

### BAB III

#### P E N Y A N D I A N

( Pembentukan teks biasa menjadi teks sandi )

Sebagai langkah awal dalam sandi Hill, dipasangkan urutan abjad baku dengan nilai numerik yang menyatakan posisinya. Dengan catatan untuk abjad Z diberi nilai 0. Untuk lebih jelasnya bisa dilihat pada tabel 1.

Tabel 1 :

A	B	C	D	E	F	G	H	I	J	K	L	M
↑	↓	↑	↓	↑	↓	↑	↓	↑	↓	↑	↓	↑
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↑	↓	↑	↓	↑	↓	↑	↓	↑	↓	↑	↓
14	15	16	17	18	19	20	21	22	23	24	25	0

Dikutip dari: Cryptography in An Algebraic Alphabet

Kunci dari penyusunan sandi n-Hill adalah adanya matriks bujursangkar ukuran  $n \times n$  dengan elemen-elemen bilangan bulat.

#### 3.1. SANDI 2-HILL

Definisi 20 :

Sandi 2-Hill adalah sandi yang terbentuk dengan menggunakan matriks transformasi ukuran  $2 \times 2$  dengan elemen-elemen bilangan bulat.

Prosedur mentransformasikan teks biasa ke teks sandi 2 - Hill adalah sebagai berikut :

Langkah 1 :

Ditentukan terlebih dahulu matriks ukuran  $2 \times 2$ , dengan elemen bilangan bulat, misalkan matriks A.

$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ ; Persyaratan tambahan tertentu pada A akan diuraikan pada bab selanjutnya.

Langkah 2 :

Huruf-huruf teks biasa yang berurutan dikelompokkan ke dalam pasangan-pasangan, satu pasang 2 huruf dan bila jumlah huruf merupakan bilangan ganjil untuk huruf yang terakhir dipasangkan dengan huruf 'boneka' sebarang. Kemudian mengganti masing-masing huruf teks biasa tersebut dengan nilai numeriknya, sesuai dengan tabel 1.

Langkah 3 :

Secara berurutan konversikan masing-masing pasangan teks biasa  $p_1, p_2$  ke matriks kolom.

$$p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

dan dibentuk perkalian matriks  $A p = c$ , akan diperoleh matriks kolom teks sandi yaitu  $c$ .

Langkah 4 :

Konversikan kembali masing-masing matriks kolom teks sandi ke abjadnya yang setara, yaitu sesuai dengan tabel 1.

Di bawah ini akan diberikan sebuah contoh penyandian dengan sandi 2-Hill.

Akan disusun menjadi teks sandi 2-Hill untuk sebuah pesan yang berbunyi : AWAS MUSUH DATANG dengan menggunakan matriks K , dimana dipilih

$$K = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$$

Penyelesaian penyandian :

Karena jumlah huruf pada AWAS MUSUH DATANG merupakan bilangan ganjil, maka menurut prosedur sandi 2-Hill harus ditambahkan sebuah huruf boneka sebarang pada akhir kalimat, misalnya huruf "G". Sehingga menjadi AWAS MUSUH DATANGG. Selanjutnya masing-masing huruf teks diganti dengan nilai numeriknya dan dikelompokkan dua-dua.

A	W	A	S	M	U	S	U
↓	↓	↓	↓	↓	↓	↓	↓
1	23	1	19	13	21	19	21
H	D	A	T	A	N	G	G
↓	↓	↓	↓	↓	↓	↓	↓
8	4	1	20	1	14	7	7

Masing-masing pasangan nilai dikonversikan dalam matriks kolom, misal untuk pasangan AW yaitu :

$$p = \begin{bmatrix} 1 \\ 23 \end{bmatrix}$$

kemudian dibentuk perkalian matriks p dengan matriks K , sehingga diperoleh :

$$c = K p = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 23 \end{bmatrix} = \begin{bmatrix} 47 \\ 69 \end{bmatrix}$$

Demikian juga untuk pasangan huruf lainnya.

This document is submitted by the author(s). The author(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for the purpose of security, back-up and preservation:

AS :

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 19 \end{bmatrix} = \begin{bmatrix} 39 \\ 57 \end{bmatrix}$$

MU : 
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 21 \end{bmatrix} = \begin{bmatrix} 55 \\ 63 \end{bmatrix}$$

SU : 
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 21 \end{bmatrix} = \begin{bmatrix} 61 \\ 63 \end{bmatrix}$$

HD : 
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 8 \\ 4 \end{bmatrix} = \begin{bmatrix} 16 \\ 12 \end{bmatrix}$$

AT : 
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 41 \\ 60 \end{bmatrix}$$

AN : 
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 14 \end{bmatrix} = \begin{bmatrix} 29 \\ 42 \end{bmatrix}$$

GG : 
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 7 \\ 7 \end{bmatrix} = \begin{bmatrix} 21 \\ 21 \end{bmatrix}$$

Kemudian dari hasil-hasil yang diperoleh dikonversikan kembali ke abjadnya yang setara sesuai tabel 1. Tetapi timbul masalah bahwa terdapat angka-angka yang lebih besar dari 25, padahal pada tabel 1 terbatas sampai bilangan 25. Maka untuk memecahkan masalah tersebut dibuat suatu permufakatan.

#### PERMUFAKATAN :

Jika terjadi bilangan lebih besar dari 25 akan digantikan dengan sisa yang dihasilkan jika bilangan tersebut dibagi 26.

Karena sisa setelah pembagian oleh 26 adalah salah satu dari bilangan-bilangan bulat  $0, 1, 2, \dots, 25$ ;

maka prosedur ini akan selalu menghasilkan bilangan bulat dengan abjad yang setara. Hal ini sesuai dengan teori tentang perhitungan modular.

Dengan demikian untuk hasil-hasil perkalian terse

but di atas dapat desederhanakan menjadi :

$$\begin{array}{llll}
 \text{AW} \rightarrow \begin{bmatrix} 21 \\ 17 \end{bmatrix} & \text{AS} \rightarrow \begin{bmatrix} 13 \\ 5 \end{bmatrix} & \text{MU} \rightarrow \begin{bmatrix} 3 \\ 11 \end{bmatrix} & \text{SU} \rightarrow \begin{bmatrix} 9 \\ 11 \end{bmatrix} \\
 \text{HD} \rightarrow \begin{bmatrix} 16 \\ 21 \end{bmatrix} & \text{AT} \rightarrow \begin{bmatrix} 15 \\ 8 \end{bmatrix} & \text{AN} \rightarrow \begin{bmatrix} 3 \\ 16 \end{bmatrix} & \text{GG} \rightarrow \begin{bmatrix} 21 \\ 21 \end{bmatrix}
 \end{array}$$

Langkah terakhir, matrik-matrik yang diperoleh berpadanan dengan pasangan-pasangan teks sandi (lihat pada tabel 1), yaitu :

$$\begin{array}{ccccc}
 21 & 17 & 13 & 5 & 3 & 11 & 9 & 11 \\
 \downarrow & \downarrow \\
 U & Q & M & E & C & K & I & K \\
 16 & 21 & 15 & 8 & 3 & 16 & 21 & 21 \\
 \downarrow & \downarrow \\
 P & L & O & H & C & P & U & U
 \end{array}$$

dan biasanya dikirim sebagai untaian tunggal (single string) tanpa spasi yaitu :

UQMECKIKPLOHCPUU

### 3.2. SANDI 3-HILL

Definisi 21 :

Sandi 3-Hill adalah sandi yang terbentuk dengan menggunakan matriks transformasi berukuran  $3 \times 3$  dengan elemen-elemen bilangan bulat.

Prosedur mentransformasikan teks biasa ke teks sandi 3-Hill adalah sebagai berikut :

Langkah 1 :

This document is under Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission or parts of it into another language and store it in electronic format. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:

Ditentukan terlebih dahulu matriks bujursangkar ukuran  $3 \times 3$  dengan elemen bilangan bulat, misalkan

$$B = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Persyaratan tambahan tertentu pada B akan diuraikan pada bab selanjutnya.

Langkah 2 :

Huruf-huruf teks biasa yang berurutan dikelompokan ke dalam pasangan-pasangan, satu pasang "3" huruf dan bila pasangan huruf terakhir kurang dari 3 maka diberi huruf boneka sebarang seperlunya. Kemudian mengganti masing-masing huruf teks biasa tersebut dengan nilai numeriknya (sesuai tabel 1).

Langkah 3 :

Secara berurutan masing-masing pasangan teks biasa  $p_1 p_2 p_3$  dikonversikan menjadi matriks kolom misal p.

$$p = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

dan dibentuk perkalian matriks  $B p = c$ . Akan diperoleh matriks kolom teks sandi yaitu c.

Langkah 4 :

Konversikan kembali masing-masing matriks kolom teks sandi ke abjadnya yang setara (lihat tabel 1)

Dibawah ini akan diberikan sebuah contoh penyandian dengan sandi 3-Hill.

Akan disusun teks sandi 3-Hill untuk sebuah pesan berisi : AWAS MUSUH DATANG dengan menggunakan matriks B,

dimana dipilih

$$B = \begin{bmatrix} 1 & 3 & 1 \\ 0 & 5 & 1 \\ 1 & 2 & 3 \end{bmatrix}$$

Penyelesaian penyandian :

Karena jumlah huruf yang akan disandikan tepat ke-lipatan 3, maka dalam hal ini tidak memerlukan huruf "boneka". Selanjutnya masing-masing huruf teks diganti dengan nilai numeriknya (pandang tabel 1) dan kemudian dielompokkan tiga-tiga.

A	W	A	S	M	U	S	U	H	D	A	T
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	23	1	19	13	21	19	21	8	4	1	20
A	N	G									
↓	↓	↓									
1	14	7									

Masing-masing pasangan nilai dikonversikan dalam matriks kolom dan kemudian dibentuk perkalian matriks dengan matriks B dan dengan berpegang pada PERMUFAKATAN yang ada.

$$\text{AWA : } \begin{bmatrix} 1 & 3 & 1 \\ 0 & 5 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 23 \\ 1 \end{bmatrix} = \begin{bmatrix} 71 \\ 116 \\ 50 \end{bmatrix} = \begin{bmatrix} 19 \\ 12 \\ 24 \end{bmatrix} \pmod{26}$$

$$\text{SMU : } \begin{bmatrix} 1 & 3 & 1 \\ 0 & 5 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 13 \\ 21 \end{bmatrix} = \begin{bmatrix} 79 \\ 86 \\ 108 \end{bmatrix} = \begin{bmatrix} 1 \\ 8 \\ 4 \end{bmatrix} \pmod{26}$$

$$\text{SUH : } \begin{bmatrix} 1 & 3 & 1 \\ 0 & 5 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 21 \\ 8 \end{bmatrix} = \begin{bmatrix} 90 \\ 113 \\ 85 \end{bmatrix} = \begin{bmatrix} 12 \\ 9 \\ 7 \end{bmatrix} \pmod{26}$$

$$\text{DAT : } \begin{bmatrix} 1 & 3 & 1 \\ 0 & 5 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 4 \\ 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 27 \\ 25 \\ 66 \end{bmatrix} = \begin{bmatrix} 1 \\ 25 \\ 14 \end{bmatrix} \pmod{26}$$

$$\text{ANG : } \begin{bmatrix} 1 & 3 & 1 \\ 0 & 5 & 1 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 50 \\ 77 \\ 50 \end{bmatrix} = \begin{bmatrix} 24 \\ 25 \\ 24 \end{bmatrix} \pmod{26}$$

Kembali dengan menggunakan tabel 1 diperoleh huruf-huruf yang berpadanan dengan bilangan-bilangan yang didapat dari perkalian 2 matriks di atas, sehingga diperoleh :

$$\begin{array}{ccc}
 19 & 12 & 24 \\
 \downarrow & \downarrow & \downarrow \\
 S & L & X
 \end{array}
 \quad
 \begin{array}{ccc}
 1 & 8 & 4 \\
 \downarrow & \downarrow & \downarrow \\
 A & H & D
 \end{array}
 \quad
 \begin{array}{ccc}
 12 & 9 & 7 \\
 \downarrow & \downarrow & \downarrow \\
 L & I & G
 \end{array}
 \quad
 \begin{array}{ccc}
 1 & 25 & 14 \\
 \downarrow & \downarrow & \downarrow \\
 A & Y & N
 \end{array}$$
  

$$\begin{array}{ccc}
 24 & 25 & 24 \\
 \downarrow & \downarrow & \downarrow \\
 X & Y & X
 \end{array}$$

karena biasanya sandi ditulis tanpa spasi maka sandi 3-Hill untuk AWAS MUSUH DATANG adalah :

SLXAHDLIGAYNXYX

### 3.3. SANDI n-HILL

Definisi 22 :

Jika  $A$  adalah matriks untuk melaksanakan penyandian ukuran  $n \times n$  dengan elemen bilangan bulat :

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \quad p = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

dan matriks kolom  $p$  yaitu konversi dari pasangan huruf teks biasa yang terdiri atas  $n$  huruf, dengan  $p_1, p_2, \dots, p_n$  adalah nilai numerik dari huruf yang sesuai (pandang tabel 1) maka  $c = Ap$  adalah matriks kolom teks sandi yang terbentuk.

Di bawah ini akan diperlihatkan contoh untuk sandi n-Hill dan diambil  $n = 5$ . (<http://eprints.undip.ac.id>)

Direncanakan mengirim pesan berisi : AWAS MUSUH DATANG dalam bentuk sandi 5-Hill dengan menggunakan matriks bujursangkar  $5 \times 5$  sebagai berikut :

$$\begin{bmatrix} 1 & 2 & 0 & -1 & 2 \\ 1 & 0 & -1 & 2 & -1 \\ 0 & 1 & 1 & 1 & 0 \\ 2 & -1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 \end{bmatrix}$$

$$\begin{array}{lllllllll} A & W & A & S & M & U & S & U & H & D \\ \downarrow & \downarrow \\ 1 & 23 & 1 & 19 & 13 & 21 & 19 & 21 & 8 & 4 \end{array}$$

$$\begin{array}{llll} A & T & A & N & G \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 20 & 1 & 14 & 7 \end{array}$$

AWASM :

$$\begin{bmatrix} 1 & 2 & 0 & -1 & 2 \\ 1 & 0 & -1 & 2 & -1 \\ 0 & 1 & 1 & 1 & 0 \\ 2 & -1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 23 \\ 1 \\ 19 \\ 13 \end{bmatrix} = \begin{bmatrix} 54 \\ 25 \\ 43 \\ 11 \\ 71 \end{bmatrix} = \begin{bmatrix} 2 \\ 25 \\ 17 \\ 11 \\ 19 \end{bmatrix} \pmod{26}$$

USUHD :

$$\begin{bmatrix} 1 & 2 & 0 & -1 & 2 \\ 1 & 0 & -1 & 2 & -1 \\ 0 & 1 & 1 & 1 & 0 \\ 2 & -1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 \end{bmatrix} \begin{bmatrix} 21 \\ 19 \\ 21 \\ 8 \\ 4 \end{bmatrix} = \begin{bmatrix} 59 \\ 12 \\ 48 \\ 35 \\ 98 \end{bmatrix} = \begin{bmatrix} 7 \\ 12 \\ 22 \\ 9 \\ 20 \end{bmatrix} \pmod{26}$$

ATANG :

$$\begin{bmatrix} 1 & 2 & 0 & -1 & 2 \\ 1 & 0 & -1 & 2 & -1 \\ 0 & 1 & 1 & 1 & 0 \\ 2 & -1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \\ 1 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 41 \\ 21 \\ 35 \\ 3 \\ 51 \end{bmatrix} = \begin{bmatrix} 15 \\ 21 \\ 9 \\ 3 \\ 25 \end{bmatrix} \pmod{26}$$

Sehingga diperoleh :

$$\begin{array}{ccccccccc} 2 & 25 & 17 & 11 & 19 & 7 & 12 & 22 & 9 & 20 \\ \downarrow & \downarrow \\ B & Y & Q & K & S & G & L & V & I & T \\ 15 & 21 & 9 & 3 & 25 & & & & & \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & & & & \\ O & U & I & C & Y & & & & & \end{array}$$

Maka teks sandi yang terjadi adalah : BYQKSGLVITOUICY

Dengan melihat tiga contoh di atas yaitu sandi 2-Hill, 3-Hill dan 5-Hill, ternyata suatu kalimat teks bisa yang sama menghasilkan teks sandi yang berlainan. Demikian juga bila sama-sama disandikan dengan sandi 5-Hill akan menghasilkan teks sandi yang berbeda jika elemen-elemen pada kedua matriks penyandiannya berlainan.