BAB III

PENYANDIAN DAN PENGURAIAN SANDI GRUP

Pandang suatu rangkaian angka 0 dan atau 1 , misal (0001 .... 01) sebanyak k digit. Kemudian pandang (0,0,0,1, ... 0,1) sebanyak k digit, adalah elemen dari hasil kali grup $Z_2 \times Z_2 \times \ldots\ldots \times Z_2$ sebanyak k faktor yang notasinya ditulis Z_2^k. Sehingga rangkaian angka 0 dan atau 1 sebanyak k digit dapat dipandang sebagai elemen dari grup Z_2^k yang ditulis tanpa koma.

Grup Z_2^k mempunyai order 2^k, abelian dan setiap elemen x dalam Z_2^k yang tidak sama dengan 0 mempunyai order 2. Sebagai konsekwensi dari sifat tersebut diatas maka setiap x dalam Z_2^k yang tidak sama dengan 0 adalah invers dari dirinya sendiri ; yaitu $x = -x$.

3.1. PENGERTIAN PENYANDIAN

Definisi 3.1.1

Misal n dan k bilangan bulat positip dengan $k < n$

Pasangan sandi adalah fungsi $\emptyset : Z_2^k \longmapsto Z_2^n$ yang satu - satu.

Untuk teks biasa X dalam Z_2^k , $Y = \emptyset(X)$ dalam Z_2^n adalah teks sandi untuk teks biasa X atau teks sandi yang berhubungan dengan teks biasa X.

Contoh :

Diberikan,

$Z_2^3 = \{(000),(001),(010),(100),(011),(101),(110),(111)\}$,

$Z_2^4 = \{(0000),(0001),(0010),(0100),(1000),(0011),(0101),(1001),(0110),(1010),(1100),(0111)$,

(1011),(1101),(1110),(1111)}.

Didefinisikan fungsi $\emptyset : Z_2^3 \longmapsto Z_2^4$ dengan ,

$\emptyset((a_1a_2a_3)) = (1a_1a_2a_3)$, sehingga diperoleh :

$\emptyset((000)) = (1000)$

$\emptyset((001)) = (1001)$

$\emptyset((010)) = (1010)$

$\emptyset((100)) = (1100)$

$\emptyset((011)) = (1011)$

$\emptyset((101)) = (1101)$

$\emptyset((110)) = (1110)$

$\emptyset((111)) = (1111)$.

Maka $\emptyset : Z_2^3 \longmapsto Z_2^4$ merupakan pasangan sandi se

bab $\emptyset : Z_2^3 \longmapsto Z_2^4$ adalah satu - satu, yaitu

untuk sembarang x_1, x_2 dalam Z_2^3 , dimana jika $x_1 \neq x_2$

maka $\emptyset(x_1) \neq \emptyset(x_2)$.

Jadi,

teks sandi untuk teks biasa (000) adalah (1000)

teks sandi untuk teks biasa (001) adalah (1001)

danseterusmya.

3.2. PENGERTIAN SANDI GRUP

Definisi 3.2.1.

Pasangan sandi $\emptyset : Z_2^k \xrightarrow{\text{1-1}} Z_2^n$ disebut sandi

Grup jika Image dari $\emptyset$ adalah subgrup dari Z_2^n .

Contoh :

1. Diberikan,

$Z_2^3 = \{(000),(001),(010),(100),(011),(101),$
$(110),(111)\}$.

$Z_2^4 = \{(0000),(0001),(0010),(0100),(1000),(0011)$
$(0101),(1001),(0110),(1010),(1100),(0111)$

$(1011),(1101),(1110),(1111)\}$.

Didefinisikan fungsi $\emptyset : Z_2^3 \longmapsto Z_2^4$ sebagai berikut,

$(000) \longmapsto \emptyset((000)) = (0000)$

$(001) \longmapsto \emptyset((001)) = (0011)$

$(010) \longmapsto \emptyset((010)) = (0101)$

$(100) \longmapsto \emptyset((100)) = (1001)$

$(011) \longmapsto \emptyset((011)) = (0110)$

$(101) \longmapsto \emptyset((101)) = (1010)$

$(110) \longmapsto \emptyset((110)) = (1100)$

$(111) \longmapsto \emptyset((111)) = (1111)$.

Maka $\emptyset : Z_2^3 \longmapsto Z_2^4$ merupakan Sandi Grup, sebab

- $\emptyset : Z_2^3 \longmapsto Z_2^4$ jelas pasangan sandi.
- Misal K = Im(Ø) maka K terdiri dari

  a = (0000) e = (0110)

  b = (0011) f = (1010)

  c = (0101) g = (1100)

  d = (1001) h = (1111)

  Akan ditunjukkan K adalah subgrup dari Z_2^4.

+	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	e	f	c	d	h	g
c	c	e	a	g	b	h	d	f
d	d	f	g	a	h	b	c	e
e	e	c	b	h	a	g	f	d
f	f	d	h	b	g	a	e	c
g	g	h	d	c	f	e	a	b
h	h	g	f	e	d	c	b	a

- dengan memperhatikan tiap-tiap baris dan

tiap - tiap kolom terlihat bahwa tertutup dipenuhi.

- terdapat elemen Identitas yaitu a :
- setiap elemen mempunyai invers, dengan di tunjukkan bahwa elemen identitas selalu ada di tiap baris maupun di tiap kolom.

Definisi 3.2.2.

Pasangan sandi $\emptyset : Z_2^k \longmapsto Z_2^n$ disebut sandi Grup jika $\emptyset$ adalah homomorfisma grup.

Definisi 3.2.1 dapat disajikan dengan definisi 3,2.2. sebab menurut theorema 2.3.1 jika fungsi $\emptyset$ homomorfisma grup maka $Im(\emptyset)$ adalah subgrup dari Z_2^n.

Contoh :

Diberikan,

$Z_2^3 = \{(000),(001),(010),(100),(011),(101),(110),(111)\}$.

$Z_2^6 = \{(000000),(000001),(000010),(000100),.....$
$.... (111110),(111111)\}$.

Didefinisikan fungsi $\emptyset$ $Z_2^3 \longmapsto Z_2^6$ sebagai berikut

$(000) \longmapsto \emptyset((000)) = (000000)$

$(001) \longmapsto \emptyset((001)) = (001011)$

$(010) \longmapsto \emptyset((010)) = (010110)$

$(100) \longmapsto \emptyset((100)) = (100100)$

$(011) \longmapsto \emptyset((011)) = (011101)$

$(101) \longmapsto \emptyset((101)) = (100111)$

$(110) \longmapsto \emptyset((110)) = (111010)$

$(111) \longmapsto \emptyset((111)) = (110001)$

Maka $\emptyset : Z_2^3 \longmapsto Z_2^6$ merupakan sandi grup, sebab

- $\emptyset : Z_2^3 \longmapsto Z_2^6$ jelas satu - satu.
- jika diambil sembarang x_1, x_2 dalam Z_2^3 maka pas-

ti akan dipenuhi $\emptyset(x_1 + x_2) = \emptyset(x_1) + \emptyset(x_2)$, se hingga $\emptyset$ merupakan homomorfisma grup.

Misalnya $x_1 = (011)$, $x_2 = (100)$ maka

$x_1 + x_2 = (011) + (100) = (111)$. Selanjutnya

$\emptyset(x_1) = \emptyset((011)) = (011101)$, $\emptyset(x_2) = \emptyset((100))$

$= (101100)$ dan $\emptyset(x_1 + x_2) = \emptyset((111)) = (110001)$

Sedangkan $\emptyset(x_1) + \emptyset(x_2) = (011101) + (101100)$

$= (110001)$.

Jadi $\emptyset(x_1 + x_2) = \emptyset(x_1) + \emptyset(x_2)$.

3.3. SANDI GRUP DENGAN MATRIKS $C = [I \mid P]$

Sandi Grup dengan matriks $C = [I \mid P]$ adalah sandi yang terbentuk dengan menggunakan matriks C ukuran k x n dengan elemen - elemen 0 dan 1, dimana sandi yang terbentuk selalu mempunyai sifat k digit pertama dari teks sandi (sebut bagian ke 1 teks sandi) sama dengan teks biasanya. Selanjutnya n-k digit lainnya disebut bagian ke 2 teks sandi atau check digit. Sebagai akibatnya matriks C dapat dipecah menjadi dua bagian, yaitu matriks identitas I ukuran k x k yang membentuk bagian ke 1 teks sandi dan matriks P ukuran k x n-k yang membentuk bagian ke 2 teks sandi yang dipisahkan dengan garis putus - putus vertikal Sehingga notasinya ditulis $C = [I \mid P]$.

Cara mentransformasikan teks biasa ke teks sandi Grup dengan matriks $C = [I \mid P]$, adalah sebagai berikut :

- Terlebih dahulu ditentukan matriks C ukuran kxn dengan elemen 0 dan 1.
- Untuk setiap teks biasa $X = (x_1 x_2 \ldots x_k)$ diubah ke matriks baris $[X] = [x_1 \; x_2 \; \ldots \; x_k]$ kemudian dilakukan perkalian matriks $[X]\,C = [Y]$.

- Didefinisikan fungsi $\emptyset : Z_2^k \longmapsto Z_2^n$ sedemikian hingga $[Y] = \emptyset(X) = [X]\,C$, maka $\emptyset : Z_2^k \longmapsto Z_2^n$ merupakan sandi Grup.

Bukti

1. Ambil sembarang X_1, X_2 dalam Z_2^k , jika $X_1 \neq X_2$ maka $\emptyset(X_1) = [X_1]\,C \neq [X_2]\,C = \emptyset(X_2)$.
   Sehingga $\emptyset : Z_2^k \longmapsto Z_2^n$ adalah fungsi satu-satu.
   Jadi $\emptyset : Z_2^k \longmapsto Z_2^n$ dengan $\emptyset(X) = [X]\,C$ merupakan pasangan sandi.
2. Ambil sembarang X_1, X_2 dalam Z_2^k , maka $\emptyset\,(X_1 + X_2) = [X_1 + X_2]\,C$, karena perkalian matriks mempunyai sifat distributif maka

$$\begin{aligned}\emptyset(X_1 + X_2) &= [X_1 + X_2]\,C \\ &= [X_1]\,C + [X_2]\,C \\ &= \emptyset(X_1) + \emptyset(X_2).\end{aligned}$$

   Sehingga $\emptyset : Z_2^k \longmapsto Z_2^n$ merupakan homomorfisma grup.

- Ubah kembali matriks baris teks sandi ke bentuk teks sandinya.

Contoh :

Diberikan ,

$Z_2^3 = \{(000),(001),(010),(100),(011),(101),(110),(111)\}$.

Dengan menggunakan matriks C dimana,

$$C = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

akan ditentukan sandi Grupnya.

Karena matriks nya berukuran 3 x 5 maka fungsinya adalah $\emptyset : Z_2^3 \longmapsto Z_2^5$, sedemikian hingga ,

$$\phi(X) = [X]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right], \quad X \text{ dalam } Z_2^3$$

Sehingga diperoleh,

$$\phi((000)) = [0\ 0\ 0]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [0\ 0\ 0\ 0\ 0]$$

$$\phi((001)) = [0\ 0\ 1]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [0\ 0\ 1\ 0\ 1]$$

$$\phi((010)) = [0\ 1\ 0]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [0\ 1\ 0\ 1\ 1]$$

$$\phi((100)) = [1\ 0\ 0]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [1\ 0\ 0\ 1\ 0]$$

$$\phi((011)) = [0\ 1\ 1]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [0\ 1\ 1\ 1\ 0]$$

$$\phi((101)) = [1\ 0\ 1]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [1\ 0\ 1\ 1\ 1]$$

$$\phi((110)) = [1\ 1\ 0]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [1\ 1\ 0\ 0\ 1]$$

$$\phi((111)) = [1\ 1\ 1]\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right] = [1\ 1\ 1\ 0\ 0]$$

Jadi sandi Grupnya adalah

$\{(00000),(00101),(01011),(10010),(01110),(10111),$
$(11001),(11100)\}$

3.4. SANDI GRUP DENGAN POLYNOMIAL PENGGANDA C(x)

Sandi Grup dengan polynomial pengganda C(x) adalah sandi yang dibentuk dengan menggunakan polynomial penggan da $C(x) = c_1x^0 + c_2x^1 + \ldots + c_{n-k+1}x^{n-k}$ anggauta $Z_2[x]$.

Adapun cara penyandiannya adalah sebagai berikut :

- Teks biasa, misal $X = (x_1x_2 \ldots x_k)$ diubah menjadi bentuk polynomial $x_1x^0 + x_2x^1 + \ldots + x_kx^{k-1}$ dengan derajat terbesar k-1.
  Sebagai contoh misal (10101) diubah menjadi $1x^0 + 0x^1 + 1x^2 + 0x^3 + 1x^4 = 1 + x^2 + x^4$. Sebaliknya $1 + x^2 + x^4$ dapat diubah kembali menjadi (10101). Untuk selanjutnya (10101) disebut rangkaian koefisien dari $1 + x^2 + x^4$.
- Ditentukan polynomial sembarang $C(x) = c_1x^0 + c_2x^1 + c_3x^2 + \ldots + c_{n-k+1}x^{n-k}$ dalam $Z_2[x]$ dengan derajat n-k dan $c_1 = 1$.
- Didefinisikan fungsi $\emptyset : Z_2^k \longmapsto Z_2^n$ sedemikian hingga $\emptyset(X) = \emptyset((x_1x_2 \ldots x_k))$ = rangkaian koefisien dari hasil pergandaan antara polynomial $x_1x^0 + x_2x^1 + \ldots + x_kx^{k-1}$ dengan polynomial C(x).
  Maka $\emptyset : Z_2^k \longmapsto Z_2^n$ merupakan sandi Grup.

  Bukti

  1. Ambil sembarang $X_1 = (x_{11}x_{12} \ldots x_{1k})$, $X_2 = (x_{21}x_{22} \ldots x_{2k})$ dalam Z_2^k. Jika $X_1 \neq X_2$, maka $x_{11}x^0 + x_{12}x^1 + \ldots + x_{1k}x^{k-1} = x_{21}x^0 + x_{22}x^1 + \ldots + x_{2k}x^{k-1}$. Sehingga $\emptyset(X_1) = C(x).(x_{11}x^0 + x_{12}x^1 + \ldots + x_{1k}x^{k-1}) \neq C(x).(x_{21}x^0 + x_{22}x^1 + \ldots + x_{2k}x^{k-1}) = \emptyset(X_2)$.

Maka $\emptyset : Z_2^k \longmapsto Z_2^n$ fungsi satu - satu ,sehingga merupakan pasangan sandi.

2. Ambil sembarang $X_1 = (x_{11}x_{12} \ldots\ldots x_{1k})$, $X_2 = (x_{21}x_{22} \ldots x_{2k})$ dalam Z_2^k .

$\emptyset(X_1 + X_2)$

= rangkaian koefisien dari

$C(x).\left[(x_{11}+ x_{21})x^0+(x_{12}+x_{22})x^1 + \ldots\ldots + (x_{1k}+ x_{2k})x^{k-1}\right]$

= rangkaian koefisien dari

$C(x).\left[(x_{11}x^0+x_{12}x^1+ \ldots x_{1k}x^{k-1})+(x_{21}x^0 + x_{22}x^1+ \ldots + x_{2k}x^{k-1})\right]$.

= rangkaian koefisien dari

$C(x).(x_{11}x^0+ x_{12}x^1+ \ldots + x_{1k}x^{k-1})$ +

$C(x).(x_{21}x^0+ x_{22}x^1+ \ldots + x_{2k}x^{k-1})$.

= rangkaian koefisien dari

$C(x).(x_{11}x^0+ x_{12}x^1+ \ldots + x_{1k}x^{k-1})$ +

rangkaian koefisien dari

$C(x).(x_{21}x^0+ x_{22}x^1+ \ldots + x_{2k}x^{k-1})$.

$= \emptyset(X_1) + \emptyset(X_2)$.

Karena dipenuhi $\emptyset(X_1+ X_2) = \emptyset(X_1) + \emptyset(X_2)$, maka $\emptyset : Z_2^k \longmapsto Z_2^n$ merupakan homomorfisma grup.

Jadi terbukti pasangan sandi $\emptyset : Z_2^k \longmapsto Z_2^n$ merupakan sandi Grup.

Dan polynomial C(x) disebut polynomial penggan-da.

Contoh :

Diberikan,

$Z_2^4 = \{(0000),(0001),(0010),(0100),(1000),(0011)$,

(0101),(1001),(0110),(1010),(1100),(0111),(1011),
(1101),(1110),(1111)}

Akan ditentukan sandi Grupnya dengan menggunakan polynomial $1 + x^2 + x^3$.

Karena derajat dari polynomial penggandanya sama dengan 3 maka fungsinya $\emptyset : Z_2^4 \longmapsto Z_2^7$, dengan

$\emptyset((x_1 x_2 x_3 x_4))$ = rangkaian koefisien dari

$(1 + x^2 + x^3).(x_1 x^0 + x_2 x^1 + x_3 x^2 + x_4 x^3)$

Sehingga

$\emptyset((0000))$ = rangkaian koefisien dari

$(1 + x^2 + x^3).(0x^0 + 0x^1 + 0x^2 + 0x^3)$

= rangkaian koefisien dari

$(0x^0 + 0x^1 + 0x^2 + 0x^3 + 0x^4 + 0x^5 + 0x^6)$

= (0000000)

$\emptyset((0001))$ = rangkaian koefisien dari

$(1 + x^2 + x^3).(0x^0 + 0x^1 + 0x^2 + 1x^3)$

= rangkaian koefisien dari

$(0x^0 + 0x^1 + 0x^2 + 1x^3 + 0x^4 + 1x^5 + 1x^6)$

= (0001011)

demikian juga untuk teks - teks biasa lainnya lakukan dengan cara yang sama seperti diatas, akan diperoleh :

$\emptyset((0010))$ = (0010110)

$\emptyset((0100))$ = (0101100)

$\emptyset((1000))$ = (1011000)

$\emptyset((0011))$ = (0011101)

$\emptyset((0101))$ = (0100111)

$\emptyset((1001))$ = (1010011)

$\emptyset((0110))$ = (0111010)

$\emptyset((1010))$ = (1001110)

$\emptyset((1100)) = (1110100)$

$\emptyset((0111)) = (0110001)$

$\emptyset((1011)) = (1000101)$

$\emptyset((1101)) = (1111111)$

$\emptyset((1110)) = (1100010)$

$\emptyset((1111)) = (1101001)$

Jadi sandi grupnya adalah,

$\{$ (0000000),(0001011),(0010110),(0101100),(1011000),
(0011101),(0100111),(1010011),(0111010),(1001110),
(1110100),(0110001),(1000101),(1111111),(1100010),
(1101001) $\}$.

3.5. PENGURAIAN SANDI

Penguraian sandi adalah merubah teks sandi menjadi teks biasa. Untuk menguraikan teks sandi Grup menjadi teks biasa, terlebih dahulu dilihat pembentuknya.

Sandi Grup $\emptyset : Z_2^k \longmapsto Z_2^n$ yang dibentuk dengan menggunakan matriks $C = [I \mid P]$ ukuran k x n, teks sandi dirubah menjadi teks biasa dimana teks biasa = k digit pertama dari teks sandi.

Sandi Grup $\emptyset : Z_2^k \longmapsto Z_2^n$ yang dibentuk dengan polynomial pengganda C(x), pertama teks sandi dirubah menjadi bentuk polynomial. Kemudian polynomial dari teks sandi dibagi dengan polynomial pengganda C(x). Selanjutnya teks biasa = rangkaian koefisien dari hasil bagi antara polynomial dari teks sandi dengan polynomial pengganda C(x).

Contoh :

1. Diterima teks sandi (001011) yang dibentuk dengan matriks $C = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$

Karema matriks yang digunakan berukuran 3 x 6 maka fungsinya $\emptyset : Z_2^3 \longmapsto Z_2^6$.

Sehingga teks biasa = 3 digit pertama dari teks sandi (001011) ; yaitu (001).

2. Diterima sandi Grup (1001110) dalam Z_2^7 dengan pengganda $1 + x^2 + x^3$.

   Karena polynomial penggandanya mempunyai derajat 3 maka fungsinya $\emptyset : Z_2^4 \longmapsto Z_2^7$.

   Polynomial dari teks sandi adalah $1x^0 + 0x^1 + 0x^2 + 1x^3 + 1x^4 + 1x^5 + 0x^6 = 1 + x^3 + x^4 + x^5$.

   Selanjutnya polynomial dari teks sandi dibagi dengan polynomial pengganda dengan cara seba - gai berikut

$$
\begin{array}{r|l}
 & x^2 + 1 \\
\hline
1+x^2+x^3 & x^5 + x^4 + x^3 + \quad + 1 \\
 & x^5 + x^4 + \quad + x^2 \quad - \\
\hline
 & \quad\quad x^3 + x^2 \quad + 1 \\
 & \quad\quad x^3 + x^2 \quad + 1 \quad - \\
\hline
 & \quad\quad\quad\quad 0
\end{array}
$$

   Sehingga teks biasanya = rangkaian koefisien dari $(1 + x^2)$ = (1010).