MODUL KRIPTOGRAFI

(CTI 312)

MODUL 3

KRIPTOGRAFI KLASIK

DISUSUN OLEH

IR. NIZIRWAN ANWAR, M.T

UNIVERSITAS ESA UNGGUL

2020

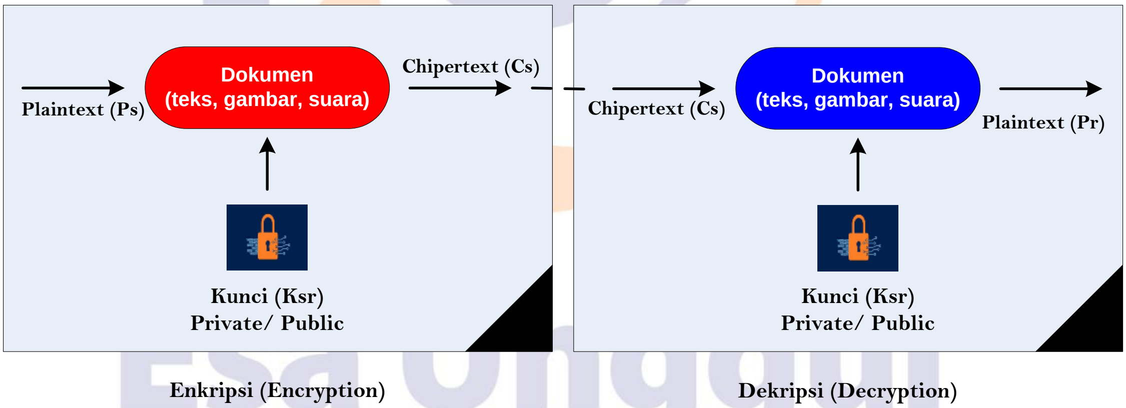
MODUL 3
TEKNIK KRIPTOGRAFI KLASIK (CHIPER)

1. KONSEP KLASIK

Kriptografi adalah suatu ilmu untuk menyamarkan suatu pesan sehingga pesan tersebut tidak dapat dibaca dan di-akses oleh pihak ketiga, dan yang dapat membaca pesan tersebut hanya 2 pihak yaitu pihak pengirim dan pihak penerima. Dalam kriptografi terdapat 2 (dua) istilah yaitu :

1) Enkripsi adalah proses menyamarkan pesan asli (plaintext) dengan algoritma kriptografi, dengan luaran enkripsi dinamakan ciphertext.

2) Dekripsi adalah proses pengembalian pesan yang telah di-enkripsi (ciphertext) menjadi pesan asli (plaintext).



Gambar 3.1 Konsep Umum dan Proses Kriptografi

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum teknologi informasi (data) komputer dikembangkan atau sudah ditemukan namun belum secanggih ilmu pengetahuan dan teknologi sekarang.Kriptografi ini melakukan pengacakan huruf pada kata terang / plaintext. Kriptografi secara operasional hanya melakukan pengacakan (random) pada huruf A – Z (26 abjad/karakter).

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	26
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

atau

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
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

Gambar 3.1 Karakter Alfabet

Meskipiun telah ditinggalkan dan berubah secara evolusi sesuai perkembangan zaman, kriptografi klasik tetap menjadi topik bahasan awal dalam mempelajari dan mengkaji bidang ilmu kriptografi sebagai pengantar kriptografi modern. Mengapa kita diharuskan membahas kriptografi klasik sebagai step-by-step mengkaji kriptografi modern …. Solusinya … "memahami konsep dasar kritografi, algoritma kriptografi modern dan dalam memahmi kelemahan system kode"

Kriptogarfi klasik memiliki beberapa karakteristik antara lain ;

1) Berbasis karakter

2) Menggunakan pena dan kertas saja, belum ada computer

3) Termasuk ke dalam kriptografi kunci simetris.

Teks sandi yang dihasilkan dengan sandi klasik mengungkapkan informasi statistik tentang teks awal, yang sering dapat digunakan untuk memecahkannya. Setelah ditemukannya analisis frekuensi oleh matematikawan Arab dan polymath Al-Kindi (juga dikenal sebagai Al Kindus) pada abad ke-9, hampir semua jenis sandi menjadi lebih sulit dipecahkan oleh penyerang yang memiliki informasi tersebut. Seperti sandi klasik yang masih populer hingga saat ini, meskipun lebih banyak dalam bentuk puzzle. Al-Kindi menuliskan buku kriptografi yang berjudul *Risalah fi Istikhraj al-Mu'amma* (Risalah untuk Mnejermahkan Pesan Kriptografi), yang menjelaskan teknik analisis frekuensi kriptanalisis yang pertama kalinya.

Gambar 3.2 Lembaran pertama dari buku Al-Kindi dalam meng-enkripsi-kan pesan

Dan algoritma ini diklasifikasikan ke dalam 2 (dua) tipe chiper,

1. **Cipher Substitusi (Substitution Cipher)**

   Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu “unit” di isini berarti satu huruf, pasanga huruf, atau dikelompokkan lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah Caesar cipher yang digunakan oleh kaisar Romawi , Julius Caesar (sehingga dinamakan juga casear cipher), untuk mengirimakan pesan yang dikirimkan kepada gubernurnya.

2. **Cipher Transposisi (Transposition Cipher)**

   Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (scrambling) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karkater tersebut.

Contoh Kriptografi Klasik

Gambar 3.2 Caesar Wheel

Gambar 3.3 Scytale

3. KRIPTOGRAFI KLASIK

Kriptografi klasik mempunyai 3 (tiga) model yaitu;

1) Caesar Cipher,

2) Vigenere Cipher,

3) dan Hill Cipher,

3.1 Caesar Ciper

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada plaintext digantikan atau ditransformasikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet.

Proses Enkripsi

$$\text{Ciphertext} = (\text{ plaintext} + \text{kunci }) \% 26 \qquad [1]$$

Contoh 1, Plaintext **ILMU** dengan **Kunci = 17**

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	26
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

Table 3.1 Proses Enkripsi dengan Kunci 17

Plaintext	9	12	13	21
Kunci	17	17	17	17
(plaintext + kunci/key) % 26	26	3	4	11
Ciphertext	**Z**	**C**	**D**	**K**

Proses Dekripsi

$$\text{Plaintext} = (\text{ Ciphertext} - \text{kunci }) \% 26 \qquad [2]$$

Contoh 2, Ciphertext **ZCGK** dengan **Kunci = 17**

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	26
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

Table 3.2 Proses Dekripsi dengan Kunci 17

Ciphertext	26	3	4	11
Kunci	17	17	17	17
(Plaintext - Kunci) % 26	9	12	13	21
Plaintext	**I**	**L**	**M**	**U**

Contoh 3, Plaintext **ENKRIPSI** dengan **Kunci = 11**

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	26

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

Dengan menggunakan persamaan enkripsi [1], diperoleh langkah-langkah berikut ini ;

Table 3.3 Proses Enkripsi dengan Kunci 11

Plaintext	5	14	11	18	9	16	19	9
Kunci	11	11	11	11	11	11	11	11
(plaintext + kunci/key) % 26	16	25	22	3	6	1	4	6
Ciphertext	**P**	**Y**	**V**	**C**	**F**	**A**	**D**	**F**

Dengan menggunakan persamaan dekripsi [2], diperoleh langkah-langkah berikut ini ;

Table 3.4 Proses Dekripsi dengan Kunci 11

Ciphertext	16	25	22	3	6	1	4	6
Kunci	11	11	11	11	11	11	11	11
(Plaintext - Kunci) % 26	5	14	11	18	9	16	19	9
Plaintext	**E**	**N**	**K**	**R**	**I**	**P**	**S**	**I**

3.2 Vigenere Cipher

Sandi Vigenère adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi Vigenère merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Giovan Batista Belaso menjelaskan metode ini dalam buku La cifra del. Sig. Giovan Batista Belaso (1553); dan disempurnakan oleh diplomat Prancis Blaise de Vigenère, pada 1586. Pada abat ke-19, banyak orang yang mengira Vigenère adalah penemu sandi ini, sehingga, sandi ini dikenal luas sebagai "sandi Vigenère".

Table 3.5 Vigenere Cipher Matriks

		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
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

Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenère (table 3.5) berbentuk bujur sangkar.

Tabel Vigenère berisi alfabet yang dituliskan dalam 26 baris dan 26 kolom, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 probabilitas sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang berulang (secara periodik).

Penyandian (enkripsi) dengan sandi Vigenère juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$$C_i \equiv (P_i + K_i) \bmod 26 \qquad [3]$$

atau C = P + K bila dijumlahkan dibawah +26 dan - 26 kalau hasil jumlah di atas 26.

Dan untuk mengembalikan pesan sebelum di-enkripsi maka kita perlu melakukan tahapan dekripsi

$$P_i \equiv (C_i - K_i) \bmod 26 \qquad [4]$$

atau P = C - K bila hasilnya positif dan +26 kalau pengurangan minus.

Contoh 1;

Jika plaintext adalah FASILKOM dan kunci adalah ANWAR maka penggunaan kunci secara periodik (rujukan gambar 3.5) sebagai berikut:

Plaintext	:	FASILKOM
Kunci	:	ANWAR
Ciphertext	:	FNOICKBI

.

Table 3.6 Vigenere Cipher Contoh 1

FASILKOM	>>>	F	A	S	I	L	K	O	M	>>>	Plaintext
ANWAR	>>>	A	N	W	A	R	A	N	W	>>>	Kunci
FNOICKBI	>>>	F	N	O	I	C	K	B	I	>>>	Ciphertext

Contoh 2;

Jika plaintext adalah INFORMATIKA dan kunci adalah TEKNIK maka penggunaan kunci secara periodik (rujukan gambar 3.5) sebagai berikut:

Plaintext : INFORMATIKA
Kunci : TEKNIK
Ciphertext : BRPBZWTXSXI

Table 3.7 Vigenere Cipher Contoh 2

INFORMATIKA	>>>	I	N	F	O	R	M	A	T	I	K	A	>>>	Plaintext
TEKNIK	>>>	T	E	K	N	I	K	T	E	K	N	I	>>>	Kunci
BRPBZWTXSXI	>>>	B	R	P	B	Z	W	T	X	S	X	I	>>>	Ciphertext

Contoh 3;

Jika plaintext adalah INFORMASI dan kunci adalah SISTEM maka penggunaan kunci secara periodik (rujukan gambar 3.5) sebagai berikut:

Plaintext : INFORMASI
Kunci : SISTEM
Ciphertext : AVXHVYSAA

Table 3.8 Vigenere Cipher Contoh 3

INFORMASI	>>>	I	N	F	O	R	M	A	S	I	>>>	Plainte
SISTEM	>>>	S	I	S	T	E	M	S	I	S	>>>	Kunci
AVXHVYSAA	>>>	A	V	X	H	V	Y	S	A	A	>>>	Cipher

Jenis variasi vigènere cipher pada dasarnya perbedaannya terletak pada cara atau pendekatan membentuk tabel atau metode dalam memperoleh kuncinya, sedangkan proses enkripsi dan dekripsi tidak ada perubahan dengan vigènere cipher standar. Beberapa variasi tersebut sebagai berikut:

1) Full Vigènere Cipher (FVC)

Pada varian ini, setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi merupakan permutasi huruf-huruf alphabet.

Contoh

Table 3.9 Vigenere Cipher - FVC

a	A	W	M	X	H	V	D	Y	Q	T	X	S	I	R	F	N	O	C	K	B

2) Auto-Key Vigènere Cipher (AKVC)

Idealnya kunci tidak digunakan secara berulang. Pada auto-key vigènere cipher, jika panjang kunci lebih kecil dari panjang plaintext, maka kunci disambung dengan plaintext tersebut.

Contoh

Plaintext : UNIVERSITAS ESA UNGGUL

Kunci : FASILKOM

Ciphertext : ???

Table 3.10 Vigenere Cipher - AKVC

Plaintext	>>>	U	N	I	V	E	R	S	I	T	A	S	E	S	A	U	N	G	G	U	L
Kunci	>>>	F	A	S	I	L	K	O	M	U	N	I	V	E	R	S	I	T	A	S	E
Ciphertext	>>>	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?

3) Running-Key Vigènere Cipher (RKVC)

Pada varian ini, kunci bukan string pendek yang diulang secara periodik seperti pada vigènere cipher standar, tetapi kunci adalah string yang sangat panjang yang diambil dari teks bermakna

Contoh

Plaintext : INDONESIA NEGARA BERDAULAT

Kunci : PERSATUAN INDONESIA

Ciphertext : ???

Table 3.11 Vigenere Cipher - RKVC

Plaintext >>>	I	N	D	O	N	E	S	I	A	N	E	G	A	R	A	B	E	R	D	A	U	L	A	T
Kunci >>>	P	E	R	S	A	T	U	A	N	I	N	D	O	N	E	S	I	A	P	E	R	S	A	T
Ciphertext >>>	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?

3.3 Hill Cipher

Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929 [2]. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya**.**

Hill Cipher yang merupakan polyalphabetic cipher yang dikategorikan sebagai block cipher [2] karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula. Hill Cipher termasuk algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila kriptanalisis-nya hanya dengan mengetahui berkas ciphertext saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila seorang kriptanalis memiliki berkas ciphertext dan potongan berkas plaintext. Teknik kriptanalisis ini disebut known-plaintext attack [1]. Algoritmanya yaitu Hill Cipher mengenkripsi plaintext sepanjang m menjadi ciphertext dengan panjang yang sama (m). Substitusinya ditentukan oleh persamaan linier m dimana masing-masing karakter diganti dengan nilai nominal (a=0, b=1, ..., z=25).

	HURUF BESAR																									
ASCII	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
Desimal	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
	HURUF KECIL																									
ASCII	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
Desimal	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122

Untuk m = 3, sistemnya seperti berikut :

$$c1 = (k11p1 + k21p2 + k31p3) \bmod 26$$
$$c2 = (k12p1 + k22p2 + k32p3) \bmod 26$$
$$c3 = (k13p1 + k23p2 + k33p3) \bmod 26$$

[5]

Jika digambarkan persamaan [5] dalam vektor baris dan matriks adalah sebagai berikut;

$$\mathbf{(C1\ C2\ C3)} = \mathbf{(P1\ P2\ P3)} \begin{vmatrix} \mathbf{K11} & \mathbf{K12} & \mathbf{K13} \\ \mathbf{K21} & \mathbf{K22} & \mathbf{K23} \\ \mathbf{K31} & \mathbf{K32} & \mathbf{K33} \end{vmatrix} \ \mathbf{MOD\ 26}$$

[6]

dimana C dan P adalah vektor baris dengan panjang 3 dan K adalah kunci enkripsi berupa matriks berukuran 3 x 3. Operasi dilakukan dengan modulo 26.

Rumus enkripsi dengan prinsip blok

C = E (K, P) = K * P mod 26 [7]

Untuk mengembalikan-nya, proses dekripsi dengan menggunakan rumus di bawah ini

P = D (K^{-1}, C) = K^{-1} * C mod 26 [8]

Dimana

- **P = Plaintext**
- **C = Chipertext**
- **K = Kunci matriks**
- **K -1 = Invers Kunci Matriks**
- **D = Dekripsi**

Tabel 3.12 Mencari Invers Mod 26

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Contoh 1; untuk memperjelas Hill Chiper, saya sajikan contoh, asumsikan meng enkripsi sebuah plain text (FASILKOM) dan matriks kunci K = $\begin{bmatrix} 4 & 8 \\ 1 & 3 \end{bmatrix}$

Proses Enkripsi

Langkah 1;

Plaintext FASILKOM dibuatkan blok dari plaintext tersebut

FA = 6, 1 atau ditulis $\begin{bmatrix} \mathrm{F} \\ \mathrm{A} \end{bmatrix}$ = $\begin{bmatrix} 5 \\ 0 \end{bmatrix}$

SI = 19, 9 atau ditulis $\begin{bmatrix} \mathrm{S} \\ \mathrm{I} \end{bmatrix}$ = $\begin{bmatrix} 18 \\ 8 \end{bmatrix}$

LK = 12, 11 atau ditulis $\begin{bmatrix} L \\ \mathrm{K} \end{bmatrix}$ = $\begin{bmatrix} 11 \\ 10 \end{bmatrix}$

$$OM = 15, 13 \text{ atau ditulis } \begin{bmatrix} O \\ M \end{bmatrix} = \begin{bmatrix} 14 \\ 12 \end{bmatrix}$$

Langkah 2;

Lakukan proses perkalian K dengan hasil dari langkah 1,

$$\begin{bmatrix} 4 & 8 \\ 1 & 3 \end{bmatrix} * \begin{bmatrix} 5 \\ 0 \end{bmatrix} = \begin{bmatrix} 20 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 8 \\ 1 & 3 \end{bmatrix} * \begin{bmatrix} 18 \\ 8 \end{bmatrix} = \begin{bmatrix} 136 \\ 42 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 8 \\ 1 & 3 \end{bmatrix} * \begin{bmatrix} 11 \\ 10 \end{bmatrix} = \begin{bmatrix} 124 \\ 41 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 8 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 14 \\ 12 \end{bmatrix} = \begin{bmatrix} 152 \\ 50 \end{bmatrix}$$

Langkah 3; Proses Enkripsi

$$C\ (FA) = \begin{bmatrix} 20 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 5 \end{bmatrix}$$

$$C\ (SI) = \begin{bmatrix} 136 \\ 42 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 \\ 16 \end{bmatrix}$$

$$C\ (LK) = \begin{bmatrix} 124 \\ 41 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 15 \end{bmatrix}$$

$$C\ (OM) = \begin{bmatrix} 152 \\ 50 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 \\ 24 \end{bmatrix}$$

Sehingga menghasilkan ciphertext

20, 5, 6, 16, 20, 15, 22, 24 = TEFPTOVX

Proses Dekripsi

Langkah 1;

mencari invers matriks kunci menggunakan invers kunci matriks dengan menetukan determinan

$$K = \begin{bmatrix} 4 & 8 \\ 1 & 3 \end{bmatrix} \rightarrow \det K = (4)(3) - (8)(1) = 4$$

Langkah 2

Tabel 3.13 Mencari Invers Mod 26

x	1	3	5	7	9	11	15	17	19	21	23	25
x^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

x = det (K) mod 26 , dimana det(K) = 4

maka

x = 4 mod 26 = 4

Jika nilai det (K) mod 26 tidak terdapat pada tabel 3.12 , maka dapat dipastikan bahwa permasalahan mencari dekripsi pada plaintext **FASILKOM** dan Kunci yang ditentukan tidak akan terpecahkan (asumsi pada kesalahan pada matriks kunci).

Contoh 2; untuk memperjelas Hill Chiper, saya sajikan dengan, asumsikan meng-enkripsi plaintext (FASILKOM) dan matriks kunci $K = \begin{bmatrix} 4 & 8 \\ 1 & 7 \end{bmatrix}$.

HURUF BESAR

ASCII	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
Desimal	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90

HURUF KECIL

ASCII	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
Desimal	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122

	F	A	S	I	L	K	O	M
ALFABET	5	0	18	8	11	10	14	12
ASCII	70	65	83	73	76	75	79	77

Proses Enkripsi

Langkah 1;

Plaintext FASILKOM dibuatkan blok dari plaintext tersebut

FA = 5, 0 atau ditulis $\begin{bmatrix} F \\ A \end{bmatrix} = \begin{bmatrix} 5 \\ 0 \end{bmatrix}$

$$SI = 18,\ 8 \text{ atau ditulis } \begin{bmatrix} S \\ I \end{bmatrix} = \begin{bmatrix} 18 \\ 8 \end{bmatrix}$$

$$LK = 11,\ 10 \text{ atau ditulis } \begin{bmatrix} L \\ K \end{bmatrix} = \begin{bmatrix} 11 \\ 10 \end{bmatrix}$$

$$OM = 14,\ 12 \text{ atau ditulis } \begin{bmatrix} O \\ M \end{bmatrix} = \begin{bmatrix} 14 \\ 12 \end{bmatrix}$$

Langkah 2;

Lakukan proses perkalian K dengan hasil dari langkah 1,

$$\begin{bmatrix} 4 & 5 \\ 1 & 7 \end{bmatrix} * \begin{bmatrix} 5 \\ 0 \end{bmatrix} = \begin{bmatrix} 20 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 5 \\ 1 & 7 \end{bmatrix} * \begin{bmatrix} 18 \\ 8 \end{bmatrix} = \begin{bmatrix} 112 \\ 74 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 5 \\ 1 & 7 \end{bmatrix} * \begin{bmatrix} 11 \\ 10 \end{bmatrix} = \begin{bmatrix} 94 \\ 81 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 5 \\ 1 & 7 \end{bmatrix} \begin{bmatrix} 14 \\ 12 \end{bmatrix} = \begin{bmatrix} 116 \\ 98 \end{bmatrix}$$

Langkah 3; Proses Enkripsi

$$C\ (FA) = \begin{bmatrix} 20 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 5 \end{bmatrix}$$

$$C\ (SI) = \begin{bmatrix} 112 \\ 74 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 22 \end{bmatrix}$$

$$C\ (LK) = \begin{bmatrix} 94 \\ 81 \end{bmatrix} \bmod 26 = \begin{bmatrix} 16 \\ 3 \end{bmatrix}$$

$$C\ (OM) = \begin{bmatrix} 116 \\ 98 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 20 \end{bmatrix}$$

Sehingga menghasilkan chipertext = **UFGWUDWU**

Proses Dekripsi

Langkah 1;

mencari invers matriks kunci menggunakan invers kunci matriks dengan menetukan determinan

$$K = \begin{bmatrix} 4 & 5 \\ 1 & 7 \end{bmatrix} \rightarrow \det K = (4)(7) - (5)(1) = 23$$

Langkah 2;

Menentukan x sebagai bilangan bulat

$$23^{-1} \bmod 26 \rightarrow 3x = 1 \bmod 26 \rightarrow 3x = 1 + 26*K$$

Dengan merujuk pada table 3.1, x = **17**.

Langkah 3;

Menentukan K^{-1} = invers modulo determinan digunakan untuk mencari invers matriks,

$$K^{-1} = 17 * \begin{bmatrix} 7 & -5 \\ -1 & 4 \end{bmatrix} = \begin{bmatrix} 119 & -85 \\ -17 & 68 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 & 19 \\ 9 & 16 \end{bmatrix}$$

Langkah 4;

Menentukan plaintext dengan cara dekripsi = invers k * cipher text

$$\begin{bmatrix} 15 & 19 \\ 9 & 16 \end{bmatrix} \begin{bmatrix} 20 \\ 5 \end{bmatrix} = \begin{bmatrix} 395 \\ 260 \end{bmatrix} \bmod 26 =$$

$$\begin{bmatrix} 15 & 19 \\ 9 & 16 \end{bmatrix} \begin{bmatrix} 8 \\ 22 \end{bmatrix} = \begin{bmatrix} 538 \\ 424 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 15 & 19 \\ 9 & 16 \end{bmatrix} \begin{bmatrix} 16 \\ 3 \end{bmatrix} = \begin{bmatrix} 297 \\ 192 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} 15 & 19 \\ 9 & 16 \end{bmatrix} \begin{bmatrix} 12 \\ 10 \end{bmatrix} = \begin{bmatrix} 560 \\ 428 \end{bmatrix} \bmod 26 =$$

Sehingga menghasilkan plaintext = **FASILKOM**