

## BAB IV TEKNIK KRIPTOGRAFI KUNO I

### 4.1 Teknik Kriptografi Klasik/Kuno I

(idokeren 2018) Kriptografi klasik/kuno merupakan Teknik substitusi yaitu penggantian setiap karakter teks asli dengan karakter lainnya, salah satu teknik substitusi pada kriptografi Klasik/Kuno adalah kode kaisar, yang beradaptasi pada penggunaan 'Roda Kaisar'.

#### 4.1.1 Monoalphabet

Perhatikan alphabet plaintext dibawah ini

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

*Gambar 4.1 Contoh Monoalphabet*

Misal, Jika penggeseran yang dilakukan sebanyak 3 kali maka kunci untuk deskripsinya adalah 3. Maka susunan huruf untuk ciphertext adalah:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

*Gambar 4.2 Contoh Monoalphabet*

Contoh Tentukan chipper text dari plaintext 'K R I P T O G R A F I'!

Plaintext : K R I P T O G R A F I

Ciphertext : N U L S W R J U D I L

#### 4.1.2 Polyalphabet

Merupakan gagasan baru dalam perkembangan kode kaisar untuk menggunakan kunci laian yang di sebut Polyalphabetic. Teknik ini cenderung menggunakan kunci berupa huruf dan **tidak ada penggunaan huruf yang di ulang**. Penggunaan tidak hanya dengan satu kunci tetapi bisa menggunakan lebih dari satu kunci.

##### 1. Satu kunci

Plaintext : B E L A J A R K R I P T O G R A F I

Kunci : M E R D E K 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
m	e	R	d	k	a	b	c	f	g	h	i	j	l	n	o	p	q	s	t	u	v	w	x	y	z

*Gambar 4.3 Contoh Polyalphabet 1 Kunci*

Ciphertext : E K I M G M Q H Q F O T N B Q M A F

##### 2. Dua Kunci

Plaintext : B E L A J A R K R I P T O G R A F I

Kunci 1 : M E R D E K A

Kunci 2 : I N D O N E S I A

Kunci 1: MERDEKA																									
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
m	e	r	d	k	a	b	c	f	g	h	i	j	l	n	o	p	q	s	t	u	v	w	x	y	z

  

Kunci 2: INDONESIA																									
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
i	n	d	o	e	s	a	b	c	f	g	h	j	k	l	m	p	q	r	t	u	v	w	x	y	z

Gambar 4.4 Contoh Polyalphabet 2 Kunci

Ciphertext : EGCJAJP BPSLTKNPJIS

### 3. Tiga Kunci

Plaintext : CEGAH PEGAWAI KPK

Kunci 1 : MERDEKA

Kunci 2 : INDONESIA

Kunci 3 : PUTIH MERAH

Kunci 1: MERDEKA																									
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
m	e	r	d	k	a	b	c	f	g	h	i	j	l	n	o	p	q	s	t	u	v	w	x	y	z

  

Kunci 2: INDONESIA																									
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
i	n	d	o	e	s	a	b	c	f	g	h	j	k	l	m	p	q	r	t	u	v	w	x	y	z

  

Kunci 3: PUTIH MERAH																									
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
p	u	t	i	h	m	e	r	a	b	c	d	f	g	j	k	l	n	o	q	s	v	w	x	y	z

Ciphertext: LEGBIDEGWBBOUDU

Gambar 4.5 Contoh Polyalphabet 3 Kunci

Ciphertext : LEGBIDEGWBBOUDU

### Soal

1. Buatlah ciphertext dari POHON HIJAU dengan menggunakan kode geser 3!
2. Buatlah ciphertext dari TELEVISI dengan menggunakan kode geser 5!

## BAB V TEKNIK KRIPTOGRAFI KUNO II & III

### 5.1 Teknik Kriptografi Klasik/Kuno II

(Kriptografi 2020) Metode dengan menggunakan lebih dari satu kunci terdiri dari 3 bagian yaitu blok, karakter, dan zigzag:

#### 5.1.1 Blok

Membagi jumlah teks-asli menjadi blok-blok yang ditentukan, tergantung dari keinginan pengirim pesan.

Plaintext : **PERHATIKAN RAKYAT KECIL**  
 Kunci 1 : **M E R D E K A**  
 Kunci 2 : **I N D O N E S I A**  
 Kunci 3 : **P U T I H M E R A H**

Plaintext diatas akan dibagi menjadi 6 blok dengan masing-masing karakter terdiri dari 4 karakter. Karena blok yang keenam tidak mencukupi maka ditambahkan dengan karakter 'X' atau karakter lain yang ditentukan.

PERH	ATIK	ANRA	KYAT	KECI	LXXX
Blok 1	Blok 2	Blok 3	Blok 4	Blok 5	Blok 6

Gambar 5.1 Contoh Plaintext 6 Blok

Kunci 1 (K1) : MERDEKA

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

Kunci 2 (K2) : INDONESIA

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

Kunci 3 (K3) : PUTIH MERAH

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

Gambar 5.2 Contoh Metode Blok Kunci 1,2,3

Maka ciphertext yang dihasilkan :

**OKQCITCGPNPHYMTGEDCDXXX**

OKQC	ITCG	PGNP	HYMT	GEDC	DXXX
K1	K2	K3	K1	K2	K3

Gambar 5.3 Hasil Ciphertext dari Metode Blok

### 5.1.2 Karakter

Metode ini adalah menggunakan pendistribusian per karakter. Perhatikan contoh dibawah ini:

Plaintext : **PERHATIKAN RAKYAT KECIL**  
 K1 : **M E R D E K A**  
 K2 : **I N D O N E S I A**  
 K3 : **P U T I H M E R A H**  
 Metode : **Karakter**

Kunci 1 (K1) : MERDEKA

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

Kunci 2 (K2) : INDONESIA

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

Kunci 3 (K3) : PUTIH MERAH

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

Gambar 5.4 Contoh Kunci(k)1,2,3 Metode Karakter

Maka cara menentukan ciphertextnya sebagai berikut:

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3
O	E	N	C	I	Q	F	G	P	L	Q	P	H	Y	P	T	G	H	R	C	D

Gambar 5.5 Hasil Ciphertext Metode Karakter

Ciphertext : **OENCIQFGPLQPHYPTGHRCD**

### 5.1.3 Zigzag

Metode ini dengan menentukan ciphertext dari plaintext pada kunci 1 (K1) kemudian mencari huruf yang sama hasil dari ciphertext K1 ke chipertext K2 dan mengambil plaintext dari ciphertext K2 untuk selanjutnya mencari huruf yang sama, hasil dari plaintext K2 dengan huruf ciphertext pada K3 dan plaintext pada ciphertext K3 tersebut yang diambil menjadi ciphertext akhir. Perhatikan contoh dibawah ini:

Plaintext : **PERHATIKAN RAKYAT KECIL**

K1 : **MERDEKA**

K2 : **INDONESIA**

K3 : **PUTIH MERAH**

Metode : **Zigzag**

Kunci 1 (K1) : MERDEKA

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

Kunci 2 (K2) : INDONESIA

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

Kunci 3 (K3) : PUTIH MERAH

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

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
L	R	H	D	A	C	O	Q	A	S	H	A	Q	Y	A	C	Q	R	U	O	I

Gambar 5.6 Contoh Kriptografi Metode Zigzag

Ciphertext : **LRHDACQASHAQYACQRUOI**

### 5.1.4 Kode Geser

Ada metode lain selain menggunakan kode geser yang diterapkan kode kaisar mono-alphabet, yaitu dengan menggunakan kode kunci berupa angka bukan banyaknya pergeseran.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 5.7 Contoh Kriptografi Metode Kode Geser

Perhatikan contoh dibawah ini:

Plaintext : **PERHATIKAN RAKYAT KECIL**

Kalimat diatas jika diubah menjadi angka sebagai berikut:

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
15	4	17	7	0	19	8	10	0	13	17	0	10	24	0	19	10	4	2	8	11

Gambar 5.8 Contoh Metode Kode Geser ke Angka

Kode Kunci : **11**

Caranya dengan menambahkan masing-masing angka plaintext dengan kode kunci 11, maka didapatkan:

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
15	4	17	7	0	19	8	10	0	13	17	0	10	24	0	19	10	4	2	8	11
0	15	2	18	11	4	19	21	11	24	2	11	21	9	11	4	21	15	13	19	22
A	P	C	S	L	E	T	V	L	Y	C	L	V	J	L	E	V	P	N	T	W

Gambar 5.9 Hasil kriptografi metode kode geser

Catatan jika ketika dijumlahkan hasilnya lebih dari 26, maka akan dikurangi 26. Misalnya:  $24 + 11 = 35 - 26 = 9$ . Selanjutnya hasil penjumlahan dikonversi menjadi huruf sesuai dengan nilai standar setiap huruf.

Ciphertext : **APCSLETVLYCLVJLEVPNTW**

## 5.2 Teknik Kriptografi Klasik/Kuno III

### 5.2.1 Kode Vigenere

(idokeren 2018) Merupakan kode abjad-majemuk. Teknik dari substitusi vigenere bisa dilakukan dengan 2 cara yaitu angka dan huruf. Teknik ini cukup mudah dipahami dan di aplikasikan. teknik ini di kenalkan oleh seorang kriptologis berkebangsaan perancis Blaise De Vigenere pada abad 16 ( 1586 ), dan teknik ini baru terkenal 200 tahun setelahnya yang kemudian dikenal dengan Code Vigenere.

Kode vigenere yang di gunakan oleh tentara konfederasi ( Confederate Army ) pada perang sipil amerika ( American civil War ). Kode vigenere berhasil di enkripsi oleh Babbage dan Kasiski pada abad 19 pertengahan. <sup>12</sup>

#### 1. Angka

Teknik ini hampir sama dengan kode geser, hanya saja pada vigenere angka caranya dilakukan dengan menukarkan huruf dengan angka dan menggunakan kode kunci berupa kumpulan angka yang sudah ditentukan.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 5.10 Contoh Kode Vigenere (Angka)

Perhatikan contoh dibawah ini:

Plaintext : **PERHATIKAN RAKYAT KECIL**

Kunci : **(2, 8, 7, 15, 4)**

P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
15	4	17	7	0	19	8	10	0	13	17	0	10	24	0	19	10	4	2	8	11
2	8	7	15	4	2	8	7	15	4	2	8	7	15	4	2	8	7	15	4	2
17	12	24	6	4	21	16	17	15	17	19	8	17	13	4	21	18	11	17	12	13
R	M	Y	G	E	V	Q	R	P	R	T	I	R	N	E	V	S	L	R	M	N

Gambar 5.11 Hasil Kriptografi Kode Vigenere (Angka)

## 2. Huruf

Pada teknik huruf menggunakan tabula recta ( bujur sangkar vigenere) dengan pola dibawah ini:

		Plaintext																									
		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
Kode Kunci	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
	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	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	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
	e	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
	f	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
	g	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
	h	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
	i	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
	j	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
	k	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
	l	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
	m	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
	n	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
	o	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
	p	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
	q	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
	r	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
	s	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
	t	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
	u	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
	v	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
	w	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
	x	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
	y	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
	z	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

Gambar 5.12 Contoh Polatabula Recta

Contoh :

Plaintext : **PERHATIKAN RAKYAT KECIL**

Kunci : **I N D O N E S I A**

Maka cara menentukan chipertext-nya adalah:

PLAINTEXT	P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
KUNCI	I	N	D	O	N	E	S	I	A	I	N	D	O	N	E	S	I	A	I	N	D
CIPHERTEXT	X	R	U	V	N	X	A	S	A	V	E	D	Y	L	E	L	S	E	K	V	O

Gambar 5.13 Hasil Kriptografi Kode Vigenere (Huruf)

Ciphertext : **XRUVNXASAVEDYLELSEKVO**

### 5.2.2 Kode Playfair

Ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tahun 1854. Cipher ini mengenkripsi pasangan huruf (digram atau digraf), bukan huruf tunggal seperti pada cipher klasik lainnya. Tujuannya adalah untuk membuat analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf-huruf di dalam cipherteks menjadi datar (flat).

Kunci kriptografinya 25 buah huruf yang disusun di dalam bujursangkat 5x5 dengan menghilangkan huruf J dari abjad.<sup>13</sup>

Dan matriks yang digunakan adalah:

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.14 Tabel Matriks Bujusangkar Kode Playfair

Ada beberapa aturan dalam melakukan enkripsi dengan kode playfair yaitu:

1. Karakter yang ada pada plaintext dibagi menjadi masing-masing 2 karakter.
2. Jika kedua huruf/ karakter tidak terletak pada satu baris atau kolom maka pergerakan karakter dimulai dari huruf kedua secara vertical menuju teks-kode. Contoh: karakter 'di' terdapat pada baris dan kolom yang berbeda maka dimulai dari 'l' tarik secara vertikal menuju baris yang terdapat huruf 'd' sebanyak 2 baris maka akan ditemukan 'n', selanjutnya 'd' ditarik vertical menuju baris yang terdapat 'l' sehingga didapatkan 'L'.

S	T	A	N	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.15 Tabel Matriks Bujusangkar Kode Playfair

3. Jika karakter-karakter yang dienkripsi atau deskripsi berada pada kolom atau baris yang sama dan saling berdekatan maka gunakan prinsip kebawah atau kesamping. Contoh karakter 'an', maka karakter disamping 'n' adalah 'd' dan karakter disamping 'a' adalah 'n' maka ciphertextnya adalah 'dn'.

S	T	A →	N →	D
E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.16 Tabel Matriks Bujusangkar Kode Playfair

4. Jika karakter yang dienkrpsi berada pada akhir baris maka diikuti aturan no 3 diatas, tetapi pada kasus baris terakhir maka karakter yang diambil adalah karakter yang disamping yaitu karakter pertama pada baris selanjutnya.

S	T	A	N	D
← E	R	C	H	B
K	F	G	I	L
M	O	P	Q	U
V	W	X	Y	Z

Gambar 5.17 Tabel Matriks Bujusangkar Kode Playfair

5. Jika terdapat karakter kembar maka cukup ditambahkan karakter yang disepakati misalnya karakter 'aa' disepakati untuk disisipkan dengan karakter 'z' maka chipertext 'aza'.
6. Untuk kepentingan analisis kode playfair maka aturan no 2 disebut ERDL (Encipher Right Decipher Left), aturan no 3 dan 4 disebut EBDA (Encipher Below Decipher Above).

Contoh: Belajarlah Cepat

Plaintext	be	la	Ja	ri	ah	ce	pa	tx
Ciphertext	rk	gd	gn	bf	nc	rh	cx	aw

Gambar 5.18 Tabel Matriks Bujusangkar Kode Playfair

Karena pada akhir tidak terdapat 2 karakter maka untuk melengkapi di tambahkan karakter yang disepakati.