BAB V

K E S I M P U L A N

Sandi Grup adalah sandi yang berbentuk rangkaian angka 0 dan atau 1 sebanyak n digit, yang berasal dari teks biasa yang berbentuk rangkaian angka 0 dan atau 1 sebanyak k digit dengan $k < n$.

Metode penyandian sandi Grup yaitu menggunakan definisi suatu fungsi dan teori homomorfisma grup yang berdasar pada Grup dari himpunan bilangan bulat modulo dua.

Fungsi tersebut diatas didefinisikan dengan menggunakan matriks $C = \left[\begin{array}{c|c} I & P \end{array}\right]$ ukuran k x n dengan elemen 0 dan 1, atau dengan polynomial derajat n-k dan bagian konstan 1 anggauta $Z_2[x]$. Selanjutnya untuk sandi Grup yang dibentuk dengan menggunakan matriks $C = \left[\begin{array}{c|c} I & P \end{array}\right]$, disebut sandi Grup dengan matriks $C = \left[\begin{array}{c|c} I & P \end{array}\right]$ sedangkan untuk sandi Grup yang dibentuk dengan menggunakan polynomial derajat n-k dengan bagian konstan 1 anggauta $Z_2[x]$ disebut sandi Grup dengan polynomial pengganda C(x).

Cara mendeteksi kesalahan pengiriman sandi Grup dengan matriks $C = \left[\begin{array}{c|c} I & P \end{array}\right]$, teks sandi $(z_1 z_2 \ldots\ldots z_n)$ yang diterima dikonversikan ke matriks baris $[z_1\ z_2 \ldots \ldots\ z_n]$, kemudian lakukan perkalian matriks

$$[z_1\ z_2 \ldots\ z_n] \begin{bmatrix} P \\ \hline I \end{bmatrix}$$

, jika hasilnya matriks 0 maka teks sandi yang diterima adalah benar. Sedangkan jika hasilnya bukan matriks 0 maka teks sandi yang diterima adalah teks sandi yang salah.

Cara mendeteksi kesalahan pengiriman sandi Grup dengan polynomial pengganda C(x), teks sandi yang diterima dikonversikan ke bentuk polynomial. Kemudian polynomial dari teks sandi yang diterima dibagi dengan polynomial pengganda C(x). Jika sisanya sama dengan 0 maka teks sandi yang diterima benar. Jika sisanya tidak sama dengan 0 maka teks sandi yang diterima salah.

Cara mengoreksi kesalahan pengiriman sandi Grup, teks sandi yang diterima dicari syndromenya. Dari syndrome tersebut akan didapatkan pola kesalahannya. Kemudian pola kesalahan yang diperoleh dijumlahkan pada teks sandi yang diterima.

Adapun syndrome dari teks sandi Grup dengan matriks C = $\left[\begin{array}{c|c} I & P \end{array}\right]$ adalah hasil kali antara matriks baris dari teks sandi yang diterima dengan matriks $\left[\begin{array}{c} P \\ \hline I \end{array}\right]$, dan syndrome dari teks sandi Grup dengan polynomial pengganda C(x) adalah sisa pembagian antara polynomial dari teks sandi yang diterima dengan polynomial pengganda C(x).