

Bahan kuliah IF4020 Kriptografi

Kriptografi Klasik

(Bagian 2)

Oleh: Dr. Rinaldi Munir

**Prodi Informatika
Sekolah Teknik Elektro dan Informatika
2019**

Beberapa *Cipher* Klasik

1. Vigenere Cipher
2. Playfair Cipher
3. Enigma Cipher
4. Affine Cipher
5. Hill Cipher

Vigènere Cipher



- Termasuk ke dalam *cipher* abjad-majemuk (*polyalphabetic substitution cipher*).
- Dipublikasikan oleh diplomat (sekaligus seorang kriptologis, Perancis, Blaise de Vigènere) pada abad 16 (tahun 1586).
- Tetapi sebenarnya Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis di dalam bukunya *La Cifra del Sig. Giovan Batista Belaso*
- Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya *cipher* tersebut kemudian dinamakan *Vigènere Cipher*

- *Cipher* ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan Abad 19 (akan dijelaskan pada bahan kuliah selanjutnya).
- *Vigènere Cipher* digunakan oleh Tentara Konfederasi (*Confederate Army*) pada Perang Sipil Amerika (*American Civil war*).
- Perang Sipil terjadi setelah *Vigènere Cipher* berhasil dipecahkan.

- *Vigènere Cipher* menggunakan Bujursangkar *Vigènere* untuk melakukan enkripsi.
- Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*.
- Kunci: $K = k_1 k_2 \dots k_m$
 k_i untuk $1 \leq i \leq m$ menyatakan jumlah pergeseran pada huruf ke- i .

Enkripsi: $c_i(p) = (p + k_i) \bmod 26$ (*)

Plainteks

	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

Gambar 4.2 Bujursangkar *Vigènere*

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik.
- Misalkan panjang kunci = 20, maka 20 karakter pertama dienkripsi dengan persamaan (*), setiap karakter ke- i menggunakan kunci k_i .

Untuk 20 karakter berikutnya, kembali menggunakan pola enkripsi yang sama.

- Contoh: kunci = sony
Plainteks: thisplaintext
Kunci: sonysonysonys

- Contoh enkripsi:

Plainteks

	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

Gambar 4.3 Enkripsi huruf T dengan kunci s

- Hasil enkripsi seluruhnya adalah sebagai berikut:

Plainteks : `thisplaintext`

Kunci : `sonysonysonys`

Cipherteks : `LVVQHZNGFHRVL`

- Pada dasarnya, setiap enkripsi huruf adalah *Caesar cipher* dengan kunci yang berbeda-beda.

$$(T + s) \bmod 26 = L$$

$$(H + o) \bmod 26 = V, \text{ dst}$$

- Huruf yang sama tidak selalu dienkripsi menjadi huruf cipherteks yang sama pula.

Contoh: huruf plainteks **T** dapat dienkripsi menjadi **L** atau **H**, dan huruf cipherteks **V** dapat merepresentasikan huruf plainteks **H**, **I**, dan **X**

- Hal di atas merupakan karakteristik dari *cipher* abjad-majemuk: setiap huruf cipherteks dapat memiliki kemungkinan banyak huruf plainteks.
- Pada *cipher* substitusi sederhana, setiap huruf cipherteks selalu menggantikan huruf plainteks tertentu.

- **Plainteks:**

Jawa Timur Bakal Tenggelam

Semburan lumpur panas di desa Porong, Sidoarjo, Jawa Timur belum juga berakhir. Sudah beberapa desa tenggelam. Entah sudah berapa rumah, bangunan, pabrik, dan sawah yang tenggelam.

Sampai kapan semburan lumpur berhenti, tiada yang tahu. Teknologi manusia tidak berhasil menutupi lubang semburan. Jika semburan lumpur tidak berhenti juga, mungkin Jawa Timur akan tenggelam

- **Kunci:** langitbiru
- **Cipherteks:**

Uajg Bbnci Vlknr Bxooxywaz

YmfcciuY lhsxns xrhls qo lxti Gicoam, Abewrluo, Wget
Uqdoc brrcf kcxu meegsajz. Jooau hmufzrjl dryi
mfvxaplms. Mguiy mfdnn jxsignu cuzgp, ubvxoyaa, viusqb,
xln fgeti grhr trtozftrg.

Dazvib liguy srsjnsie ffmcaz ufzyyytv, zqtei puyg ggpn.
Umbhzlbnq fbvlmta goltl jvlsafot ffvlnfpv rcubvx
mpmoazto. Rzel srsjnsie ffmcaz mjltre meenmguq aora,
zavzlqe Dlwn Zqfvz reln kvzhmcux

- *Vigènere Cipher* dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama seperti pada *cipher* abjad-tunggal.
- Jika periode kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditentukan dengan menulis program komputer untuk melakukan *exhaustive key search*.

- Contoh: Diberikan cipherteks sbb:

TGCSZ GEUAA EFWGQ AHQMC

dan diperoleh informasi bahwa panjang kunci adalah p huruf dan plainteks ditulis dalam Bahasa Inggris, maka *running* program dengan mencoba semua kemungkinan kunci yang panjangnya tiga huruf, lalu periksa apakah hasil dekripsi dengan kunci tersebut menyatakan kata yang berarti.

Cara ini membutuhkan usaha percobaan sebanyak 26^p kali.

Varian *Vigenere Cipher*

1. *Full Vigenere cipher*

- Setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi merupakan permutasi huruf-huruf alfabet.
- Misalnya pada baris *a* susunan huruf-huruf alfabet adalah acak seperti di bawah ini:

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

2. Auto-Key Vigènere cipher

- Jika panjang kunci lebih kecil dari panjang plainteks, maka kunci disambung dengan plainteks tersebut.

- Misalnya,

Pesan: negara penghasil minyak

Kunci: INDO

maka kunci tersebut disambung dengan plainteks semula sehingga panjang kunci menjadi sama dengan panjang plainteks:

- Plainteks : negarapenghasilminyak
- Kunci : INDONEGARAPENGHASILMI

3. *Running-Key Vigènere cipher*

- Kunci adalah string yang sangat panjang yang diambil dari teks bermakna (misalnya naskah proklamasi, naskah Pembukaan UUD 1945, terjemahan ayat di dalam kitab suci, dan lain-lain).
- Misalnya,
Pesan: `negarapenghasilminyak`
Kunci: `KEMANUSIAANYANGADILDA (NBERADAB)`
- Selanjutnya enkripsi dan dekripsi dilakukan seperti biasa.

Playfair Cipher

- Termasuk ke dalam *polygram cipher*.
- Ditemukan oleh Sir Charles Wheatstone namun dipromosikan oleh Baron Lyon Playfair pada tahun 1854.



Sir Charles Wheatstone



Baron Lyon Playfair

- *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.

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

Jumlah kemungkinan kunci:

$$25! = 15.511.210.043.330.985.984.000.000$$

Kunci dapat dipilih dari sebuah kalimat yang mudah diingat, misalnya:

JALAN GANESHA SEPULUH

Buang huruf yang berulang dan huruf J jika ada:

ALNGESHPU

Lalu tambahkan huruf-huruf yang belum ada (kecuali J):

ALNGESHPUBCDFIKMOQRTVWXYZ

Masukkan ke dalam bujursangkar:

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

Pesan yang akan dienkripsi diatur terlebih dahulu sebagai berikut:

1. Ganti huruf j (bila ada) dengan i
2. Tulis pesan dalam pasangan huruf (*bigram*).
3. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan x di tengahnya
4. Jika jumlah huruf ganjil, tambahkan huruf x di akhir

Contoh:

Plainteks: `temui ibu nanti malam`

→ Tidak ada huruf `j`, maka langsung tulis pesan dalam pasangan huruf:

te mu ix ib un an ti ma la mx

Algoritma enkripsi:

1. Jika dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya.
2. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Plainteks: temui ibu nanti malam

Bigram: te mu ix ib un an ti ma la mx

Kunci:

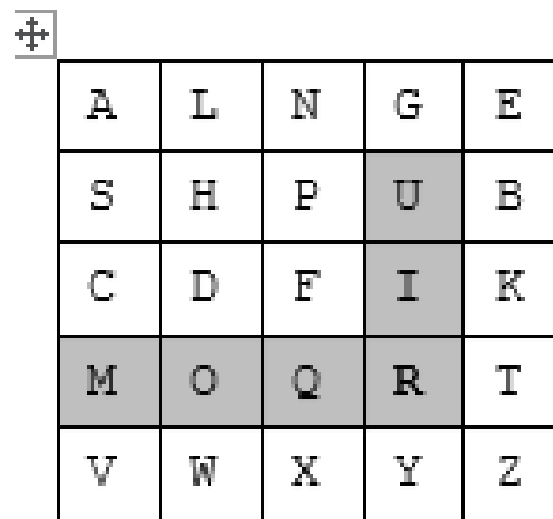
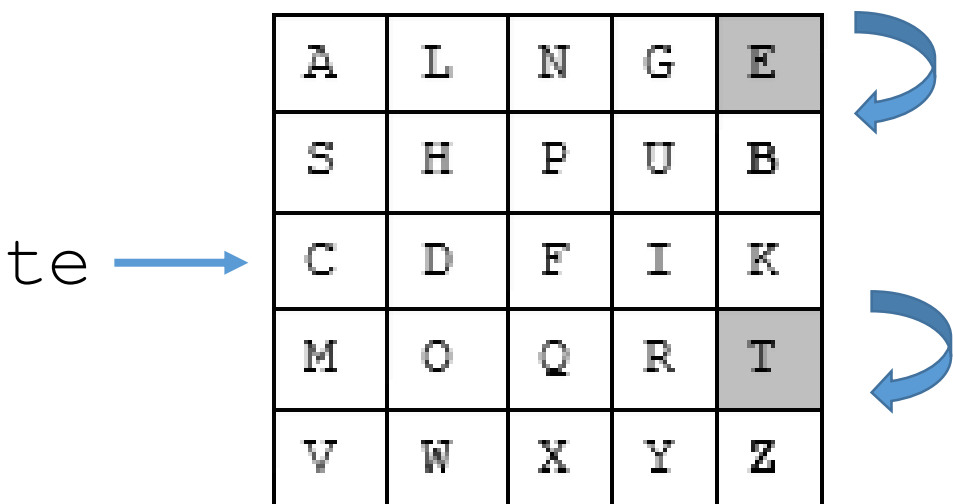
^E	A	L	N	G	E
S	H	P	U	B	
C	D	F	I	K	
M	O	Q	R	T	
V	W	X	Y	Z	

Cipherteks: ZB RS FY KU PG LG RK VS NL QV

Cara enkripsinya sebagai berikut:

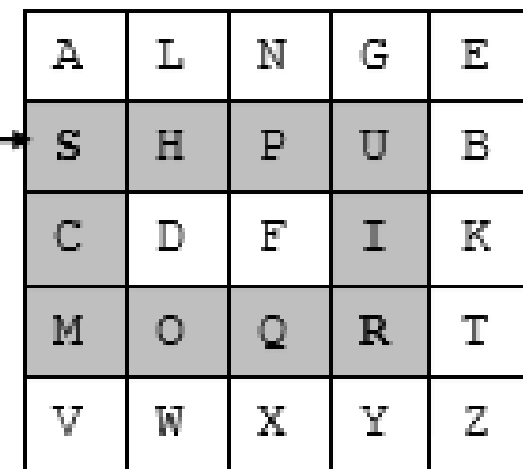
Bigram: te mu ix ib un an ti ma la mx

Cipherteks: ZB RS FY KU PG LG RK VS NL QV



Perpotongan baris M dan kolom U adalah R

Titik sudut ke-4



Titik sudut yang keempat adalah S

mu ↑

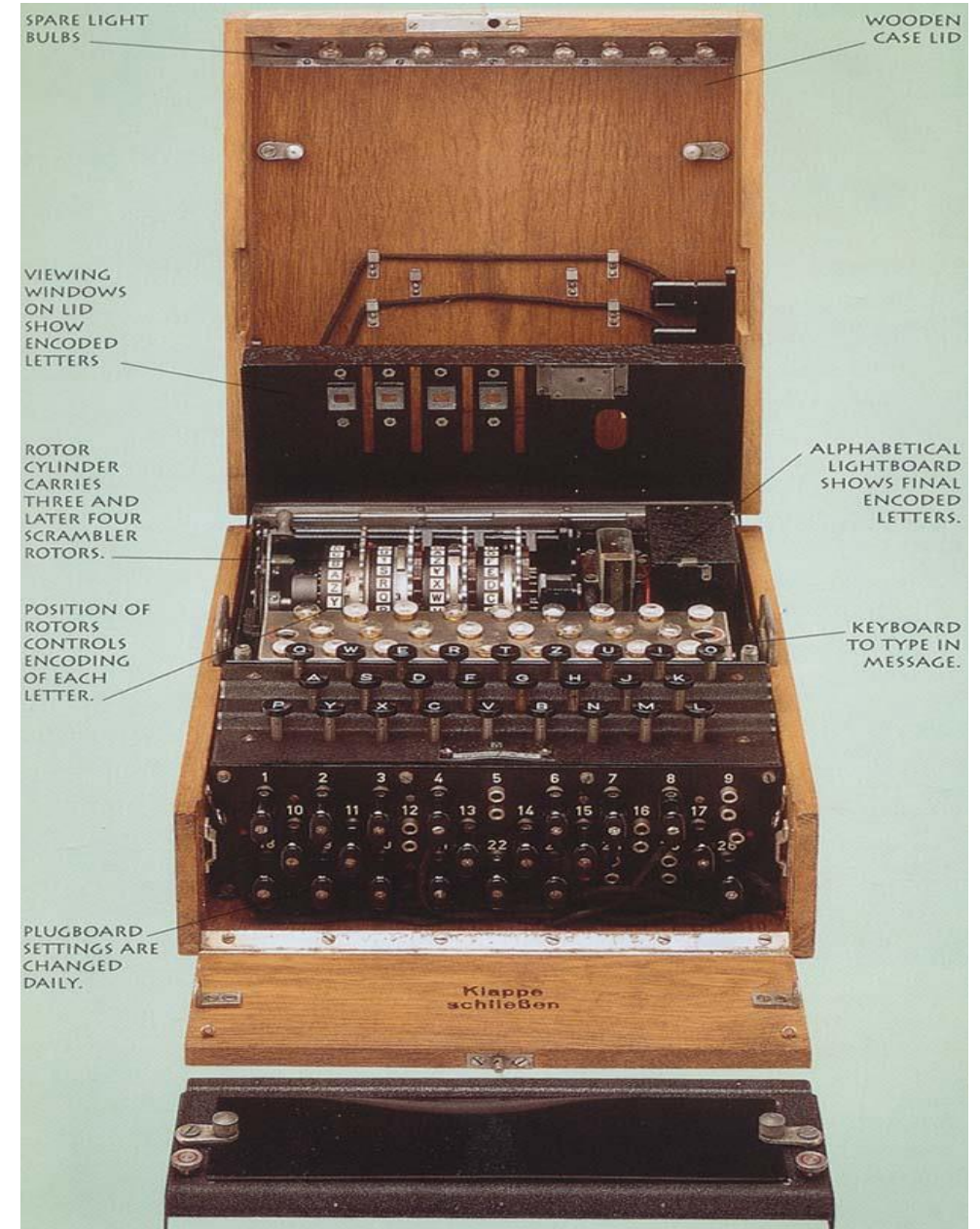
Algoritma dekripsi kebalikan dari algoritma enkripsi. Langkah-langkahnya adalah sebagai berikut:

1. Jika dua huruf terdapat pada baris bujursangkar yang sama maka tiap huruf diganti dengan huruf di kirinya.
2. Jika dua huruf terdapat pada kolom bujursangkar yang sama maka tiap huruf diganti dengan huruf di atasnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang digunakan sampai sejauh ini.
4. Buanglah huruf X yang tidak mengandung makna.

- Karena ada 26 huruf abjad, maka terdapat $26 \times 26 = 677$ bigram, sehingga identifikasi bigram individual lebih sukar.
- Sayangnya ukuran poligram di dalam *Playfair cipher* tidak cukup besar, hanya dua huruf sehingga *Playfair cipher* tidak aman.
- Meskipun *Playfair cipher* sulit dipecahkan dengan analisis frekuensi relatif huruf-huruf, namun ia dapat dipecahkan dengan analisis frekuensi pasangan huruf.
- Dalam Bahasa Inggris kita bisa mempunyai frekuensi kemunculan pasangan huruf, misalnya pasangan huruf TH dan HE paling sering muncul.

Enigma Cipher

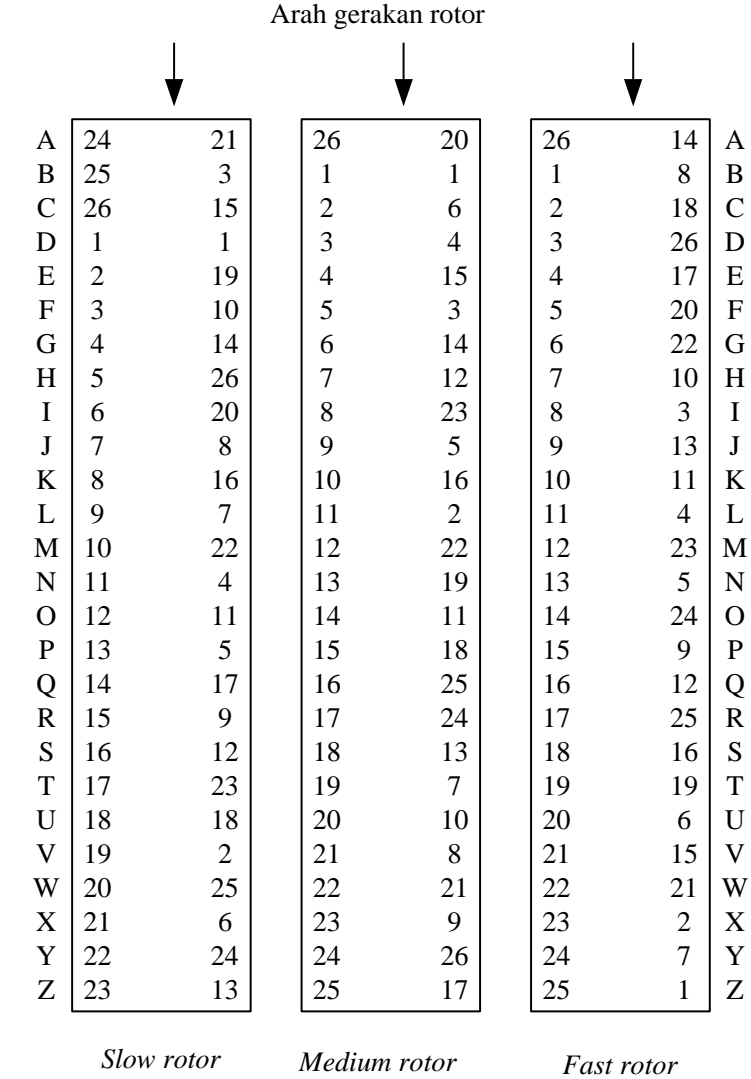
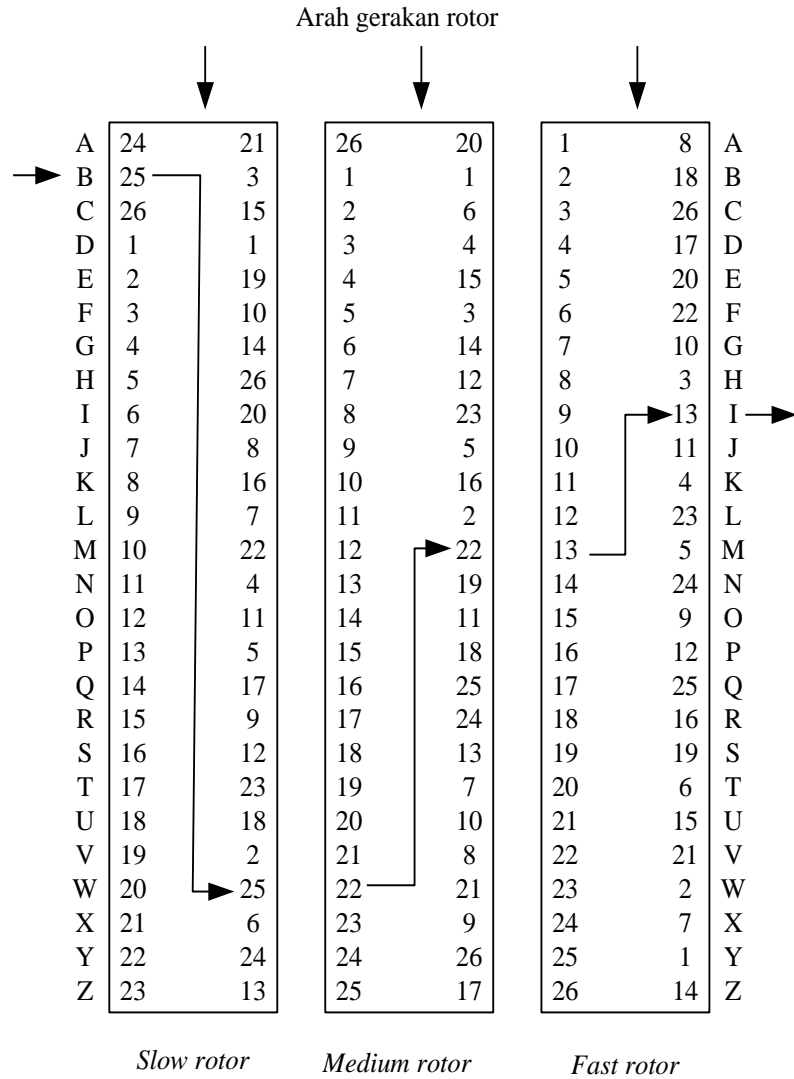
- Enigma adalah mesin yang digunakan Jerman selama Perang Dunia II untuk mengenkripsi/dekripsi pesan-pesan militer.



- Enigma menggunakan sistem *rotor* (mesin berbentuk roda yang berputar) untuk membentuk huruf cipherteks yang berubah-ubah.
- Setelah setiap huruf dienkrupsi, *rotor* kembali berputar untuk membentuk huruf cipherteks baru untuk huruf plainteks berikutnya.



- Enigma menggunakan 4 buah *rotor* untuk melakukan substitusi.
- Ini berarti terdapat $26 \times 26 \times 26 \times 26 = 456.976$ kemungkinan huruf cipherteks sebagai pengganti huruf plainteks sebelum terjadi perulangan urutan cipherteks.
- Setiap kali sebuah huruf selesai disubstitusi, *rotor* pertama bergeser satu huruf ke atas.
- Setiap kali *rotor* pertama selesai bergeser 26 kali, rotor kedua juga melakukan hal yang sama, demikian untuk *rotor* ke-3 dan ke-4.



(a) Kondisi rotor pada penekanan huruf A

(b) Posisi rotor setelah penekanan huruf A

- Posisi awal keempat *rotor* dapat di-*set*; dan posisi awal ini menyatakan kunci dari Enigma.
- Jerman meyakini bahwa cipherteks yang dihasilkan Enigma tidak mungkin dipecahkan. Namun, sejarah membuktikan bahwa pihak Sekutu berhasil juga memecahkan kode Enigma.
- Keberhasilan memecahkan Enigma dianggap sebagai faktor yang memperpendek Perang Dunia II menjadi hanya 2 tahun.

Affine Cipher

- Perluasan dari *Caesar cipher*
- Enkripsi: $C \equiv mP + b \pmod{n}$
- Dekripsi: $P \equiv m^{-1}(C - b) \pmod{n}$
- Kunci: m dan b

Keterangan:

1. n adalah ukuran alfabet
2. m bilangan bulat yang relatif prima dengan n
3. b adalah jumlah pergeseran
4. *Caesar cipher* adalah khusus dari *affine cipher* dengan $m = 1$
5. m^{-1} adalah inversi $m \pmod{n}$, yaitu $m \cdot m^{-1} \equiv 1 \pmod{n}$

- Contoh:

Plainteks: k r i p t o (10 17 8 15 19 14)

$n = 26$, ambil $m = 7$ (7 relatif prima dengan 26)

Enkripsi: $C \equiv 7P + 10 \pmod{26}$

$$p_1 = 10 \rightarrow c_1 \equiv 7 \cdot 10 + 10 \equiv 80 \equiv 2 \pmod{26} \quad (\text{huruf 'C'})$$

$$p_2 = 17 \rightarrow c_2 \equiv 7 \cdot 17 + 10 \equiv 129 \equiv 25 \pmod{26} \quad (\text{huruf 'Z'})$$

$$p_3 = 8 \rightarrow c_3 \equiv 7 \cdot 8 + 10 \equiv 66 \equiv 14 \pmod{26} \quad (\text{huruf 'O'})$$

$$p_4 = 15 \rightarrow c_4 \equiv 7 \cdot 15 + 10 \equiv 115 \equiv 11 \pmod{26} \quad (\text{huruf 'L'})$$

$$p_5 = 19 \rightarrow c_5 \equiv 7 \cdot 19 + 10 \equiv 143 \equiv 13 \pmod{26} \quad (\text{huruf 'N'})$$

$$p_6 = 14 \rightarrow c_6 \equiv 7 \cdot 14 + 10 \equiv 108 \equiv 4 \pmod{26} \quad (\text{huruf 'E'})$$

Cipherteks: CZOLNE

- Dekripsi:

- Mula-mula hitung m^{-1} yaitu $7^{-1} \pmod{26}$ dengan memecahkan $7x \equiv 1 \pmod{26}$

Solusinya: $x \equiv 15 \pmod{26}$ sebab $7 \cdot 15 = 105 \equiv 1 \pmod{26}$.

- Jadi, $P \equiv 15(C - 10) \pmod{26}$

$$c_1 = 2 \rightarrow p_1 \equiv 15 \cdot (2 - 10) = -120 \equiv 10 \pmod{26} \quad (\text{huruf 'k'})$$

$$c_2 = 25 \rightarrow p_2 \equiv 15 \cdot (25 - 10) = 225 \equiv 17 \pmod{26} \quad (\text{huruf 'r'})$$

$$c_3 = 14 \rightarrow p_3 \equiv 15 \cdot (14 - 10) = 60 \equiv 8 \pmod{26} \quad (\text{huruf 'i'})$$

$$c_4 = 11 \rightarrow p_4 \equiv 15 \cdot (11 - 10) = 15 \equiv 15 \pmod{26} \quad (\text{huruf 'p'})$$

$$c_5 = 13 \rightarrow p_5 \equiv 15 \cdot (13 - 10) = 45 \equiv 19 \pmod{26} \quad (\text{huruf 't'})$$

$$c_6 = 4 \rightarrow p_6 \equiv 15 \cdot (4 - 10) = -90 \equiv 14 \pmod{26} \quad (\text{huruf 'o'})$$

Plainteks yang diungkap kembali: `kripto`

- *Affine cipher* tidak aman, karena kunci mudah ditemukan dengan *exhaustive search*,
- sebab ada 25 pilihan untuk b dan 12 buah nilai m yang relatif prima dengan 26 (yaitu 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, dan 25).

- Salah satu cara memperbesar faktor kerja untuk *exhaustive key search*: enkripsi tidak dilakukan terhadap huruf individual, tetapi dalam blok huruf.

- Misal, pesan kriptografi dipecah menjadi kelompok 4-huruf:

krip togr a fi

(ekivalen dengan 10170815 19140617 000508, dengan memisalkan 'A' = 0, 'B' = 1, ..., 'Z' = 25)

- Nilai terbesar yang dapat muncul untuk merepresentasikan blok: 25252525 (ZZZZ), maka 25252525 dapat digunakan sebagai modulus n .
- Nilai m yang relatif prima dengan 25252525, misalnya 21035433,
- b dipilih antara 1 dan 25252525, misalnya 23210025.

- Fungsi enkripsi menjadi:

$$C \equiv 21035433P + 23210025 \pmod{25252525}$$

- Fungsi dekripsi, setelah dihitung, menjadi

$$P \equiv 5174971 (C - 23210025) \pmod{25252525}$$

- *Affine cipher* mudah diserang dengan *known-plaintext attack*.
- Misalkan kriptanalisis mempunyai dua buah plainteks, P_1 dan P_2 , yang berkoresponden dengan cipherteks C_1 dan C_2 ,
- maka m dan b mudah dihitung dari buah kekongruenan simultan berikut ini:

$$C_1 \equiv mP_1 + b \pmod{n}$$

$$C_2 \equiv mP_2 + b \pmod{n}$$

- Contoh: Misalkan kriptanalis menemukan
cipherteks C dan plainteks berkoresponden K
cipherteks E dan plainteks berkoresponden O .

- Kriptanalis m dan n dari kekongruenan berikut:

$$2 \equiv 10m + b \pmod{26} \quad (i)$$

$$4 \equiv 14m + b \pmod{26} \quad (ii)$$

- Kurangkan (ii) dengan (i), menghasilkan

$$2 \equiv 4m \pmod{26} \quad (iii)$$

$$\text{Solusi: } m = 7$$

Substitusi $m = 7$ ke dalam (i),

$$2 \equiv 70 + b \pmod{26} \quad (iv)$$

$$\text{Solusi: } b = 10.$$

Hill Cipher

- Dikembangkan oleh Lester Hill (1929)
- Menggunakan m buah persamaan linier
- Untuk $m = 3$ (enkripsi setiap 3 huruf),

$$C_1 = (k_{11} p_1 + k_{12} p_2 + k_{13} p_3) \text{ mod } 26$$

$$C_2 = (k_{21} p_1 + k_{22} p_2 + k_{23} p_3) \text{ mod } 26$$

$$C_3 = (k_{31} p_1 + k_{32} p_2 + k_{33} p_3) \text{ mod } 26$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

$$\mathbf{C} = \mathbf{K} \mathbf{P}$$

- Contoh:

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Plainteks: paymoremoney

Enkripsi tiga huruf pertama: pay = (15, 0, 24)

$$\text{Cipherteks: } \mathbf{C} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS}$$

Cipherteks selengkapnya: LNSHDLEWMTRW

- Dekripsi perlu menghitung \mathbf{K}^{-1} sedemikian sehingga $\mathbf{K}\mathbf{K}^{-1} = \mathbf{I}$ (\mathbf{I} matriks identitas).

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

sebab

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- Cara menghitung matriks invers 2 x 2:

$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad K^{-1} = \frac{1}{\det(K)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
$$= \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Contoh: $K = \begin{pmatrix} 3 & 10 \\ 15 & 9 \end{pmatrix}$

$$\det(K) = (3)(9) - (15)(10) = 27 - 150 = -123 \pmod{26} = 7$$

$$\begin{aligned} \mathbf{K}^{-1} &= \frac{1}{7} \begin{pmatrix} 3 & 10 \\ 15 & 9 \end{pmatrix} = 7^{-1} \begin{pmatrix} 9 & -10 \\ -15 & 3 \end{pmatrix} \\ &= 15 \begin{pmatrix} 9 & -10 \\ -15 & 3 \end{pmatrix} = 15 \begin{pmatrix} 9 & 16 \\ 11 & 3 \end{pmatrix} = \begin{pmatrix} 135 & 240 \\ 165 & 45 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 6 \\ 9 & 19 \end{pmatrix} \end{aligned}$$

Keterangan: (i) $7^{-1} \pmod{26} \equiv 15$, karena
 $(7)(15) = 105 \pmod{26} = 1$
(ii) $-10 \equiv 16 \pmod{26}$
(iii) $-15 \equiv 11 \pmod{26}$)

Periksa bahwa:

$$\begin{aligned} \mathbf{K}\mathbf{K}^{-1} &= \begin{pmatrix} 3 & 10 \\ 15 & 9 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 9 & 19 \end{pmatrix} = \begin{pmatrix} 3 \cdot 5 + 10 \cdot 9 & 3 \cdot 6 + 10 \cdot 19 \\ 15 \cdot 5 + 9 \cdot 9 & 15 \cdot 6 + 9 \cdot 19 \end{pmatrix} \\ &= \begin{pmatrix} 105 & 208 \\ 156 & 261 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

- Untuk matriks 3 x 3:

$$\mathbf{K} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}, \quad \mathbf{K}^{-1} = \frac{1}{\det(\mathbf{K})} \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}^T = \frac{1}{\det(\mathbf{K})} \begin{pmatrix} A & D & G \\ B & E & H \\ C & F & I \end{pmatrix}$$

- yang dalam hal ini,

$$A = (ei - hf) \quad B = -(di - fg) \quad C = (dh - eg)$$

$$D = -(bi - hc) \quad E = (ai - cg) \quad F = -(ah - bg)$$

$$G = (bf - ec) \quad H = -(af - cd) \quad I = (ae - bd)$$

dan

$$\det(\mathbf{K}) = aA + bB + cC$$

- Dekripsi:

$$\mathbf{P} = \mathbf{K}^{-1} \mathbf{C}$$

Cipherteks: LNS atau $\mathbf{C} = (11, 13, 18)$

$$\text{Plainteks: } \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \begin{pmatrix} 431 \\ 494 \\ 570 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$$

$$\mathbf{C} = (15, 0, 24) = (\text{P}, \text{A}, \text{Y})$$

- Kekuatan Hill cipher terletak pada penyembunyian frekuensi huruf tunggal
- Huruf plainteks yang sama belum tentu dienkripsi menjadi huruf cipherteks yang sama.

- *Hill cipher* mudah dipecahkan dengan *known-plaintext attack*.
- Misalkan untuk *Hill cipher* dengan $m = 2$ diketahui:
 - $P = (19, 7) \rightarrow C = (0, 23)$
 - $P = (4, 17) \rightarrow C = (12, 6)$
 - Jadi, $\mathbf{K}(19, 7) = (0, 23)$ dan $\mathbf{K}(4, 17) = (12, 6)$

$$\begin{pmatrix} 0 & 12 \\ 23 & 6 \end{pmatrix} = \mathbf{K} \begin{pmatrix} 19 & 4 \\ 7 & 17 \end{pmatrix} \pmod{26}$$

$$\begin{matrix} \leftarrow C \rightarrow & & \leftarrow P \rightarrow \\ & & \left(\begin{pmatrix} 19 & 4 \\ 7 & 17 \end{pmatrix} \right)^{-1} \end{matrix} \pmod{26} = \begin{pmatrix} 25 & 14 \\ 5 & 5 \end{pmatrix}$$

- Inversi dari P adalah $P^{-1} = \begin{pmatrix} 19 & 4 \\ 7 & 17 \end{pmatrix}^{-1} \pmod{26} = \begin{pmatrix} 25 & 14 \\ 5 & 5 \end{pmatrix}$
- Sehingga

$$\mathbf{K} = \mathbf{C}P^{-1} \pmod{26} = \begin{pmatrix} 0 & 12 \\ 23 & 6 \end{pmatrix} \begin{pmatrix} 25 & 14 \\ 5 & 5 \end{pmatrix} \pmod{26} = \begin{pmatrix} 8 & 8 \\ 7 & 14 \end{pmatrix}$$