KRIPTOGRAFI KLASIK

1. Vigenere Chiper

- Teknik substitusi dengan:
  - Angka
  - Huruf

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Angka
  - Teknik ini menggunakan angka dengan menukarkan huruf dengan angka
  - Contoh: Kunci = CIPHER → K = (2,8,15,7,4,17)

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

  - Plaintext = “This cryptosystem is not secure”

- K = (2,8,15,7,4,17)
- Plaintext = THIS CRYPTOSYSTEM IS NOT SECURE

T	H	I	S	C	R	Y	P	T	O	S	Y	S	T
19	7	8	18	2	17	24	15	19	14	18	24	18	19
2	8	15	7	4	17	2	8	15	7	4	17	2	8

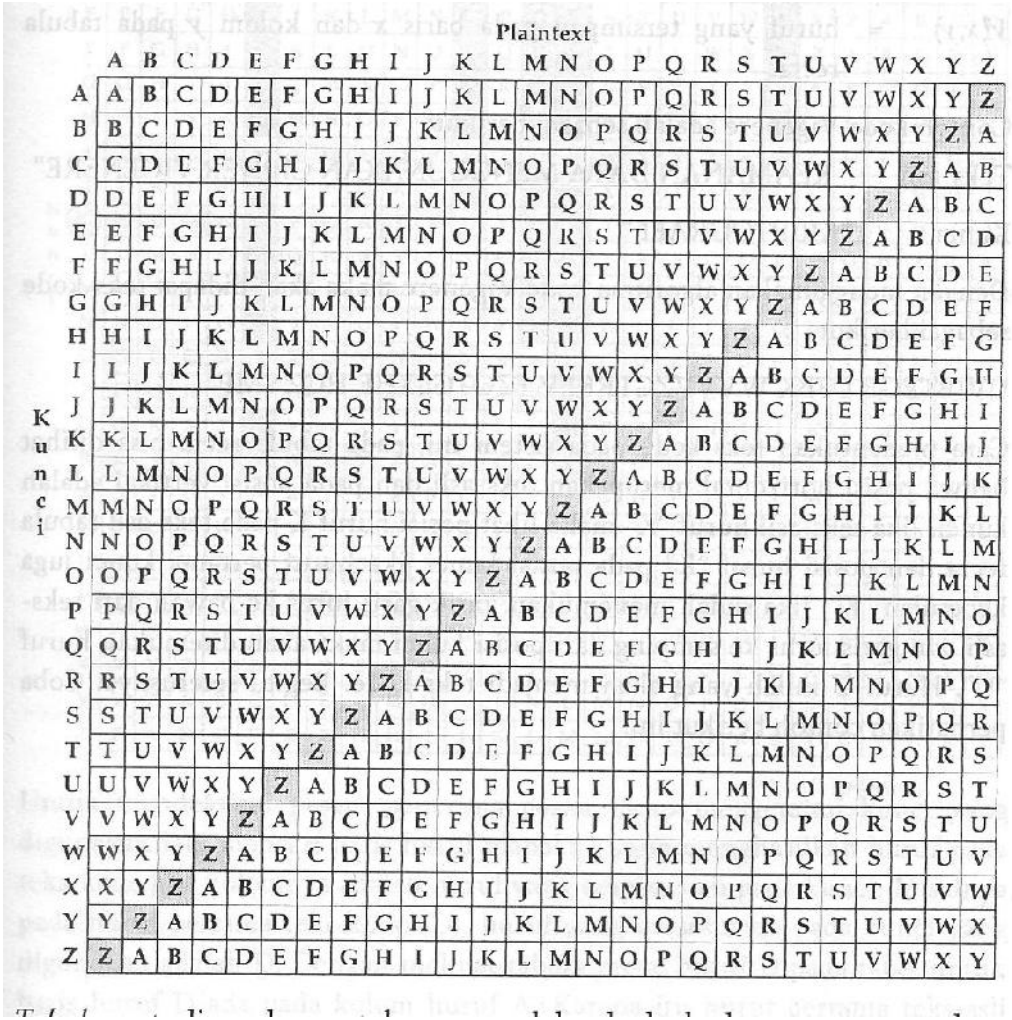
21 15 23 25 6 8 0 23 8 21 22 15 20 1

E	M	I	S	N	O	T	S	E	C	U	R	E
4	12	8	18	13	14	19	18	4	2	20	17	4
15	7	4	17	2	8	15	7	4	17	2	8	15

19 19 12 9 15 22 8 25 8 19 22 25 19

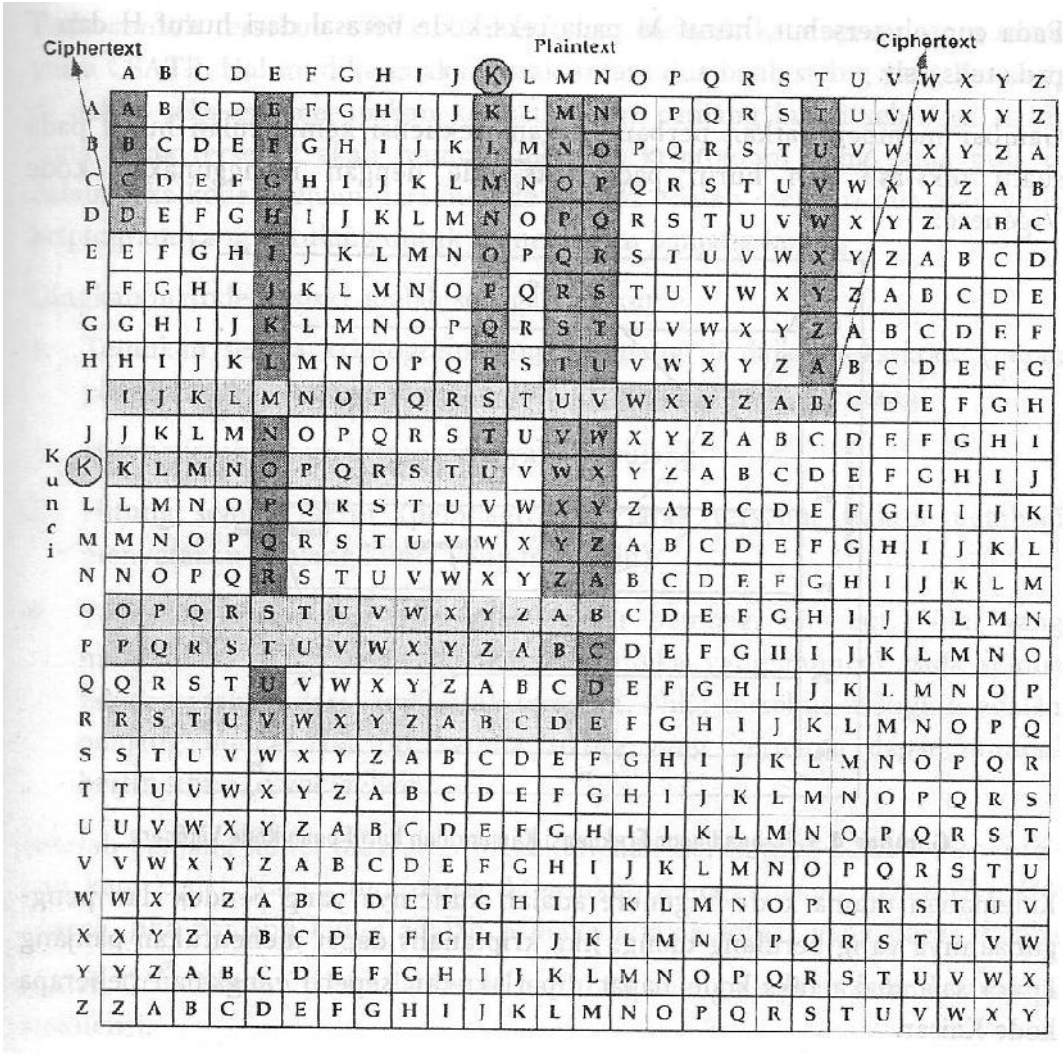
- Chipertext = VPXZGIAIVWPUBTTMJPWIZITWZT

- Huruf
  - Teknik ini menggunakan huruf berdasarkan tabel berikut



Plaintext

Kunci	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



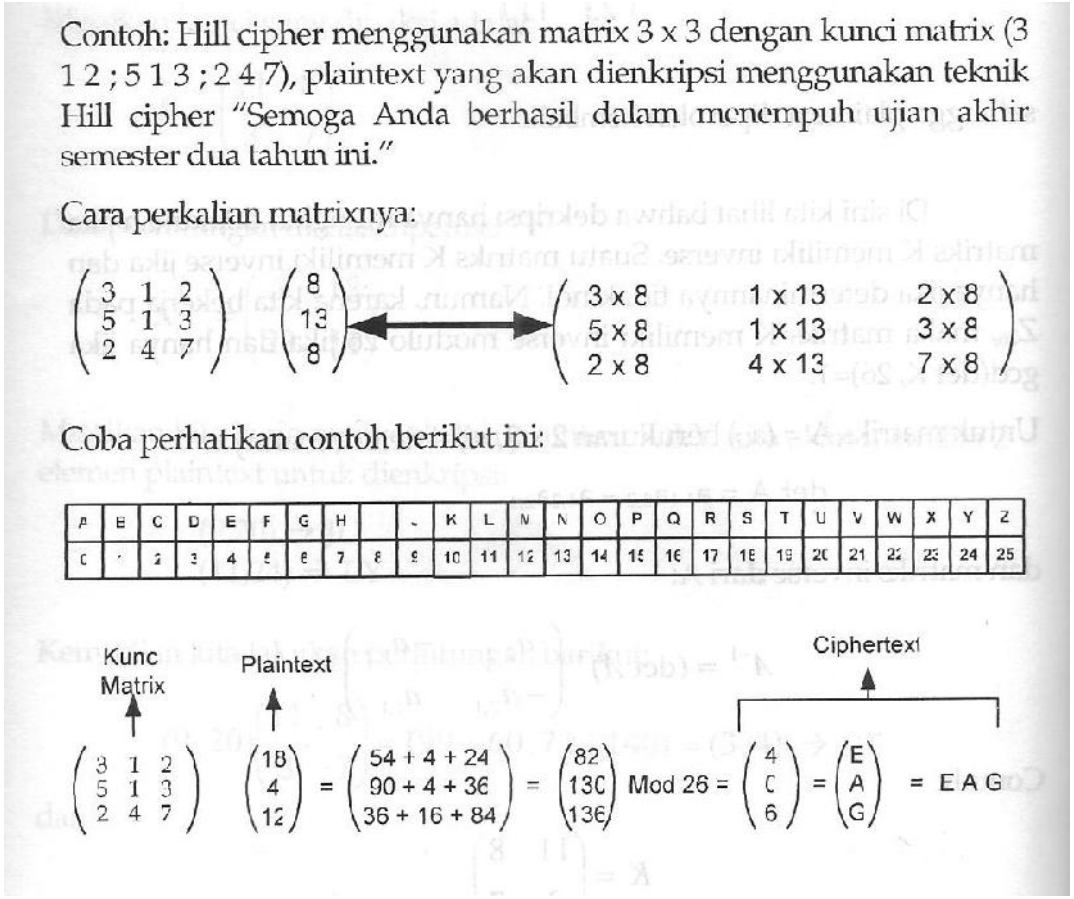
Plain = KEAMANAN DATA MENGGUNAKAN CIPHER VIGENERE

Key = KRIPTOGRAFI

Chiper = UVIBTBGEDFBKWVVVZCTRKFV.....

2. Hill Chiper

- Teknik ini menggunakan matrix:



Contoh: Hill cipher menggunakan matrix 3 x 3 dengan kunci matrix (3 1 2 ; 5 1 3 ; 2 4 7), plaintext yang akan dienkripsi menggunakan teknik Hill cipher "Semoga Anda berhasil dalam menempuh ujian akhir semester dua tahun ini."

Cara perkalian matrixnya:

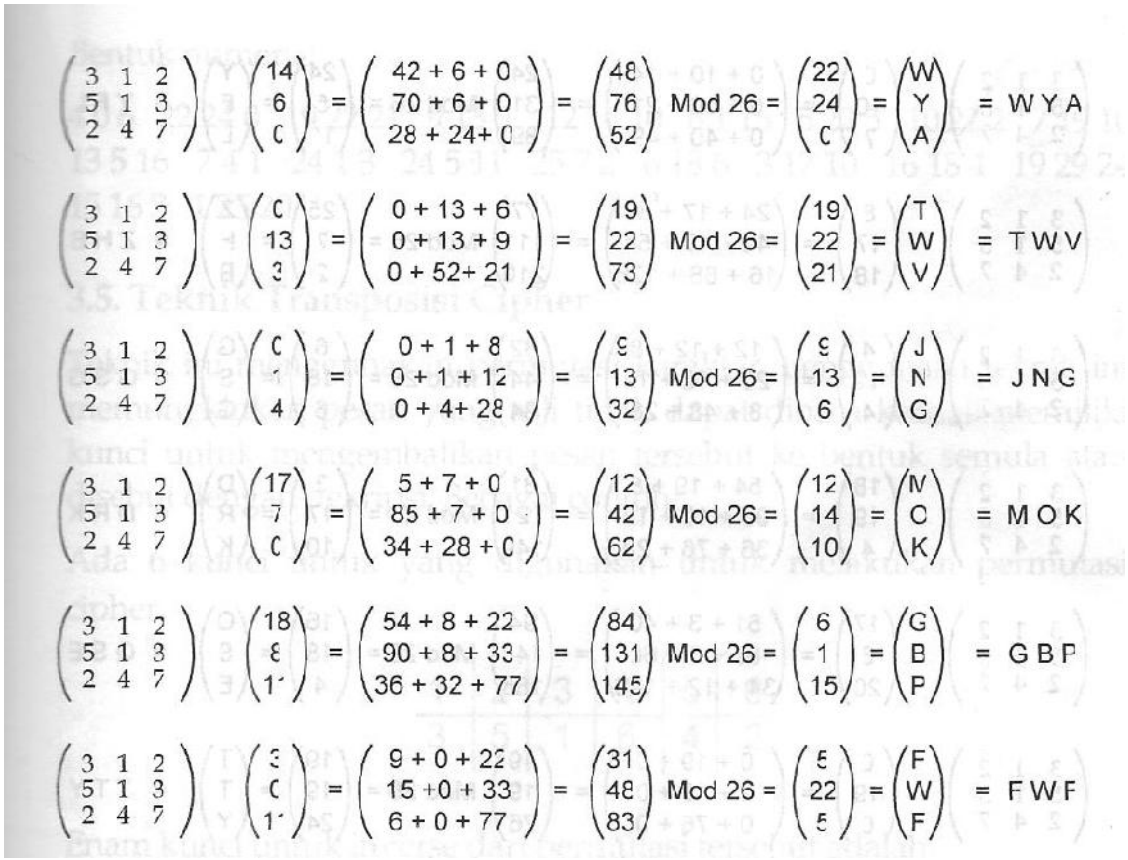
$$\begin{pmatrix} 3 & 1 & 2 \\ 5 & 1 & 3 \\ 2 & 4 & 7 \end{pmatrix} \begin{pmatrix} 8 \\ 13 \\ 8 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 3 \times 8 & 1 \times 13 & 2 \times 8 \\ 5 \times 8 & 1 \times 13 & 3 \times 8 \\ 2 \times 8 & 4 \times 13 & 7 \times 8 \end{pmatrix}$$

Coba perhatikan contoh berikut ini:

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

Kunc Matrix — Plaintext — Ciphertext

$$\begin{pmatrix} 3 & 1 & 2 \\ 5 & 1 & 3 \\ 2 & 4 & 7 \end{pmatrix} \begin{pmatrix} 18 \\ 4 \\ 12 \end{pmatrix} = \begin{pmatrix} 54 + 4 + 24 \\ 90 + 4 + 36 \\ 36 + 16 + 84 \end{pmatrix} = \begin{pmatrix} 82 \\ 130 \\ 136 \end{pmatrix} \text{ Mod } 26 = \begin{pmatrix} 4 \\ 0 \\ 6 \end{pmatrix} = \begin{pmatrix} E \\ A \\ G \end{pmatrix} = \text{E A G}$$



...dst

- Plain = Semoga anda berhasil dalam menempuh ujian akhir semester dua tahun ini
- Kunci matrix = 3 x 3
- Chiper = EAG WAY TWU JNG MOK GBP FWF ...

3. Transposisi Chiper

- Teknik ini menggunakan permutasi karakter
- Mis:

Ada 6 kunci untuk yang digunakan untuk melakukan permutasi cipher.

1	2	3	4	5	6
3	5	1	6	4	2

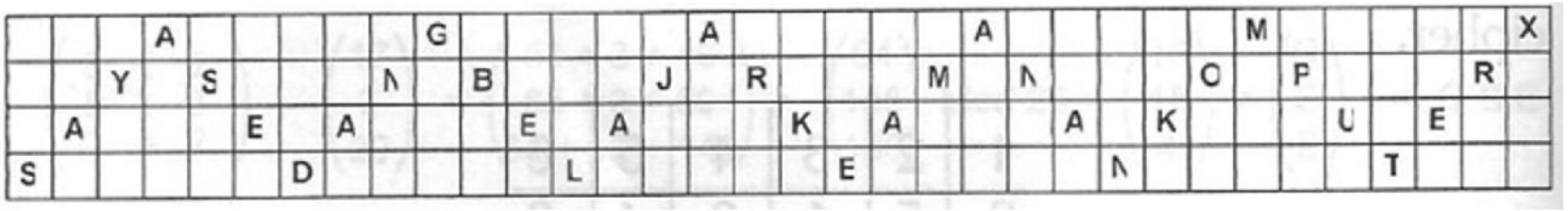
Enam kunci untuk inverse dari permutasi tersebut adalah

1	2	3	4	5	6
3	6	1	5	2	4

- PLAIN : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER
  - Sebelumnya dibagi menjadi 6 block sesuai bentuk diatas, jika terjadi kekurangan dari block bisa ditambah dengan huruf yang disukai mis: X
- PLAIN BLOCK: SAYASE DANGBE LAJARK EMANA NKOMPU TERXXX
- CHIPER : YSEEAA NBDEGA JRLKAA MNEAAA OPNUMK RXTXXE

Teknik lain dari Transposisi Chiper

- Zig zag : memasukkan plaintext dengan pola zigzag



- CHIPER = AGAAMXYSNBJRMNOPRAEAEAKAAKUESDLENT

Teknik lain dari Transposisi Chiper

- Segitiga : memasukkan plaintext dengan pola segitiga

					S					
				A	Y	A				
			B	E	L	A	J			
		R	K	E	A	M	A	N		
	A	N	K	O	M	P	U	T	E	
R	X	X	X	X	X	X	X	X	X	X

- CHIPER = RAXRNXBKKXAEEOXSYLAMXAAMPXJAUXNTXEXX

Teknik lain dari Transposisi Chiper

- Spiral : memasukkan plaintext dengan pola spiral serta dapat dibaca dari atas ke bawah

S	A	Y	A	S	E
A	M	A	N	A	D
E	E	R	X	N	A
K	T	X	X	K	N
R	U	P	M	O	G
A	J	A	L	E	B

- CHIPER = SAEKRAAMETUJYARXPAANXXMLSANKOEEDANGB

Teknik lain dari Transposisi Chiper

- Diagonal : memasukkan plaintext dengan cara diagonal

S	D	L	E	N	E
A	A	A	A	K	R
Y	N	J	M	O	X
A	G	A	A	M	X
S	B	R	N	P	X
E	E	K	A	U	X

- CHIPER = SDLENEAAAAKRYNJMOXAGAAMXSBRNPXEEKAUX