x_2 = o \setminus o = m;$
$y_3 = x_2 \setminus x_3 = o \setminus e = b;$ $y_4 = x_3 \setminus x_4 = e \setminus e = i;$
$y_5 = x_4 \setminus x_5 = e \setminus i = l;$ $y_6 = x_5 \setminus x_6 = i \setminus a = u;$
$y_7 = x_6 \setminus x_7 = a \setminus m = a;$ $y_8 = x_7 \setminus x_8 = m \setminus k = n;$
$y_9 = x_8 \setminus x_9 = k \setminus g = g;$ $y_{10} = x_9 \setminus x_{10} = g \setminus n = d;$
$y_{11} = x_{10} \setminus x_{11} = n \setminus r = i;$ $y_{12} = x_{11} \setminus x_{12} = r \setminus e = l;$
$y_{13} = x_{12} \setminus x_{13} = e \setminus m = o;$ $y_{14} = x_{13} \setminus x_{14} = m \setminus e = k;$
$y_{15} = x_{14} \setminus x_{15} = e \setminus b = e;$ $y_{16} = x_{15} \setminus x_{16} = b \setminus o = r.$

Dari proses *decipher* yang ke dua di atas diperoleh *plaintext* yang asli yakni, $y = ambiluangdiloker = u$. ■