TEKNIK CRYPTOGRAPHY (KRIPTOGRAFI) BAGIAN 2

PERTEMUAN 5

METODE DENGAN LEBIH DARI SATU KUNCI

- Blok
- Karakter
- Zig-zag

BLOK

- Membagi jumlah teks-asli menjadi blok-blok yang ditentukan, tergantung dari keinginan pengirim pesan.
- Contoh plaintext: PERHATIKAN RAKYAT KECIL
  - Kunci 1: MERDEKA
  - Kunci 2: INDONESIA
  - Kunci 3: PUTIH MERAH

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.

JAWAB

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

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

Maka Ciphertext yang dihasilkan:

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

'OKQCITCGPGNPHYMTGEDCDXXX' adalah ciphertext dari plaintext **PERHATIKAN RAKYAT KECIL**

KARAKTER

- Metode ini adalah menggunakan pendistribusian perkarakter.
- Perhatikan contoh dibawah ini:
  - Plaintext : PERHATIKAN RAKYAT KECIL
  - K1 : MERDEKA
  - K2 : INDONESIA
  - K3 : PUTIH MERAH
  - Metode : Karakter

JAWAB

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

Maka cara menentukan ciphertextnya sebagai berikut:

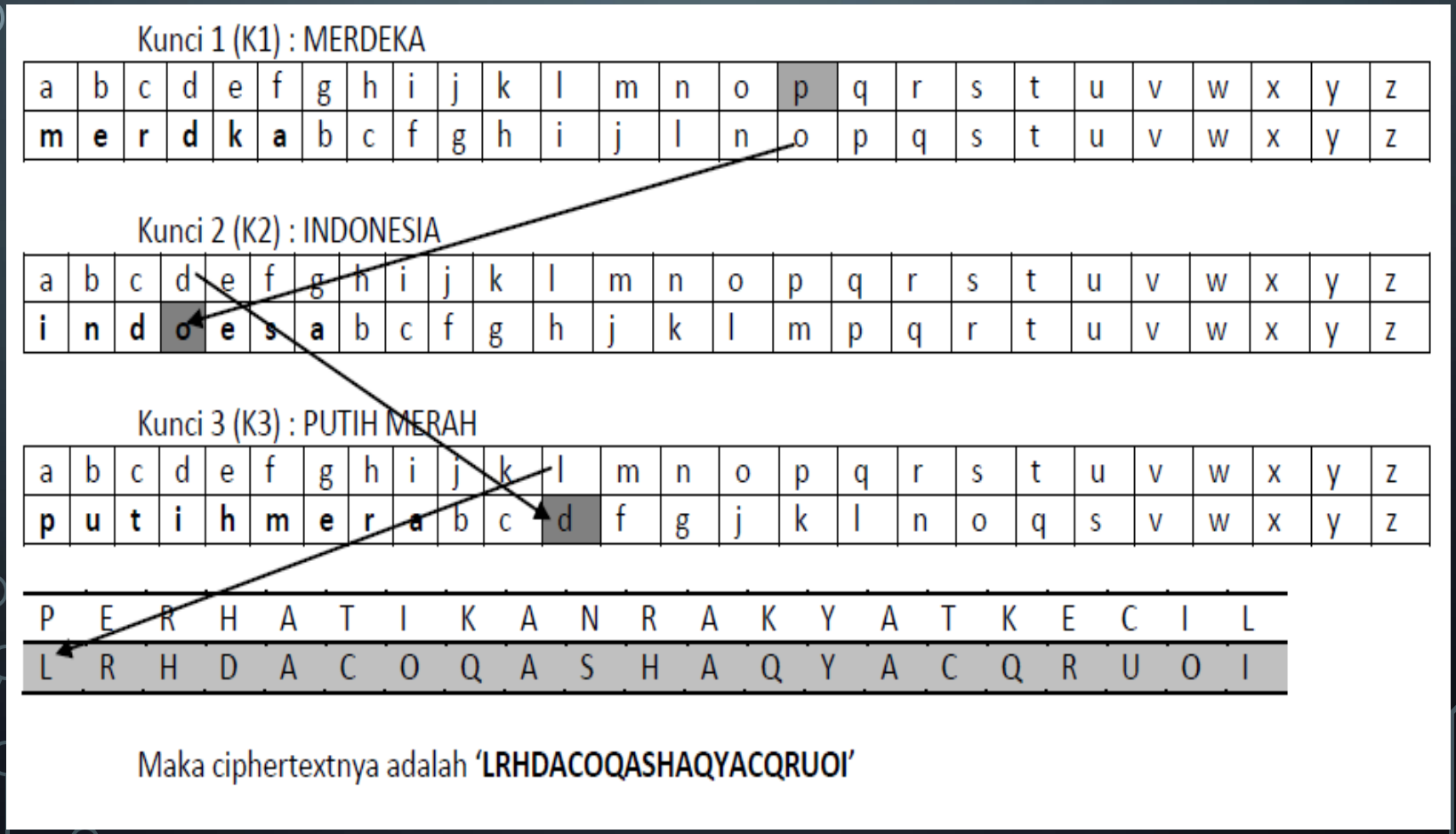
P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L
K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3
O	E	N	C	I	Q	F	G	P	L	Q	P	H	Y	P	T	G	H	R	C	D

Dengan metode karakter maka **'OENCIQFGPLQPHYPTGHRCD'** adalah chipertect dari plaintext **PERHATIKAN RAKYAT KECIL**.

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

JAWAB



Maka ciphertextnya adalah '**LRHDACOQASHAQYACQRUOI**'

POLYALPHABETIC SUBSTITUTION CIPHER

- Merupakan sandi substitusi-ganda (multiplesubstitution cipher) yang melibatkan penggunaan kunci berbeda
- Sandi abjad-majemuk dibuat dari sejumlah sandi abjad-tunggal, masing-masing dengan kunci yang berbeda
- Kebanyakan sandi abjad-majemuk adalah sandi substitusi periodik
- Contoh sandi substitusi periodik adalah vigenère cipher

KARAKTERISTIK TEKNIK POLYALPHABETIC

- Sekumpulan aturan substitusi monoalphabetic yang terkait digunakan
- Sebuah kunci menentukan bagian aturan mana yang dipilih untuk transformasi

VIGENÈRE CIPHER (1)

- Pertama kali dipopulerkan oleh Blaise de Vigenère, seorang kriptografer asal Prancis
- Sandi Vigenère adalah salah satu metode enkripsi yang menggunakan sejumlah sandi Caesar berbeda, berdasarkan huruf-huruf dari sebuah kata kunci
- Cipher ini merupakan bentuk sederhana dari substitusi polyalphabet

VIGENÈRE CIPHER (2)

- Angka

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

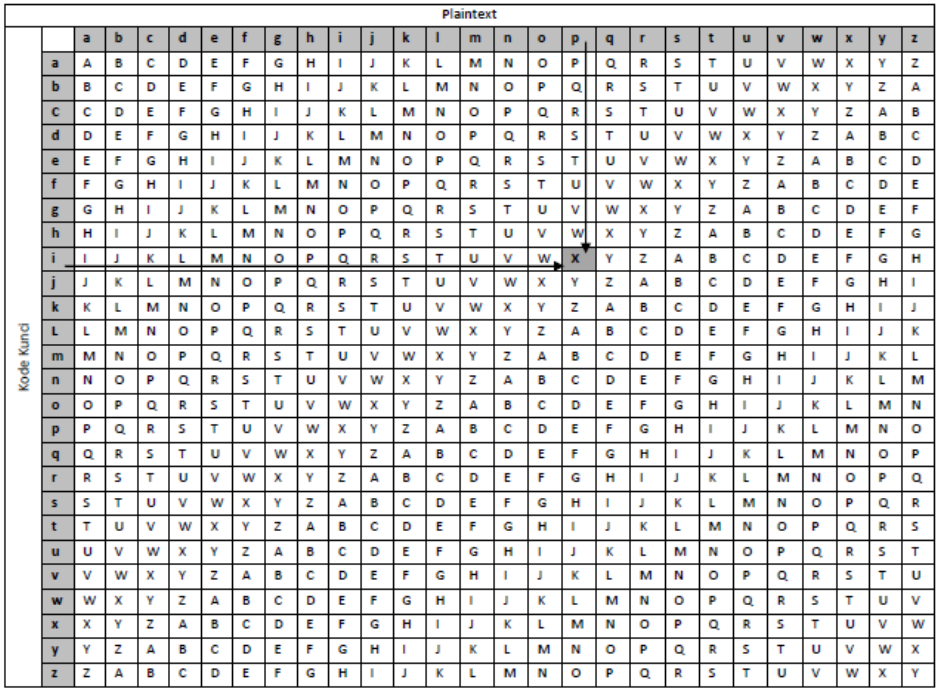
Perhatikan contoh dibawah ini:
Plaintext : PERHATIKAN RAKYAT KECIL
Kunci : (2, 8, 7, 15, 4)

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**

Ciphertext : 'RMYGEVQRPRTIRNEVSLRMN'

VIGENÈRE CIPHER (3)

- Huruf



Kode Kunci \ 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
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

VIGENÈRE CIPHER (4)

CONTOH HURUF

Contoh:

Plaintext : PERHATIKAN RAKYAT KECIL

Kunci : INODNESIA

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

VIGENÈRE CIPHER (DENGAN RUMUS)

P E R H A T I K A N R A K Y A T K E C I L

I ND ON E S I A I N D O N E S I A I ND

15	4	17	7	0	19	8	10	0	13
+8	+13	+3	+14	+13	+4	+18	+8	+0	+8
23	17	20	21	13	23	26	18	0	21
						-26			
						0			
X	R	U	V	N	X	A	S	A	V

VIGENÈRE CIPHER (DENGAN RUMUS)

17	0	10	24	0	19
+13	+3	+14	+13	+4	+18
30	3	24	37	4	37
-26			-26		-26
4			11		11
E	D	Y	L	E	L

VIGENÈRE CIPHER (DENGAN RUMUS)

10	4	2	8	11
+8	+0	+8	+13	+3
18	4	10	21	14
S	E	K	V	O

Ciphertext = XRUVNXASAV EDYLEL SEKVO

Bagaimana jika sebaliknya dengan melakukan dekripsi pada ciphertext XRUVNXASAV EDYLEL SEKVO?