Beberapa Algoritma Kriptografi Klasik

Bahan Kuliah IF4020 Kriptografi

Vigènere Cipher

- Termasuk ke dalam *cipher* abjad-majemuk (*polyalpabetic 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 Konfiderasi (*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: $K = k_1 k_2 \ldots k_m$

  k_i untuk $1 \le i \le m$ menyatakan jumlah pergeseran pada huruf ke-i.

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

Plainteks

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

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

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

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) mod 26 = L
(H + o) mod 26 = V, dst

- Huruf yang sama tidak selalu dienkripsi menjadi huruf cipheteks 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 mfvxaplns. Mguiy mfdnn jxsigu cuzgp,
ubvxoyaa, viusqb, xln fgeti grhr trtozftrg.

Dazvib liguy srsjnsie ffmcaz ufzyyytv, zqtei
puyg ggpn. Umbhzlbmq fbvlmta goltl jvlsafot
ffvlnfpv rcubvx mpmoazto. Rzel srsjnsie ffmcaz
mjlre 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 Vigènere 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: `NEGARA PENGHASIL MINYAK`

  Kunci: `KEMANUSIAN YANG ADIL DAN BERADAB`

- 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.

Contoh kunci:

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

Jumlah kemungkinan kunci:
25!=15.511.210.043.330.985.984.000.000

- Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam.

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

Baris ke-6 = baris ke-1

Kolom ke-6 = kolom ke-1

- 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 `Z` di
- tengahnya
- 4. Jika jumlah huruf ganjil,tambahkan
- huruf `Z` di akhir

Contoh:

Plainteks: `GOOD BROOMS SWEEP CLEAN`

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

<u>GO</u> <u>OD</u> <u>BR</u> <u>OZ</u> <u>OM</u> <u>SZ</u> <u>SW</u> <u>EZ</u> <u>EP</u> <u>CL</u> <u>EA</u> <u>NZ</u>

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.

Contoh: Kunci (yang sudah diperluas) ditulis kembali sebagai berikut:

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

Plainteks (dalam pasangan huruf):

GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Cipherteks:

FP UT EC UW PO DV TV BV CM BG CS DY

Enkripsi `OD` menjadi **`UT`** ditunjukkan pada bujursangkar di bawah ini:

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

titik sudut ke-4

↓

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

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`

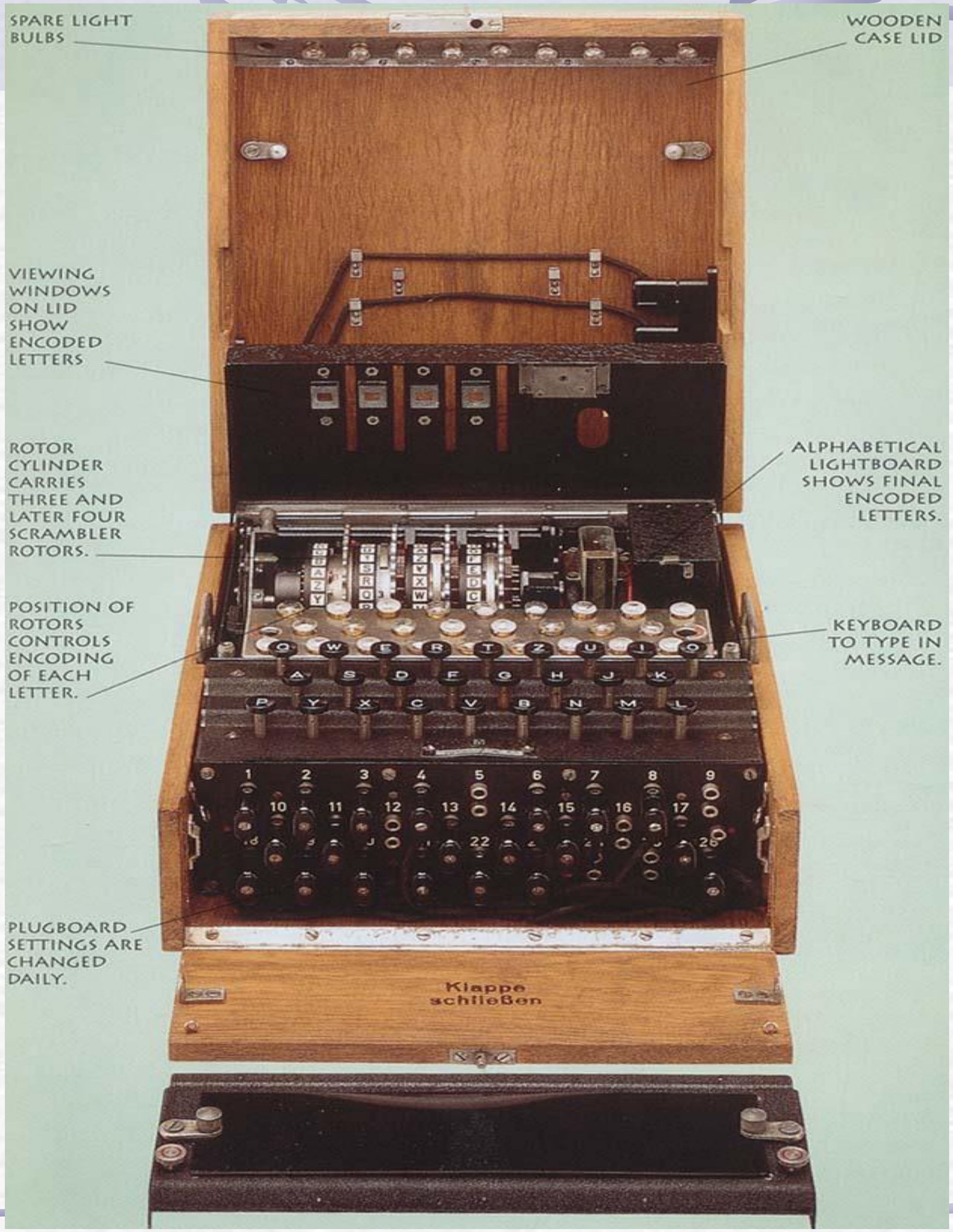
Masukkan ke dalam bujursangkar:

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

- Karena ada 26 huruf abjad, maka terdapat 26 x 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.
- Dengan menggunakan tabel frekuensi kemunculan pasangan huruf di dalam Bahasa Inggris dan cipherteks yang cukup banyak, *Playfair cipher* dapat dipecahkan.

Enigma *Cipher*

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


SPARE LIGHT BULBS
WOODEN CASE LID
VIEWING WINDOWS ON LID SHOW ENCODED LETTERS
ROTOR CYLINDER CARRIES THREE AND LATER FOUR SCRAMBLER ROTORS.
ALPHABETICAL LIGHTBOARD SHOWS FINAL ENCODED LETTERS.
POSITION OF ROTORS CONTROLS ENCODING OF EACH LETTER.
KEYBOARD TO TYPE IN MESSAGE.
PLUGBOARD SETTINGS ARE CHANGED DAILY.
Klappe schließen

- Enigma menggunakan sistem *rotor* (mesin berbentuk roda yang berputar) untuk membentuk huruf cipherteks yang berubah-ubah.
- Setelah setiap huruf dienkripsi, *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.

Arah gerakan rotor

	Slow rotor		Medium rotor		Fast rotor		
A	24	21	26	20	1	8	A
B	25	3	1	1	2	18	B
C	26	15	2	6	3	26	C
D	1	1	3	4	4	17	D
E	2	19	4	15	5	20	E
F	3	10	5	3	6	22	F
G	4	14	6	14	7	10	G
H	5	26	7	12	8	3	H
I	6	20	8	23	9	13	I
J	7	8	9	5	10	11	J
K	8	16	10	16	11	4	K
L	9	7	11	2	12	23	L
M	10	22	12	22	13	5	M
N	11	4	13	19	14	24	N
O	12	11	14	11	15	9	O
P	13	5	15	18	16	12	P
Q	14	17	16	25	17	25	Q
R	15	9	17	24	18	16	R
S	16	12	18	13	19	19	S
T	17	23	19	7	20	6	T
U	18	18	20	10	21	15	U
V	19	2	21	8	22	21	V
W	20	25	22	21	23	2	W
X	21	6	23	9	24	7	X
Y	22	24	24	26	25	1	Y
Z	23	13	25	17	26	14	Z

(a) Kondisi rotor pada penekanan huruf A

Arah gerakan rotor

	Slow rotor		Medium rotor		Fast rotor		
A	24	21	26	20	26	14	A
B	25	3	1	1	1	8	B
C	26	15	2	6	2	18	C
D	1	1	3	4	3	26	D
E	2	19	4	15	4	17	E
F	3	10	5	3	5	20	F
G	4	14	6	14	6	22	G
H	5	26	7	12	7	10	H
I	6	20	8	23	8	3	I
J	7	8	9	5	9	13	J
K	8	16	10	16	10	11	K
L	9	7	11	2	11	4	L
M	10	22	12	22	12	23	M
N	11	4	13	19	13	5	N
O	12	11	14	11	14	24	O
P	13	5	15	18	15	9	P
Q	14	17	16	25	16	12	Q
R	15	9	17	24	17	25	R
S	16	12	18	13	18	16	S
T	17	23	19	7	19	19	T
U	18	18	20	10	20	6	U
V	19	2	21	8	21	15	V
W	20	25	22	21	22	21	W
X	21	6	23	9	23	2	X
Y	22	24	24	26	24	7	Y
Z	23	13	25	17	25	1	Z

(b) Posisi rotor stelah 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

<u>Keterangan</u>:

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: `KRIPTO` (10 17 8 15 19 14)

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

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

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

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

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

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

$p_5 = 19 \rightarrow c_1 \equiv 7 \cdot 19 + 10 \equiv 143 \equiv 13 \pmod{26}$ (huruf 'N')

$p_6 = 14 \rightarrow c_1 \equiv 7 \cdot 14 + 10 \equiv 108 \equiv 4 \pmod{26}$ (huruf 'E')

Cipherteks: **`CZOLNE`**

- Dekripsi:

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

    Solusinya: $x \equiv 15$ (mod 26) sebab $7 \cdot 15 = 105 \equiv 1$(mod 26).

  - Jadi, $P \equiv 15\,(C - 10)$ (mod 26)

$c_1 = 2 \rightarrow p_1 \equiv 15 \cdot (2 - 10) = -120 \equiv 10$ (mod 26) (huruf 'K')
$c_2 = 25 \rightarrow p_2 \equiv 15 \cdot (25 - 10) = 225 \equiv 17$ (mod 26) (huruf 'R')
$c_3 = 14 \rightarrow p_3 \equiv 15 \cdot (14 - 10) = 60 \equiv 8$ (mod 26) (huruf 'I')
$c_4 = 11 \rightarrow p_4 \equiv 15 \cdot (11 - 10) = 15 \equiv 15$ (mod 26) (huruf 'P')
$c_5 = 13 \rightarrow p_5 \equiv 15 \cdot (13 - 10) = 45 \equiv 19$ (mod 26) (huruf 'T')
$c_6 = 4 \rightarrow p_6 \equiv 15 \cdot (4 - 10) = -90 \equiv 14$ (mod 26) (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 AFI`

  (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 kriptanalis 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 berkorepsonden `K` cipherteks **E** dan plainteks berkoresponden `O`.

- Kriptanalis *m* dan *n* dari kekongruenan berikut:

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

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

- Kurangkan (ii) dengan (i), menghasilkan

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

  Solusi: $m = 7$

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

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

Solusi: $b = 10$.

Cipher lainnya

1. Hill cipher

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

$$C_1 = (k_{11}\, p_1 + k_{12} p_2 + k_{13}\, p_3) \bmod 26$$
$$C_2 = (k_{21}\, p_1 + k_{22} p_2 + k_{23}\, p_3) \bmod 26$$
$$C_3 = (k_{31}\, p_1 + k_{32} p_2 + k_{33}\, p_3) \bmod 26$$

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

- 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)`

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

Cipherteks selengkapnya: **LNSHDLEWMTRW**

- Dekripsi perlu menghitung $\mathbf{K}^{-1}$ sedemikian sehingga $\mathbf{KK}^{-1} = \mathbf{I}$ ($\mathbf{I}$ 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} = $\dfrac{1}{\det(K)}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$= \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

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

det(K) = (3)(9) – (15)(10) = 27 – 150

= –123 mod 26 = 7

$$\mathbf{K}^{-1} = \frac{1}{7}\begin{pmatrix} 3 & 10 \\ 15 & 9 \end{pmatrix} = 7^{-1}\begin{pmatrix} 9 & -10 \\ -15 & 3 \end{pmatrix}$$

$$= 15\begin{pmatrix} 9 & -10 \\ -15 & 3 \end{pmatrix} = 15\begin{pmatrix} 9 & 16 \\ 11 & 3 \end{pmatrix} = \begin{pmatrix} 135 & 240 \\ 165 & 45 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 6 \\ 9 & 19 \end{pmatrix}$$

Keterangan: (i) 7^{-1} (mod 26) ≡ 15, karena

(7)(15) = 105 mod 26 = 1

(ii) –10 ≡ 16 (mod 26)

(iii) –15 ≡ 11 (mod 26))

Periksa bahwa:

$$\mathbf{KK}^{-1} = \begin{pmatrix} 3 & 10 \\ 15 & 9 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 9 & 19 \end{pmatrix} = \begin{pmatrix} 3\cdot 5+10\cdot 9 & 3\cdot 6+10\cdot 19 \\ 15\cdot 5+9\cdot 9 & 15\cdot 6+9\cdot 19 \end{pmatrix}$$

$$= \begin{pmatrix} 105 & 208 \\ 156 & 261 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- 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:

P = **K**$^{-1}$ **C**

Cipherteks: `LNS` atau C = (11, 13, 18)

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

C = (15, 0, 24) = (P, A, 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) → C = (0, 23)
  - P = (4, 17) → C = (12, 6)
  - Jadi, **K**(19, 7) = (0, 23) dan **K**(4, 17) = (12, 6)

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

$$\leftarrow \mathrm{C} \rightarrow \qquad \leftarrow \mathrm{P} \rightarrow$$

  - Inversi dari P adalah P^{-1} = $\begin{pmatrix} 19 & 4 \\ 7 & 17 \end{pmatrix}^{-1} \bmod 26 = \begin{pmatrix} 25 & 14 \\ 5 & 5 \end{pmatrix}$
  - Sehingga
    $\mathbf{K} = \mathbf{CP}^{-1} \bmod 26 = \begin{pmatrix} 0 & 12 \\ 23 & 6 \end{pmatrix}\begin{pmatrix} 25 & 14 \\ 5 & 5 \end{pmatrix} \bmod 26 = \begin{pmatrix} 8 & 8 \\ 7 & 14 \end{pmatrix}$