Bahan kuliah II4031 Kriptografi dan Koding

03 – Ragam Cipher Klasik
(Bagian 2)

Oleh: Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2024

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: `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')

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

  $p_6 = 14 \rightarrow c_6 \equiv 7 \cdot 14 + 10 \equiv 108 \equiv 4 \pmod{26}$ (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, $P \equiv 15\,(C - 10) \pmod{26}$

  Cipherteks: `CZOLNE` (dalam angka: 2, 25, 14, 11, 13, 4)

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

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

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

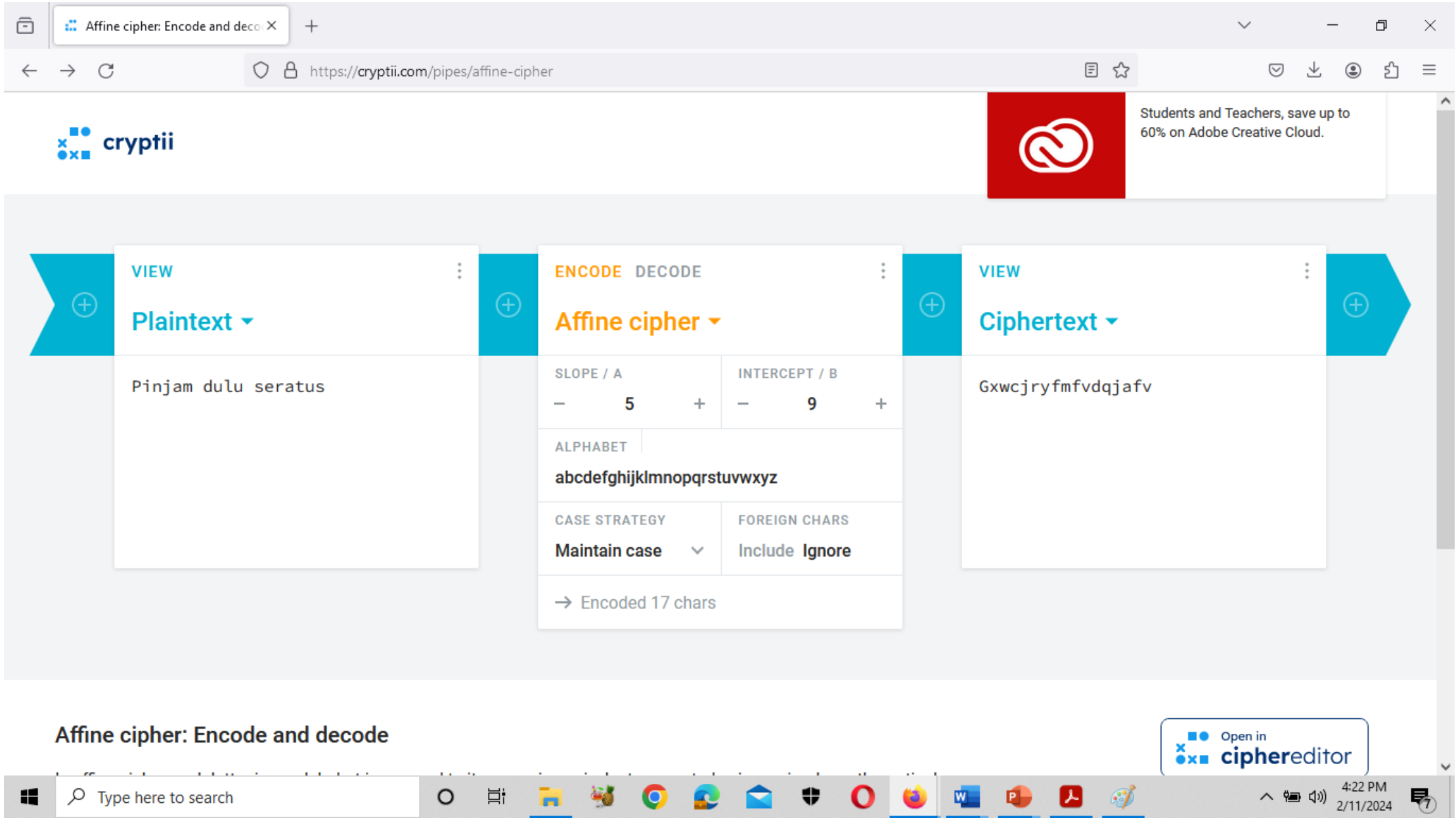
  $c_4 = 11 \rightarrow p_4 \equiv 15 \cdot (11 - 10) = 15 \equiv 15 \pmod{26}$ (huruf 'p')

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

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

  Plainteks yang diungkap kembali: `kripto`

Demo affine cipher online: https://cryptii.com/pipes/affine-cipher



Vigènere Cipher

- Termasuk ke dalam *cipher* abjad-majemuk (*polyalpabetic substitution cipher*).

- Penemu cipher ini sebenarnya adalah Giovan Batista Belaso, karena ia menggambarkan pertama kali pada tahun 1553 seperti ditulis di dalam bukunya *La Cifra del Sig. Giovan Batista Belaso.*

- Namun, *cipher* ini disempurnakan dan dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16 (tahun 1586).

- Pada abat ke-19, banyak orang yang mengira Vigenère adalah penemu cipher ini, sehingga dikenal luas sebagai *Vigenère Cipher*.

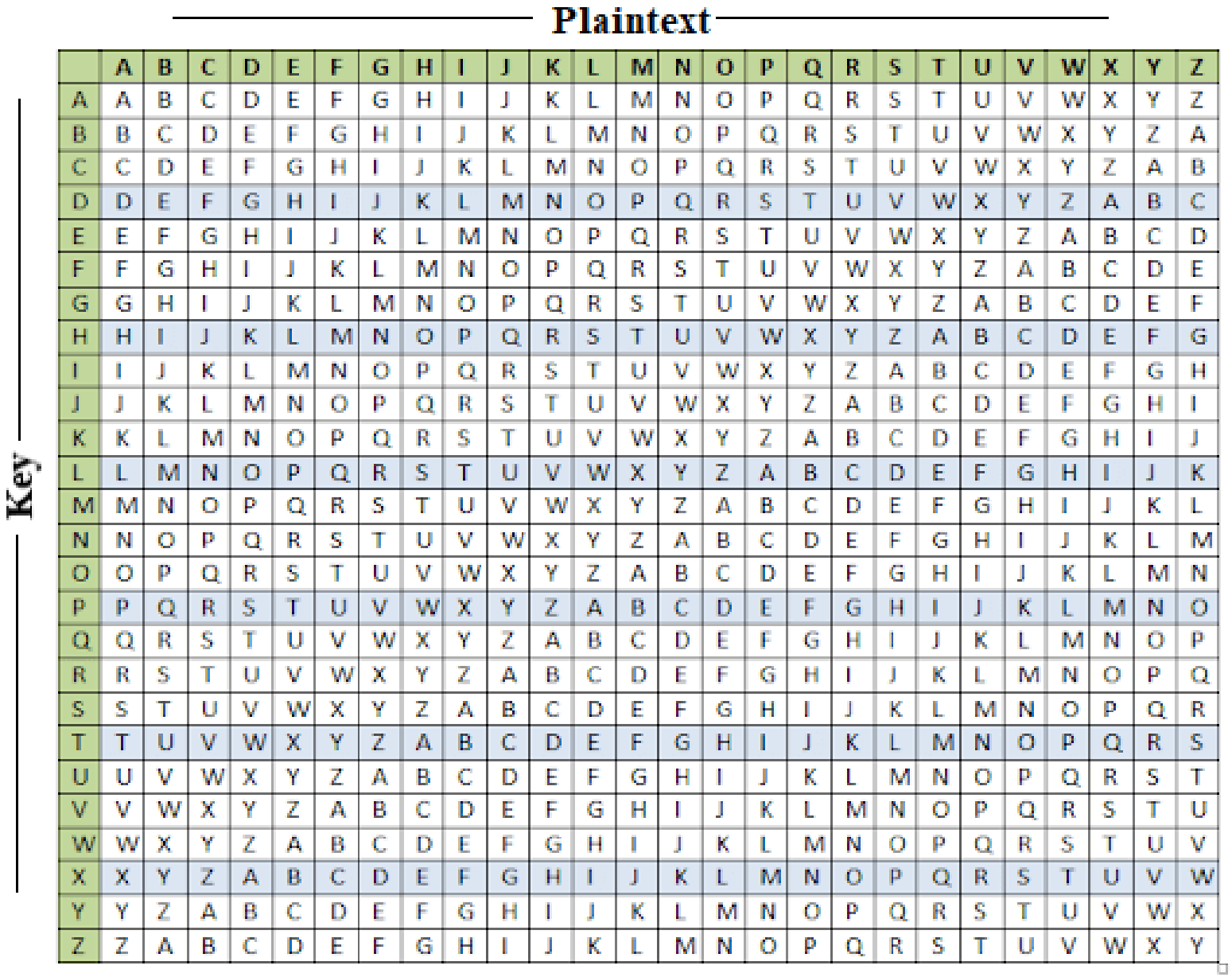
- *Cipher* ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan Abad 19 (akan dijelaskan pada materi selanjutnya).

- Kasiski menguraikan langkah-Langkah untuk menemukan panjang kunci (bukan huruf-huruf kuncikunci).

- *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 matriks *Vigènere* (*Vigenere square*) untuk melakukan enkripsi dan dekripsi.



	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

- Setiap baris *i* di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh menggunakan *Caesar Cipher* dengan kunci *k* = *i*.
- Artinya, setiap baris *i* merupakan pergeseran huruf alfabet sejauh *i* ke kanan

Plaintext

Key

	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

→ baris ke-0

→ baris ke-25

A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7, I = 8, J = 9, K = 10
L = 11, M = 12, N = 13, O = 14, P = 15, Q = 16, R = 17, S = 18, T = 19, U = 20
V = 21, W = 22, X = 23, Y = 24, Z = 25

- Kunci adalah string: $K = k_1 k_2 \ldots k_m$

  k_i untuk $1 \leq i \leq m$ menyatakan huruf-huruf alfabet

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik.

- Misalkan panjang kunci m = 10, maka 10 huruf pertama plainteks dienkripsi dengan kunci K, setiap huruf ke-i menggunakan kunci k_i.

Contoh: kunci = `sony` (dalam angka: 18, 14, 13, 24)

Plainteks: `thisplaintext`

Kunci: `sonysonysonys`

Ini artinya setiap huruf plainteks dienkripsi menggunakan *Caesar Cipher* dengan kunci *k* yang berbeda-beda

Untuk 10 karakter berikutnya, kembali menggunakan pola enkripsi yang sama.

- Enkripsi dilakukan dengan mencari titik potong huruf plainteks dengan huruf kunci:

Plainteks : **t**hisplaintext
Kunci : **s**onysonysonys
Cipherteks: **L**

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

A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7, I = 8, J = 9, K = 10
L = 11, M = 12, N = 13, O = 14, P = 15, Q = 16, R = 17, S = 18, T = 19, U = 20
V = 21, W = 22, X = 23, Y = 24, Z = 25

- Hasil enkripsi seluruhnya adalah sebagai berikut:

  Plainteks : `thisplaintext`
  Kunci : `sonysonysonys`
  Cipherteks : `LVVQHZNGFHRVL`

- Tanpa menggunakan *Vigenere Square* pun enkripsi tetap dapat dihitung secara *Caesar Cipher* dengan menjumlahkan plainteks p_j dengan kunci k_i dalam modulus 26:

  Enkripsi: $c_j = E(p_j) = (p_j + k_i) \bmod 26$ (1)

  Dekripsi: $p_j = D(c_j) = (c_j - k_i) \bmod 26$ (2)

  Contoh:

  (t + s) mod 26 = (19 + 18) mod 26 = 37 mod 26 = 11 = L

  (h + o) mod 26 = (7 + 14) mod 26 = 21 mod 26 = 21 = V, dst

- Kelebihan Vigenere Cipher: huruf plainteks yang sama tidak selalu dienkripsi menjadi huruf cipheteks yang sama pula, bergantung huruf kunci yang digunakan.

  Contoh: pada contoh di atas, 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.

- Bandingkan dengan *cipher* abjad-tunggal, setiap huruf cipherteks selalu menggantikan huruf plainteks tertentu.

Plainteks:

Dinas Pendidikan Kota Ternate meminta kepada pihak sekolah dan orang tua siswa untuk jenjang pendidikan SD dan SMP se-Kota Ternate untuk melarang para siswa membawa permainan lato-lato yang sedang tren itu ke sekolah, karena akan mengganggu kegiatan belajar mengajar yang dinilai berbahaya sehingga mengantisipasi kecelakaan bagi anak di daerah itu.

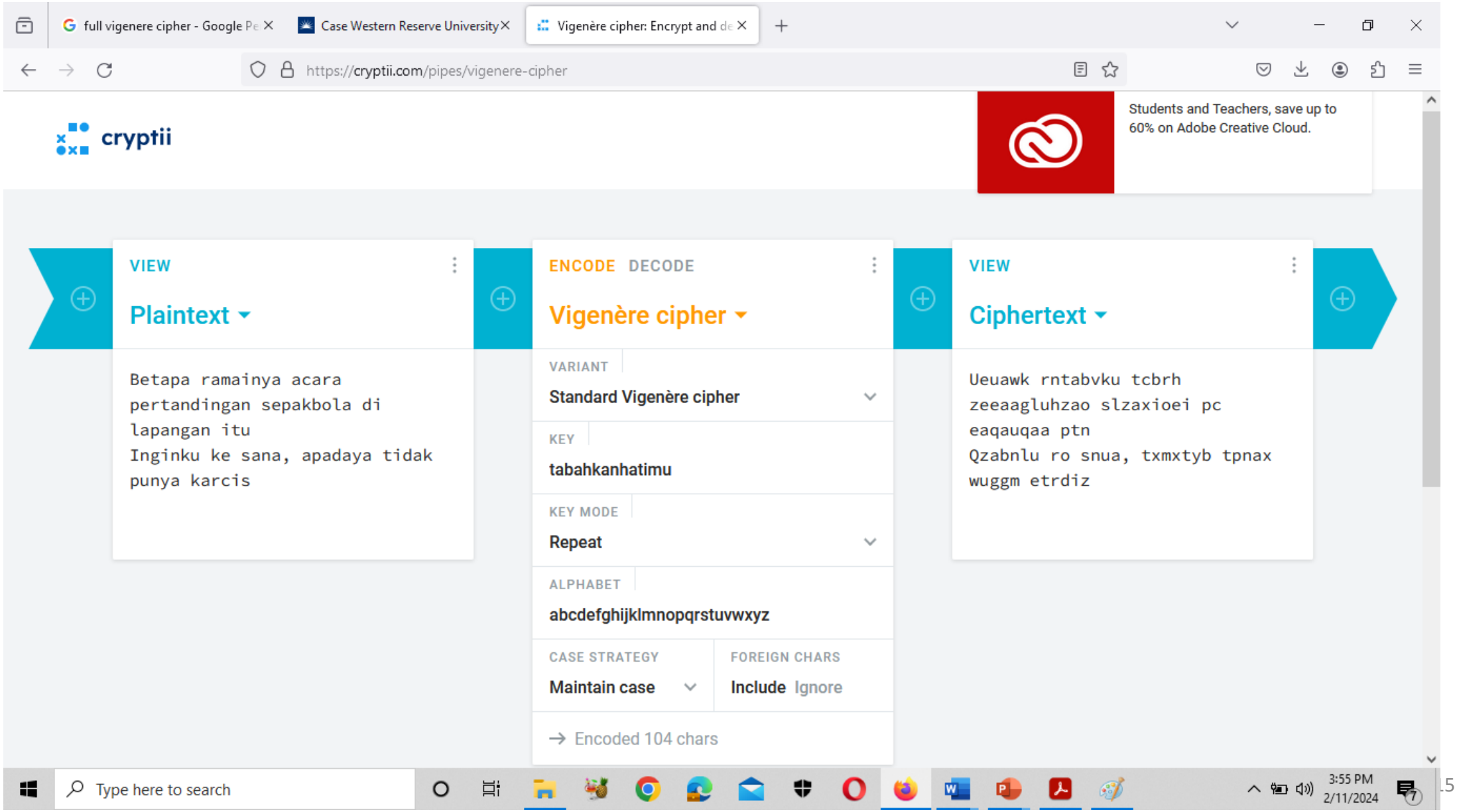
Kunci: selatsunda

Cipherteks:

(dikelompokkan 4-huruf)

```
VMYAL HYAGI VMVAG CIGDT WVYAM WGRPI FXLKX HUQDP ALLKL
WEBOA ZHLNH JUAJT MEDIL OUHQT MOUEG BUAJP WROIW AENQS
VHLNL EJFHK GXLTX JHNWE MREUD EYYDR SRRPT JUFLS OEXEF
TUJDP WVXAB FUAOA LSWAM GSNQG KIOAG YNEHN AXFKX KYXRL
SLVAK WHNDK SRXEG YANQG YYVEZ AUGDN TIWAC SLZHN YEUAK
QUAJD ARTLT AVRUB SLLYT KYULN YKLMX FANQT AWTPT KCXHC
WPLKT SHODG AEYAD VCQDE JESIM M
```

- Demo Vigenere Cipher online: https://cryptii.com/pipes/vigenere-cipher



- *Vigènere Cipher* dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama seperti pada *cipher* abjad-tunggal.

- Sayangnya, Vigenere Cipher sudah tidak aman, karena *cipher* ini sudah berhasil dipecahkan oleh Friedrich Kasiski pada tahun 1863. Metodenya dinamakan metode Kasiski

Friedrich Kasiski
Born: November 29, 1805 @ Schlochau, Kingdom of Prussia
Died: May 22, 1881 (aged 75) @ Neustettin, German Empire
Nationality: German

Varian *Vigenere Cipher*

Untuk mengatasi serangan dengan metode Kasiski, maka dibuat varian Vigenere Cipher sebagai berikut:

1. *Full Vigènere cipher*
   - Setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi merupakan permutasi huruf-huruf alfabet (lihat contoh table pada halaman berikut).
   - Tabel tersebut harus dirahasiakan.

   - Proses enkripsi dan dekripsi tetap sama seperti Vigenere standard:

Contoh sebuah full Vigènere square

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

2. *Auto-Key Vigènere cipher*

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

- Misalnya,

  Pesan: `negara penghasil minyak mentah di dunia`

  Kunci: `INDO`

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

  Plainteks: `negarapenghasilminyakmentahdidunia`

  Kunci: `INDONEGARAPENGHASILMINYAKMENTAHDID`

  Cipherteks: `VRJOEEVEEGWEFOSMAVJMSZCNDMLQBDBQQD`

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: `negarapenghasilminyakmentahdidunia`

  Kunci: `KERAKYATANYANGDIPIMPINOLEHHIKMATPE`

- Selanjutnya enkripsi dan dekripsi dilakukan seperti Vigenere cipher biasa.

Playfair Cipher

- Termasuk ke dalam *polygram cipher*.

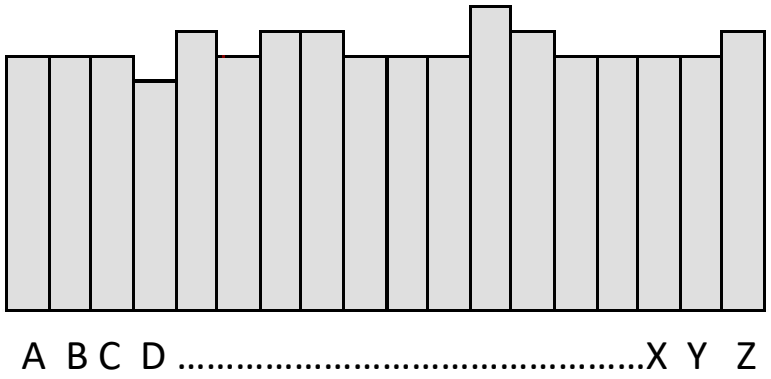
- Ditemukan oleh Sir Charles Wheatstone namun dipromosikan oleh Baron Lyon Playfair pada tahun 1854.

Sir Charles Wheatstone

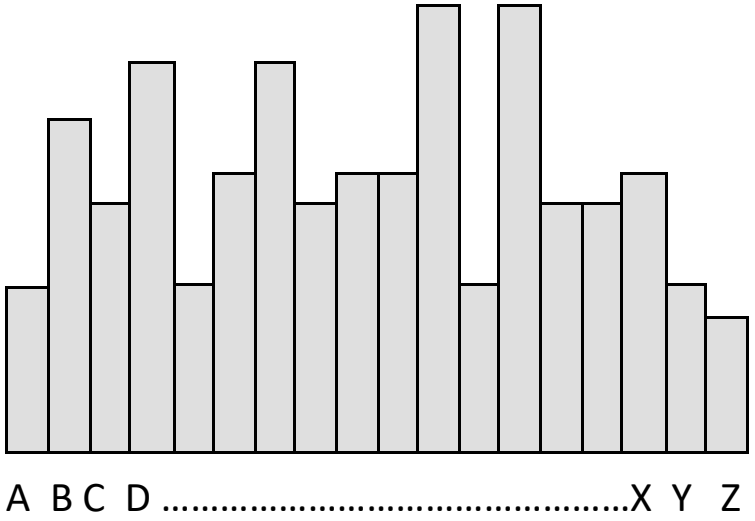
Baron Lyon Playfair

- *Cipher* ini mengenkripsi pasangan huruf (bigram), 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*).



Flat histogram



Bukan flat histogram

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. Buang semua spasi

2. Ganti huruf `j` (bila ada) dengan `i`

3. Tulis pesan dalam pasangan huruf (*bigram*).

4. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan `x` di tengahnya

5. 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 (setelah semua spasi dibuang):

`te mu ii bu na nt im al am`

→ Ada bigram dengan huruf yang berulang (`ii`), sisipkan huruf `x` di tengahnya:

`te mu ix ib un an ti ma la m`

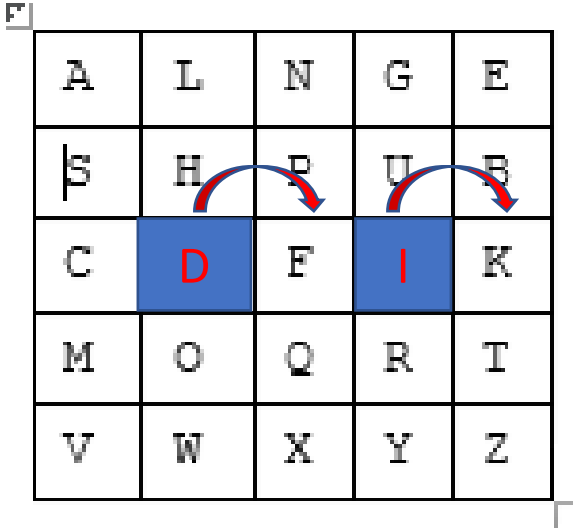
→ Tambahkan huruf `x` jika bigram terakhir hanya satu huruf:

`te mu ix ib un an ti ma la mx`

Algoritma enkripsi:

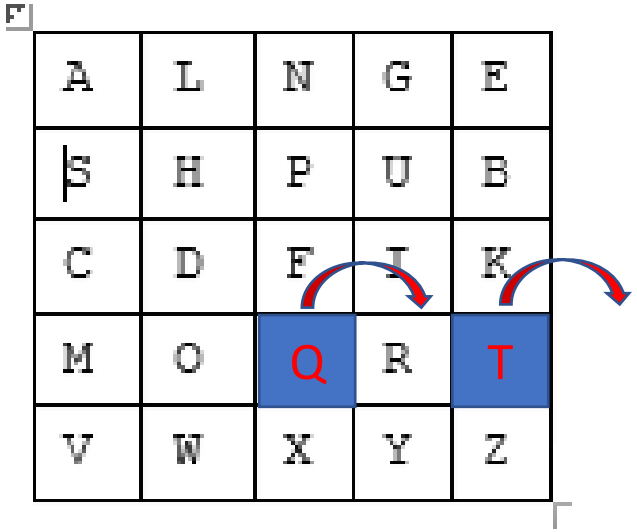
1. Jika dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya (bersifat siklik).

Bigram: di



Cipherteks: FK

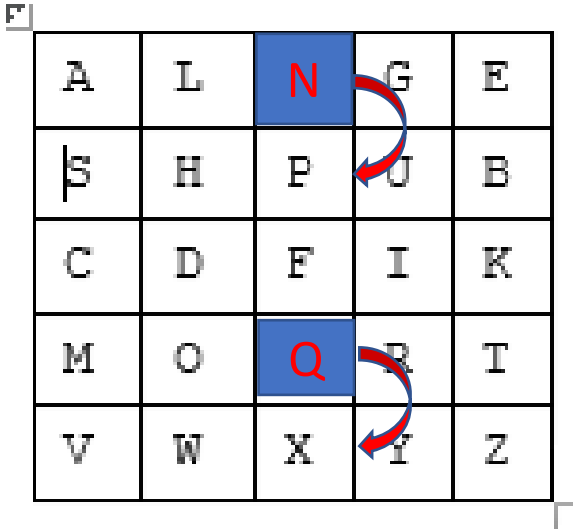
Bigram: qt



Cipherteks: RM

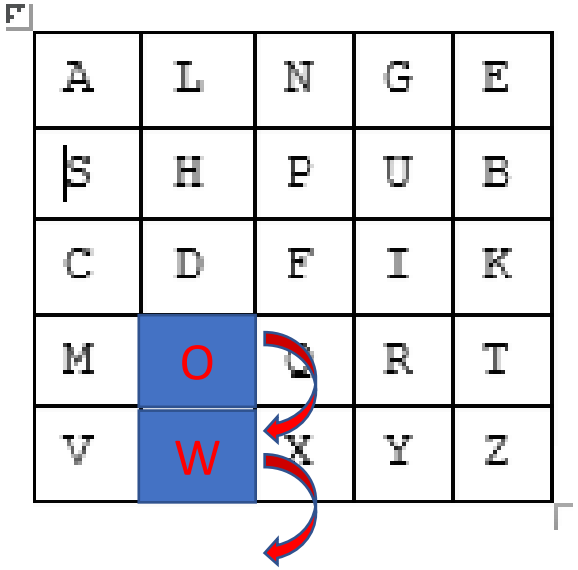
2. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya (bersifat siklik).

Bigram: `nq`



Cipherteks: `PX`

Bigram: `ow`

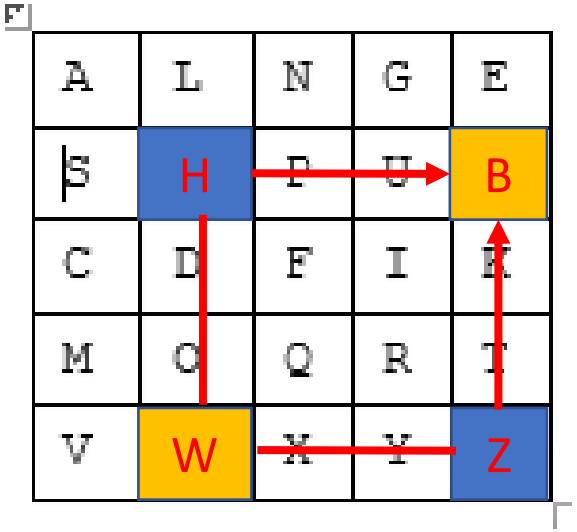


Cipherteks: `WL`

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.

Bigram: `hz`



Cipherteks: `BW`

Plainteks: temui ibu nanti malam

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

Kunci:

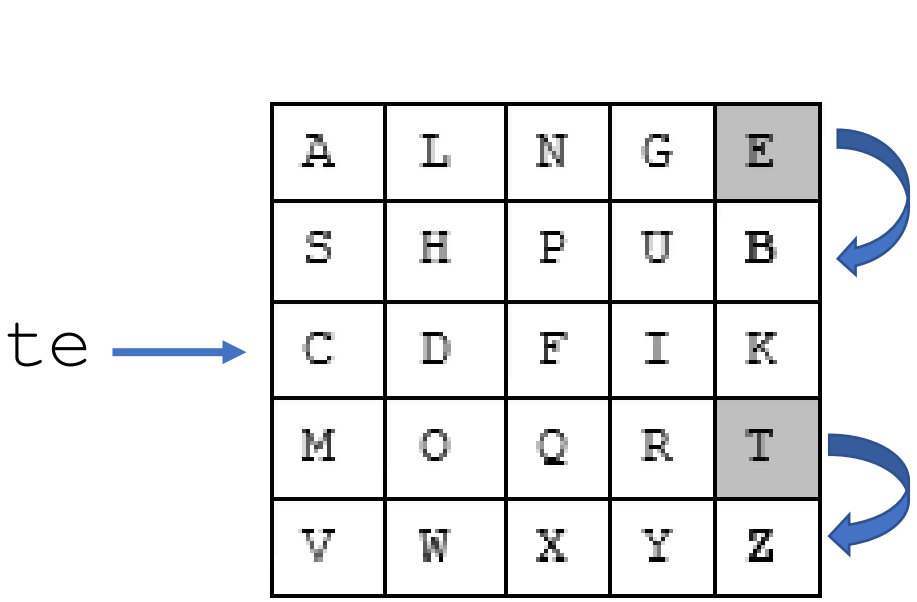
A	L	N	G	E
S	H	P	U	B
C	D	F	I	K
M	O	Q	R	T
V	W	X	Y	Z

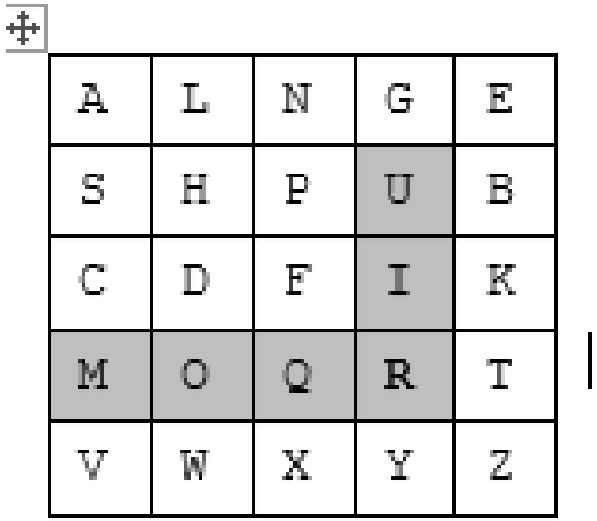
Cipherteks: ZB RS FY KU PG LG RK VS NL QV

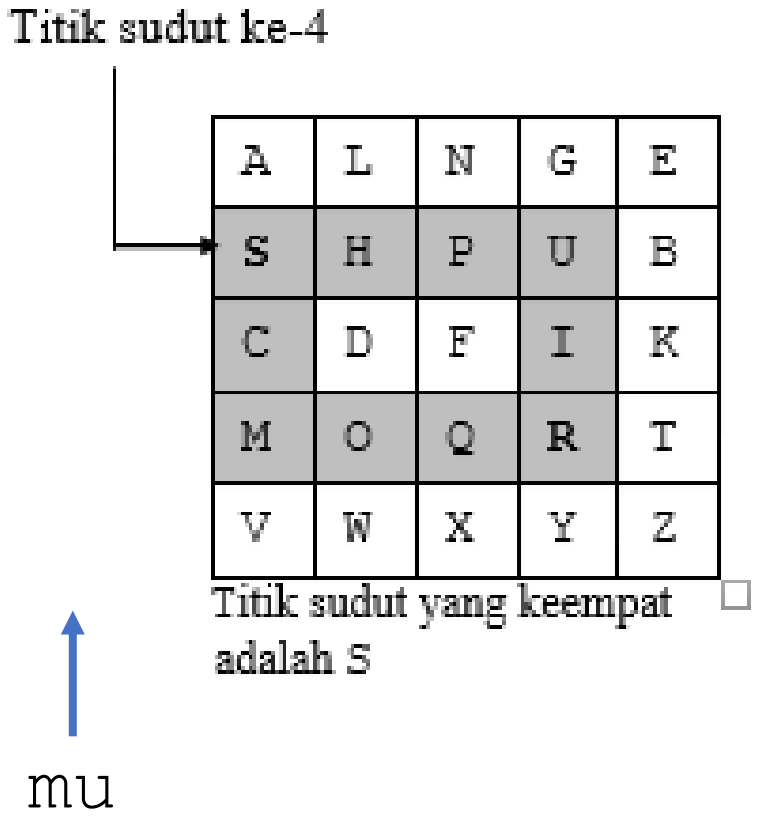
Cara enkripsinya sebagai berkut:

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

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



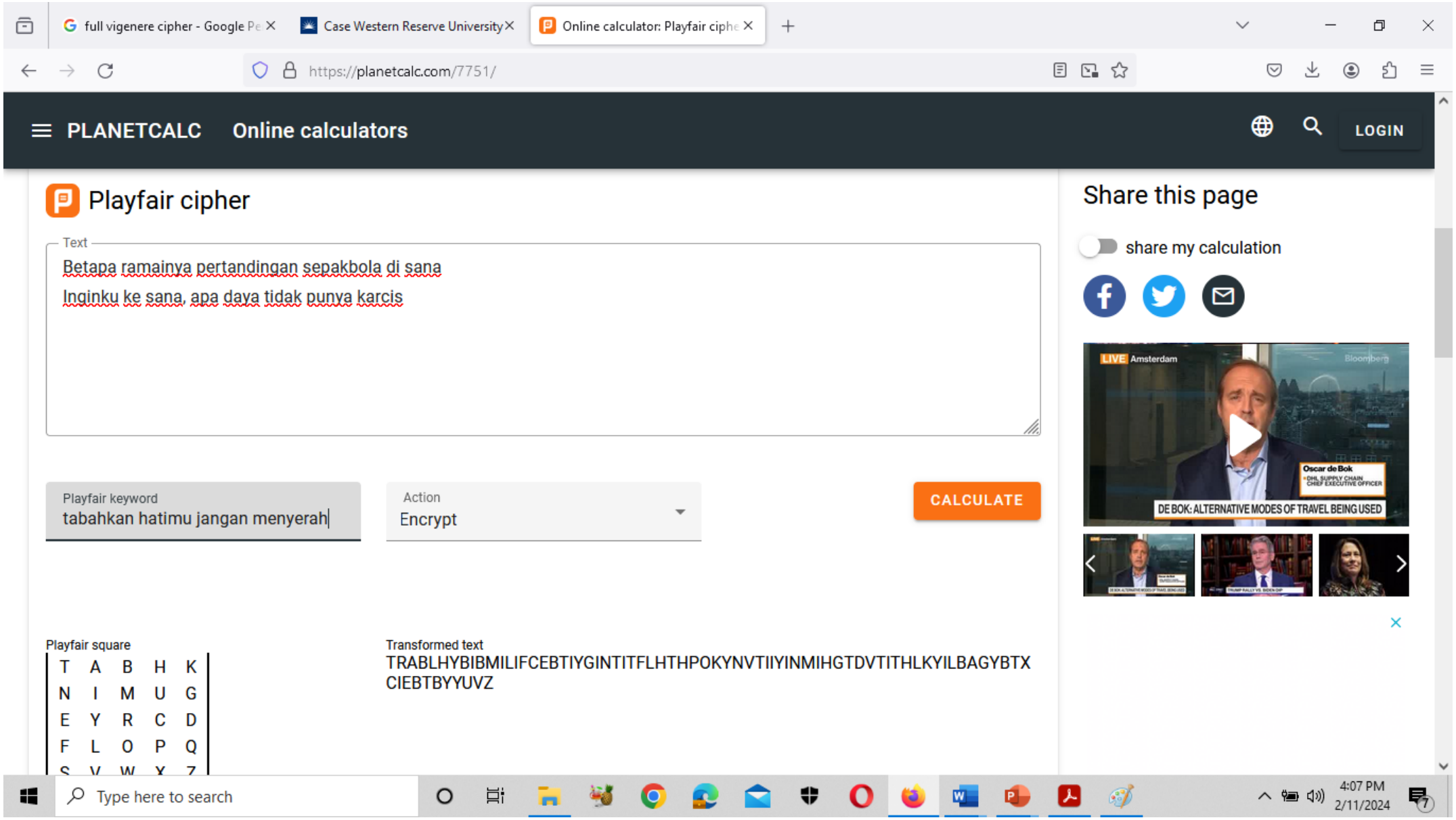




Algoritma dekripsi kebalikan dari algoritma enkripsi. Langkah-langkahnya adalah sebagai berikut:

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.

Demo Playfair cipher online: https://planetcalc.com/7751/



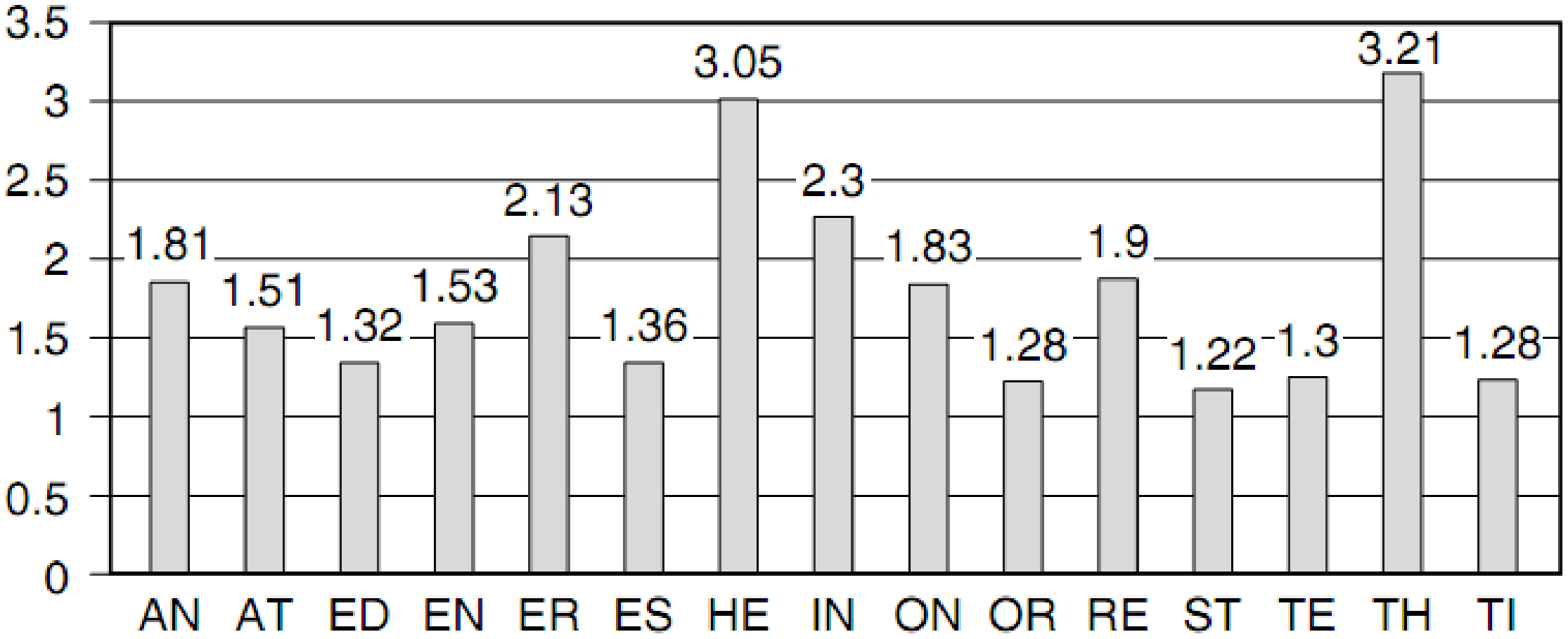
Kriptanalisis Playfair Cipher

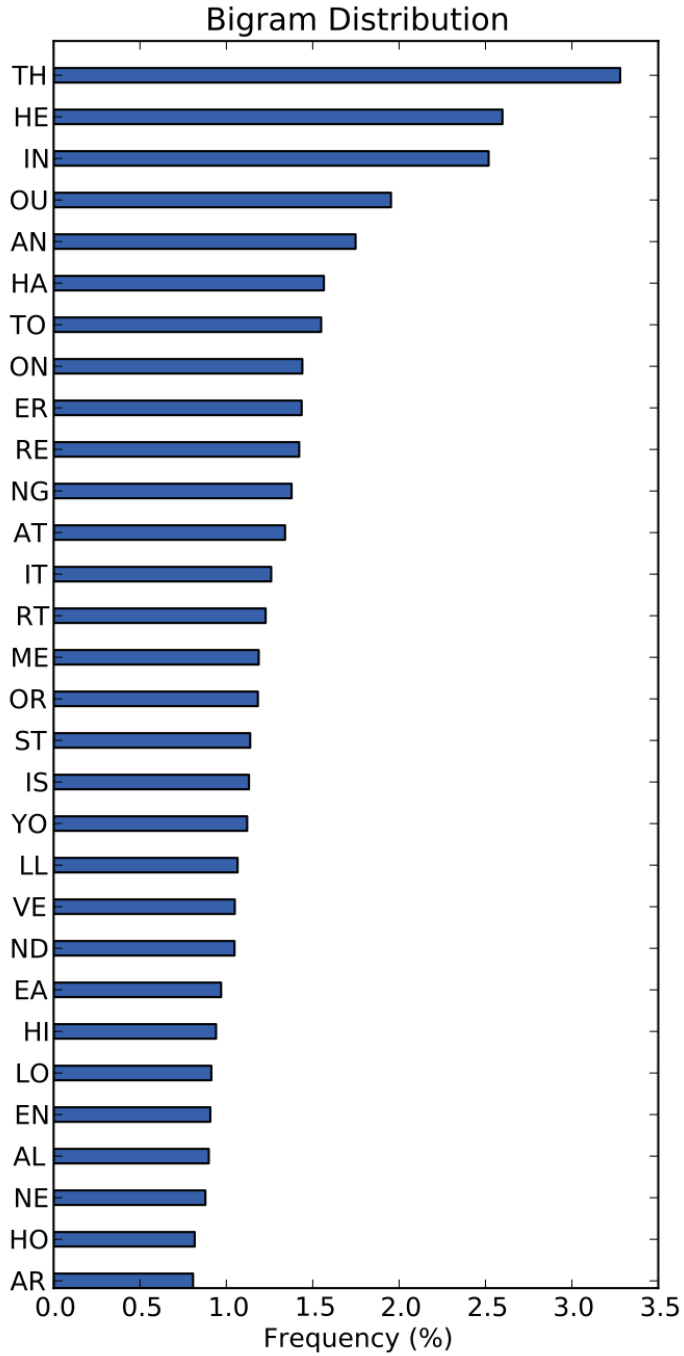
- Karena ada 26 huruf abjad, maka terdapat 26 x 26 = 677 bigram, sehingga identifikasi bigram individual lebih sukar.

- Sayangnya ukuran poligram di dalam *Playfair cipher* tidak cukup besar, hanya dua huruf sehingga *Playfair cipher* tetap 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.


3.5
3
2.5
2
1.5
1
0.5
0
1.81
1.51
1.32
1.53
2.13
1.36
3.05
2.3
1.83
1.28
1.9
1.22
1.3
3.21
1.28
AN
AT
ED
EN
ER
ES
HE
IN
ON
OR
RE
ST
TE
TH
TI

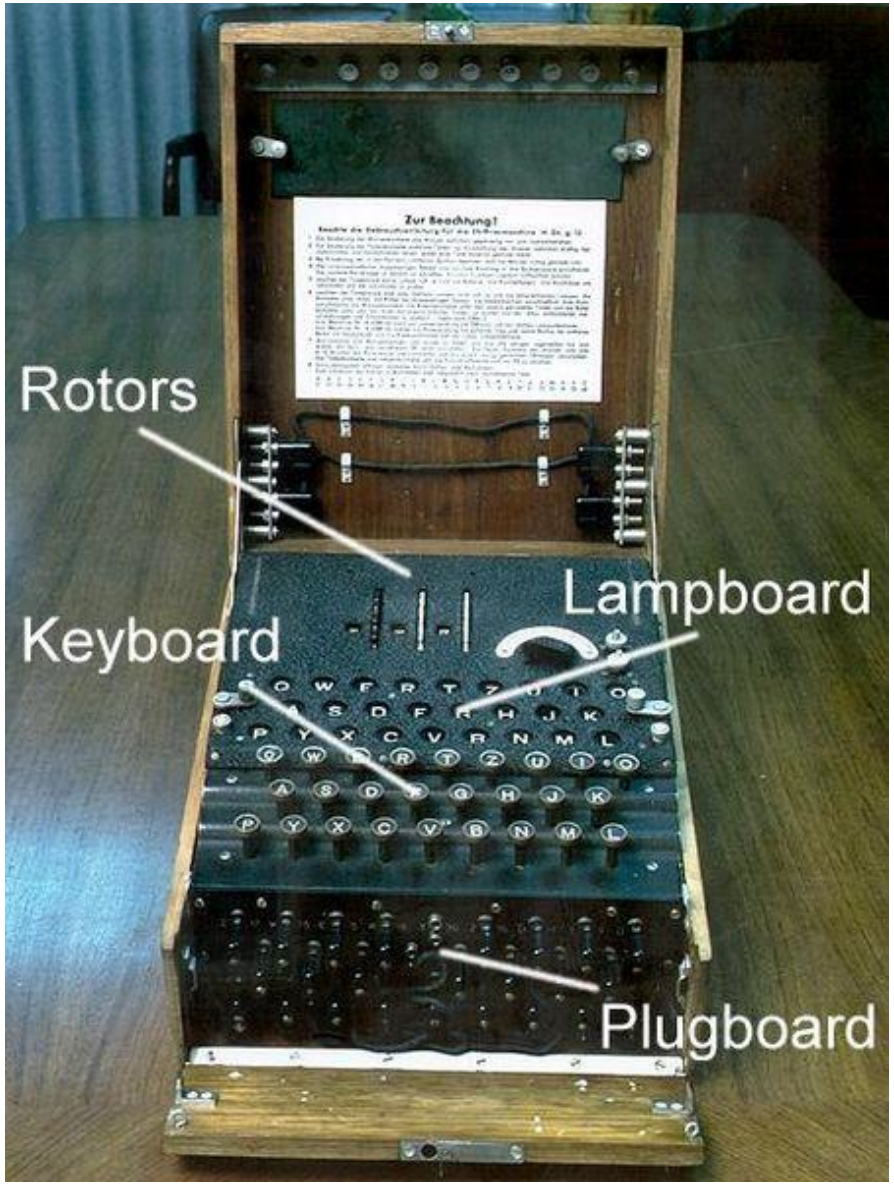

Bigram Distribution
TH
HE
IN
OU
AN
HA
TO
ON
ER
RE
NG
AT
IT
RT
ME
OR
ST
IS
YO
LL
VE
ND
EA
HI
LO
EN
AL
NE
HO
AR
0.0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
Frequency (%)

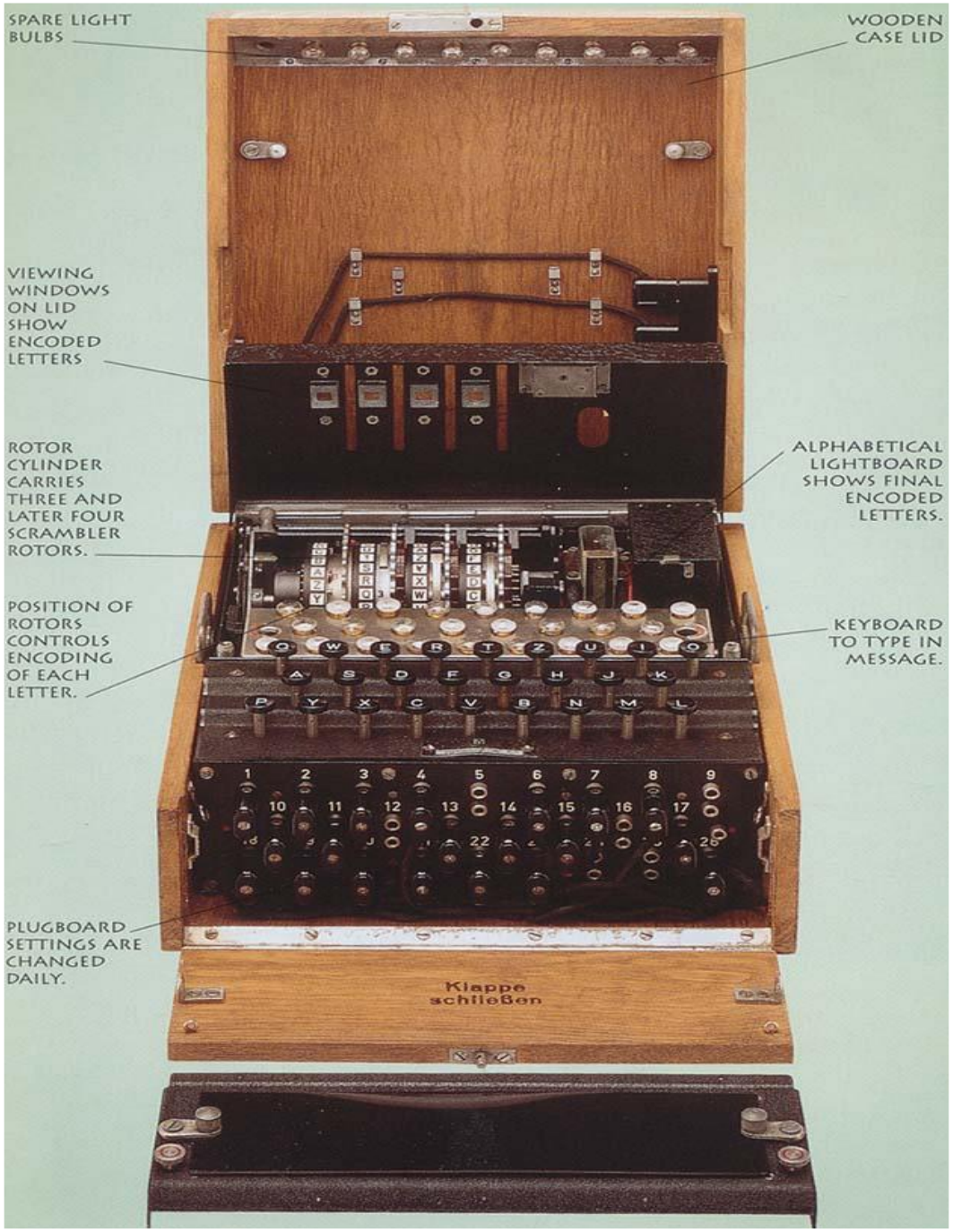
- Dengan menggunakan tabel frekuensi kemunculan pasangan huruf di dalam Bahasa Inggris dan cipherteks yang cukup banyak, *Playfair cipher* dapat dipecahkan.

- Kelemahan lainnya, bigram dan kebalikannya (misal AB dan BA) akan didekripsi menjadi pola huruf plainteks yang sama (misal RE dan ER). Di dalam bahasa Inggris terdapat banyak kata yang mengandung bigram terbalik seperti REceivER dan DEpartED.

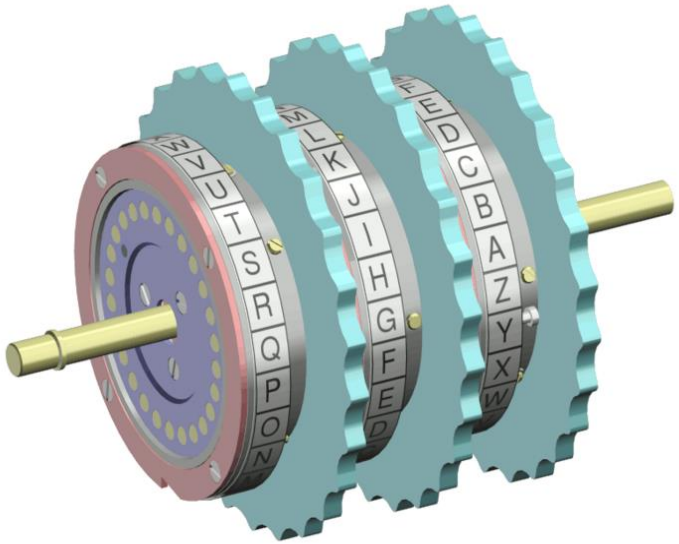
Enigma *Cipher*

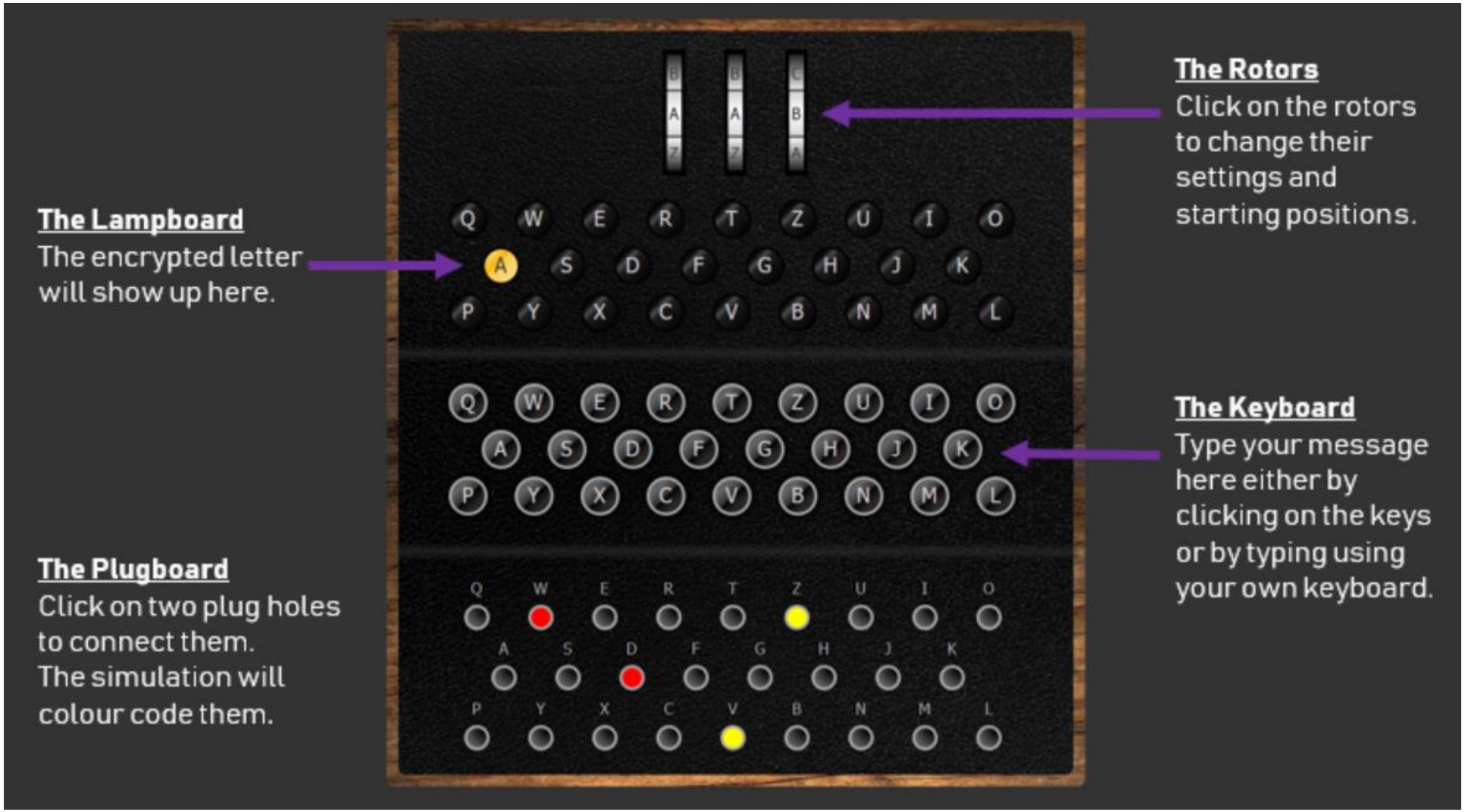
- Enigma adalah mesin enkripsi elektromekanik untuk melakukan enkripsi dan dekripsi.
- Ditemukan dan dipatenkan oleh insinyur Jerman, Arthur Scherbius, untuk tujuan komersil, diplomatik, dan militer
- Menjadi terkenal karena digunakan oleh tantara Nazi Jerman selama Perang Dunia II untuk mengenkripsi/dekripsi pesan-pesan militer.
- Enigma berasal dari bahasa latin, *enigmae*, yang artinya teka-teki.





Enigma Rotors





Sumber gambar: https://www.101computing.net/enigma/enigma-instructions.html

Operator mengetik huruf plainteks pada keyboard, lalu menyalin ulang huruf cipherteks yang menyala pada *lampboard*. Cipherteks dikirim ke penerima pesan

- Enigma menggunakan sistem *rotor* (roda berputar) untuk membentuk huruf cipherteks yang berubah-ubah.

- Setiap rotor melakukan substitusi abjad-tunggal (*monoalphabetic cipher*).

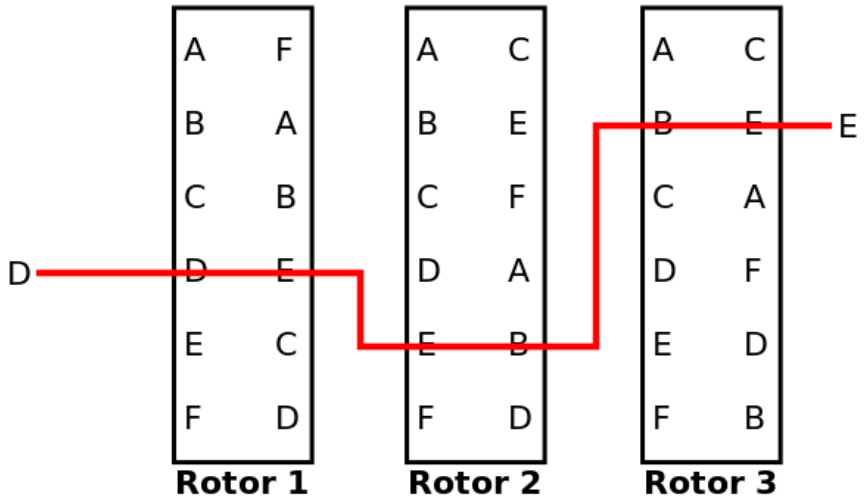
- Hasil substitusi oleh suatu rotor menjadi huruf input untuk operasi substitusi rotor selanjutnya.

- Hasil substitusi oleh rotor terakhir menjadi huruf cipherteks.

- Setiap kali sebuah huruf dienkripsi oleh sebuah rotor, *rotor* berputar satu huruf untuk membentuk huruf cipherteks baru bagi huruf plainteks berikutnya.

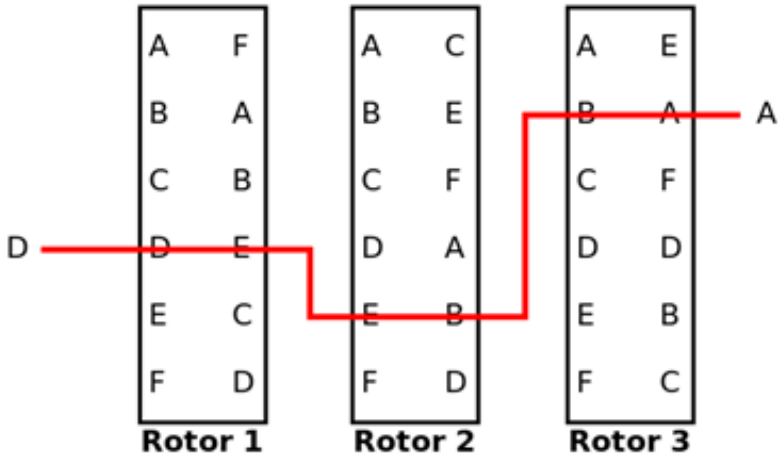
- Setelah berputar 26 huruf rotor kembali pada posisi semula. Jadi, diperoleh cipher abjad-majemuk dengan periode 26.

- Sebagai contoh, tinjau 3 rotor yang disederhanakan menjadi hanya 6 huruf alfabet:



- Misalkan huruf plainteks D ditekan pada keyboard
- Huruf D dienkripsi oleh roto pertama menjadi E
- Huruf E menjadi input untuk rotor kedua, dienkripsi menjadi B
- Huruf B menjadi input untuk rotor ketiga, dienkripsi menjadi E
- Jadi, huruf D dienkripsi menjadi E

- Setelah D dienkripsi menjadi E, rotor ketiga bergeser satu huruf.
- Jika D dienkripsi kembali, maka hasilnya adalah A



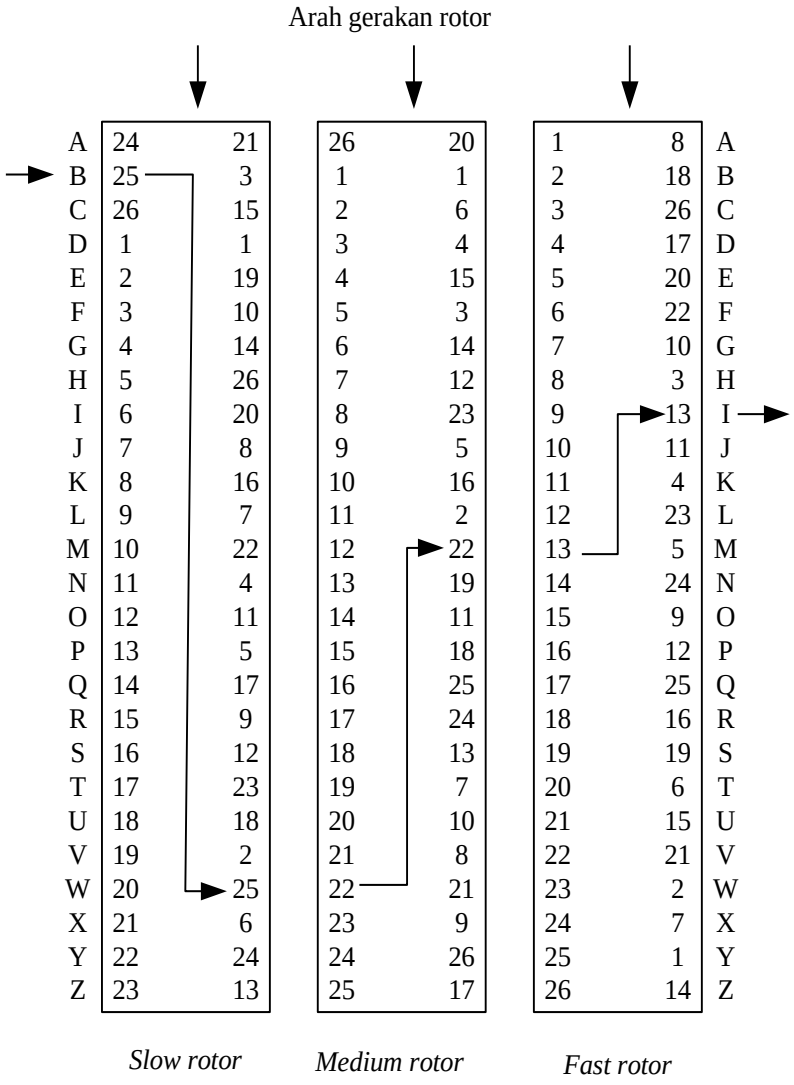
Sumber: https://www.usna.edu/Users/cs/nchamber/courses/ic211/s19/lab/l04/realenigma.html

- Model mesin enigma ada yang menggunakan 3 rotor atau 4 rotor, setiap rotor melakukan operasi substitusi cipher abjad-tunggal.

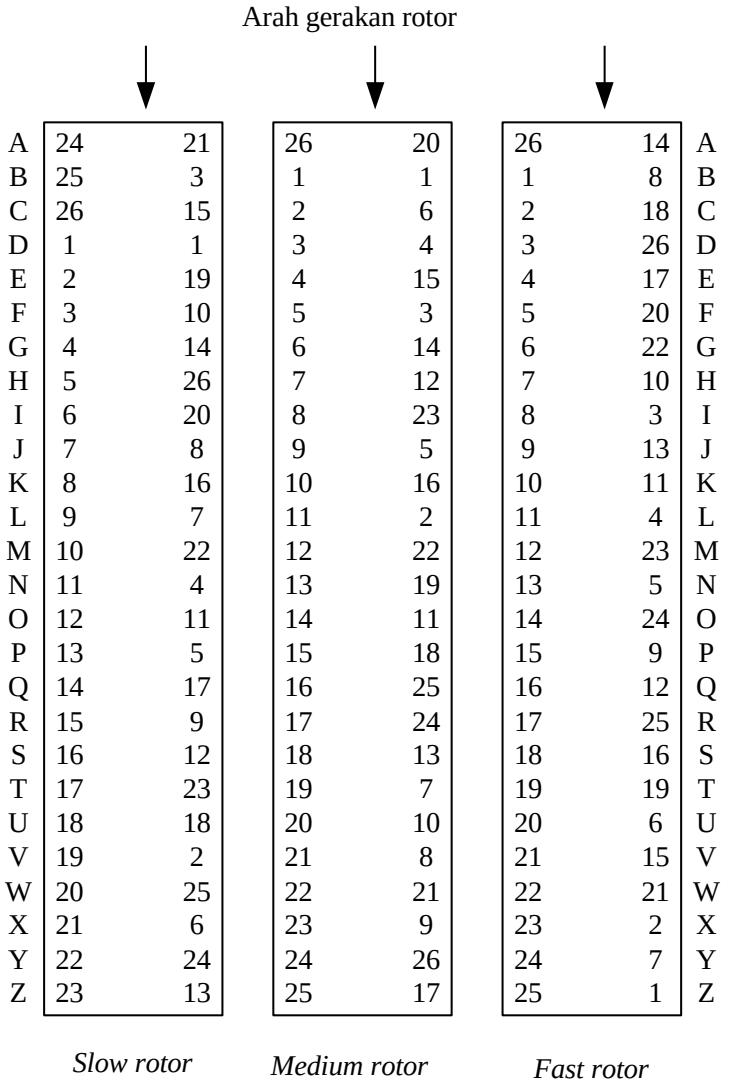
- Untuk mesin enigma 4-rotor, berarti terdapat $26 \times 26 \times 26 \times 26 = 456.976$ kemungkinan huruf cipherteks sebagai pengganti huruf plainteks sebelum terjadi perulangan urutan cipherteks.

- Setiap kali sebuah huruf selesai disubstitusi, *rotor* pertama bergeser satu huruf.

- Setiap kali *rotor* pertama selesai bergeser 26 kali, rotor kedua bergeser satu huruf. Setelah rotor kedua bergeser 26 kali, rotor ketiga bergeser satu huruf. Setelah rotor ketiga bergeser 26 kali, rotor keempat bergeser satu huruf.



(a) Kondisi rotor pada penekanan huruf B. Huruf B menjadi huruf cipherteks I

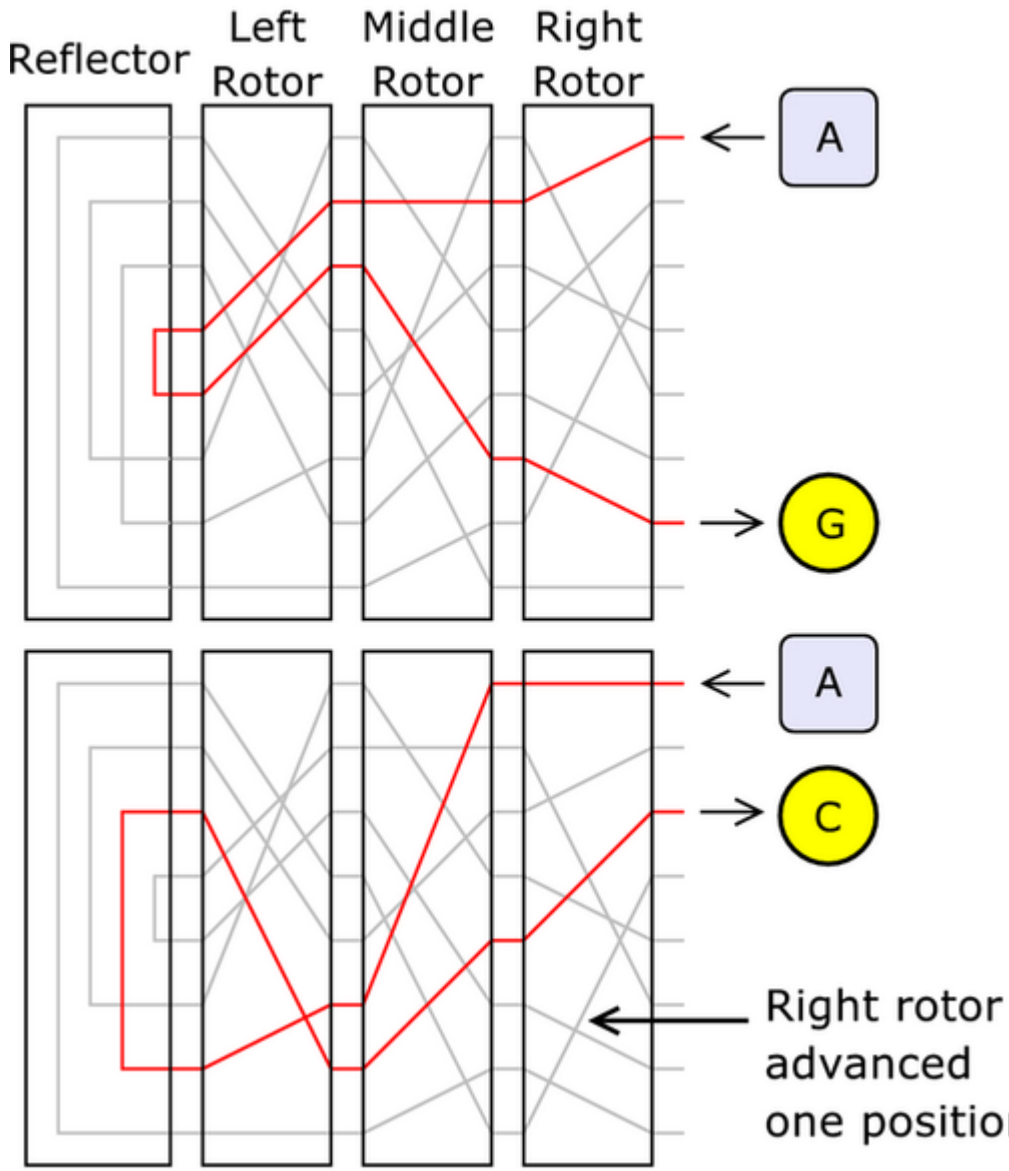


(b) Posisi rotor setelah penekanan huruf B

- Posisi awal keempat *rotor* dapat di-*set*; dan posisi awal ini menyatakan kunci dari Enigma.

- Kriptanalisis mesin Enigma pertama kali ditemukan pada tahun 1932 oleh kriptografer Polandia, yaitu Marian Rejewski, Jerzy Różycki dan Henryk Zygalski.

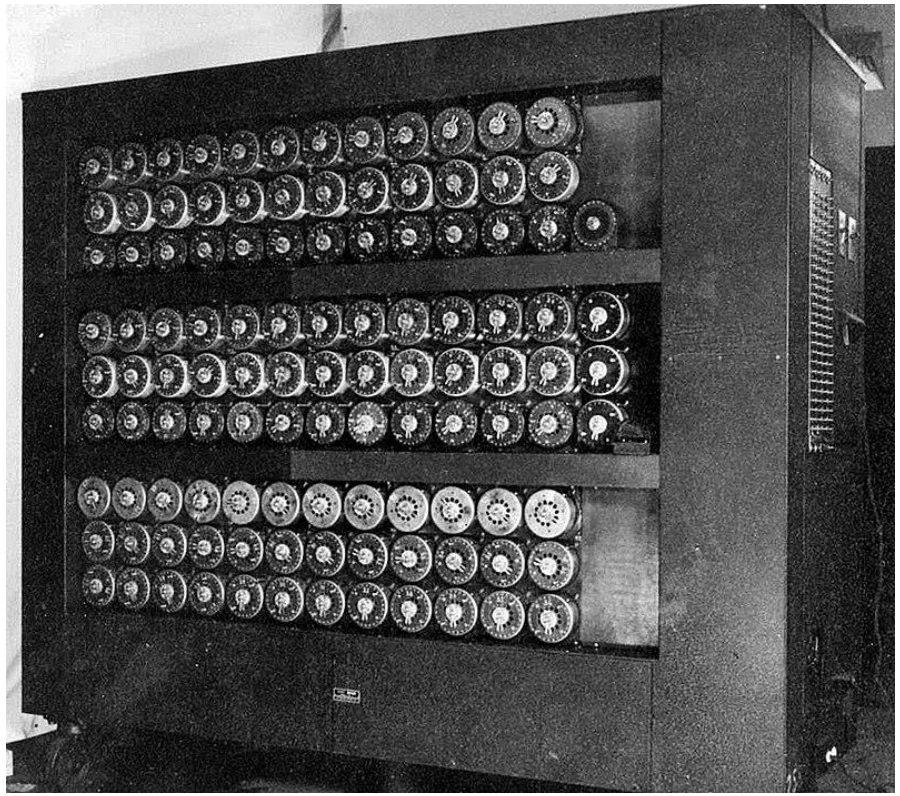
- Pemerintahan Nazi Jerman kemudian mendesain ulang mesin Enigma pada tahun 1939 dengan menambahkan *plugboard* dan *refelector*, sehingga proses enkripsi menjadi lebih kompleks. Metode kriptanalisis Enigma sebelumnya tidak dapat digunakan lagi.



- Jerman sangat percaya diri bahwa Enigma tidak akan dapat dipecahkan.

- Namun, dengan bantuan Polandia, Perancis dan Inggris kemudian membuat mesin pemecah Enigma baru ini, yang diberi nama *bombe*.

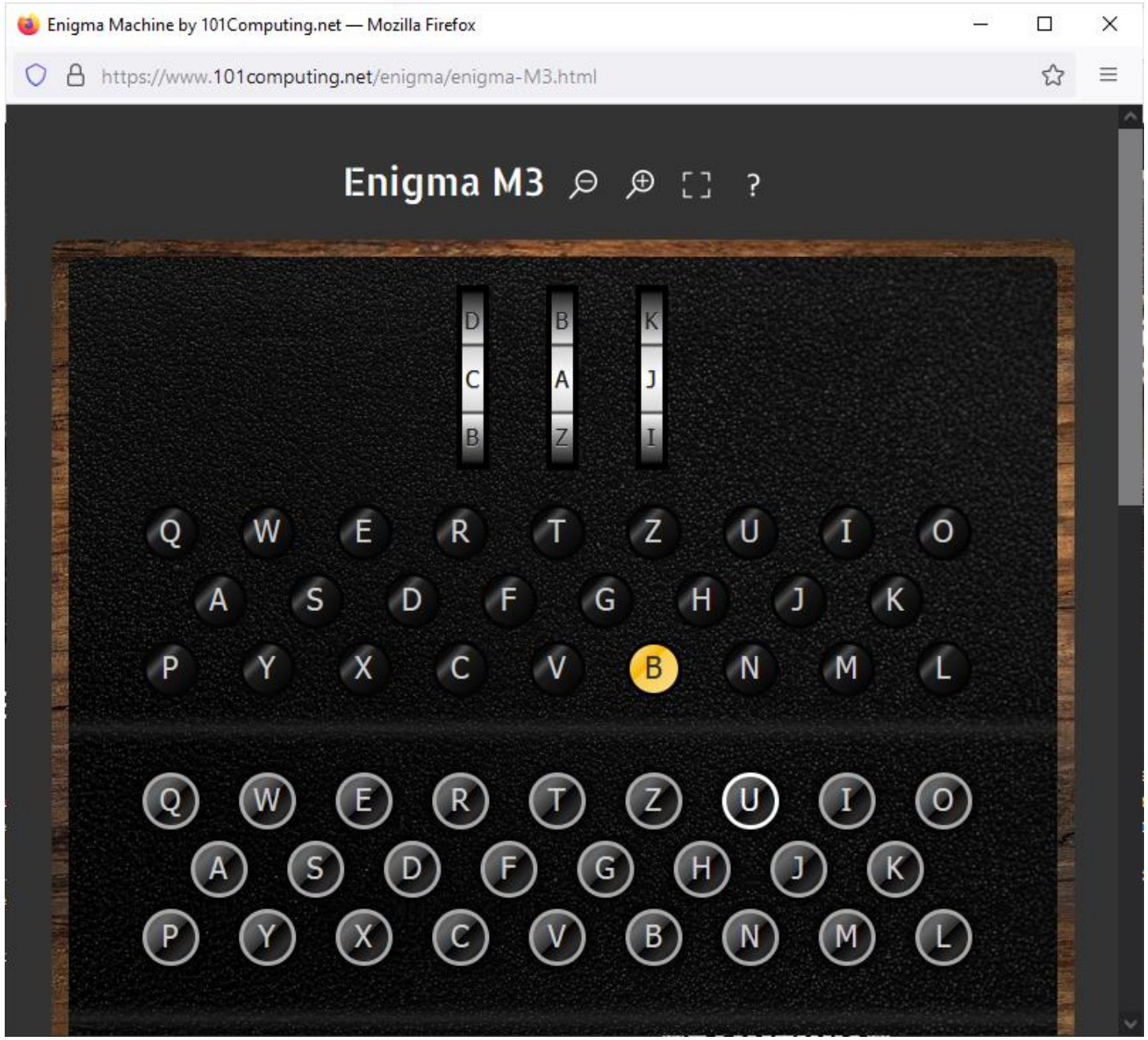
- *Bombe* dirancang oleh Alan Turing.



- *Bombe* berhasil memecahkan Enigma Cipher buatan Jerman.

- Keberhasilan memecahkan Enigma Cipher dianggap sebagai faktor yang memperpendek perang dunia kedua menjadi hanya dua tahun.

Coba simulator online Enimga di: https://www.101computing.net/enigma/enigma-instructions.html


Enigma Machine by 101Computing.net — Mozilla Firefox
https://www.101computing.net/enigma/enigma-M3.html
Enigma M3
D C B
B A Z
K J I
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

Tamat