KRIPTOGRAFI KLASIK

KULIAH KRIPTOGRAFI DAN KEAMANAN JARINGAN

OUTLINE

- **Caesar cipher**
- **Affine cipher**
- **Playfair cipher**
- **Hill cipher**
- **Vigenère cipher**
- **Transposition technique**

KONSEP PENYANDIAN KLASIK

- **Plaintext dipandang sebagai sekuens dari elemen (misalnya berupa bit atau karakter)**
- **Substitution cipher: mengganti setiap elemen pada plaintext dengan elemen yang lain.**
  - Contoh: penyandian Caesar
- **Transposition (permutation) cipher: menyusun kembali urutan elemen-elemen pada plaintext.**
  - Contoh: penyandian transposisi baris
- **Product cipher (super enkripsi): menggunakan beberapa kali substitusi dan transposisi**
  - Juga digunakan dalam kriptografi modern
  - Tujuan: meningkatkan tingkat keamanan

1. SUBSTITUTION CIPHER

- **Penyandian ini memetakan setiap huruf plaintext ke satu atau lebih huruf lainnya.**
- **2 tipe:**
  - monoalphabetic cipher: substitusi tetap ke setiap elemen di dalam alfabet
    - Contoh: Caesar cipher
  - polyalphabetic cipher: setiap huruf plaintext dapat dipetakan ke huruf-huruf yang berbeda, tergantung pada kuncinya.
    - Contoh: Vigenere cipher, Vernam cipher, one-time pad

SHIFT CIPHER DAN CAESAR CIPHER

- **Caesar cipher: mengganti setiap huruf pada alfabet dengan huruf ketiga berikutnya pada alfabet.**
  - Contoh:

    s e c u r e → V H F X U H
  - Secara matematis, petakan huruf ke angka:

    a, b, c, ..., x, y, z

    0, 1, 2, ..., 23, 24, 25
  - Algoritma enkripsi:

    $C = E(3, p) = (p + 3) \bmod 26$
- **Secara umum disebut sebagai shift cipher**
  - Algoritma enkripsi: $C = E(k, p) = (p + k) \bmod 26$
  - Algoritma dekripsi: $p = D(k, C) = (C - k) \bmod 26$

Caesar wheel

- **Brute-force analysis dapat dilakukan dengan mudah:**
  - Algoritma enkripsi dan dekripsi diketahui.
  - Hanya terdapat 25 kunci
  - Bahasa dari plaintext diketahui
    - Perbaikan: penggunaan ZIP sebagai plaintext
- **Perbaikan: suatu kunci (berupa kata) digunakan.**
  - Bagaimana caranya?

1A. MONOALPHABETIC CIPHER

- **Substitusi dengan huruf alfabet yang lain.**
  - Shift cipher merupakan salah satu contoh dari monoalphabetic cipher
- **Petakan setiap huruf plaintext ke huruf ciphertext yang sebenarnya merupakan alfabet dengan urutan random :**

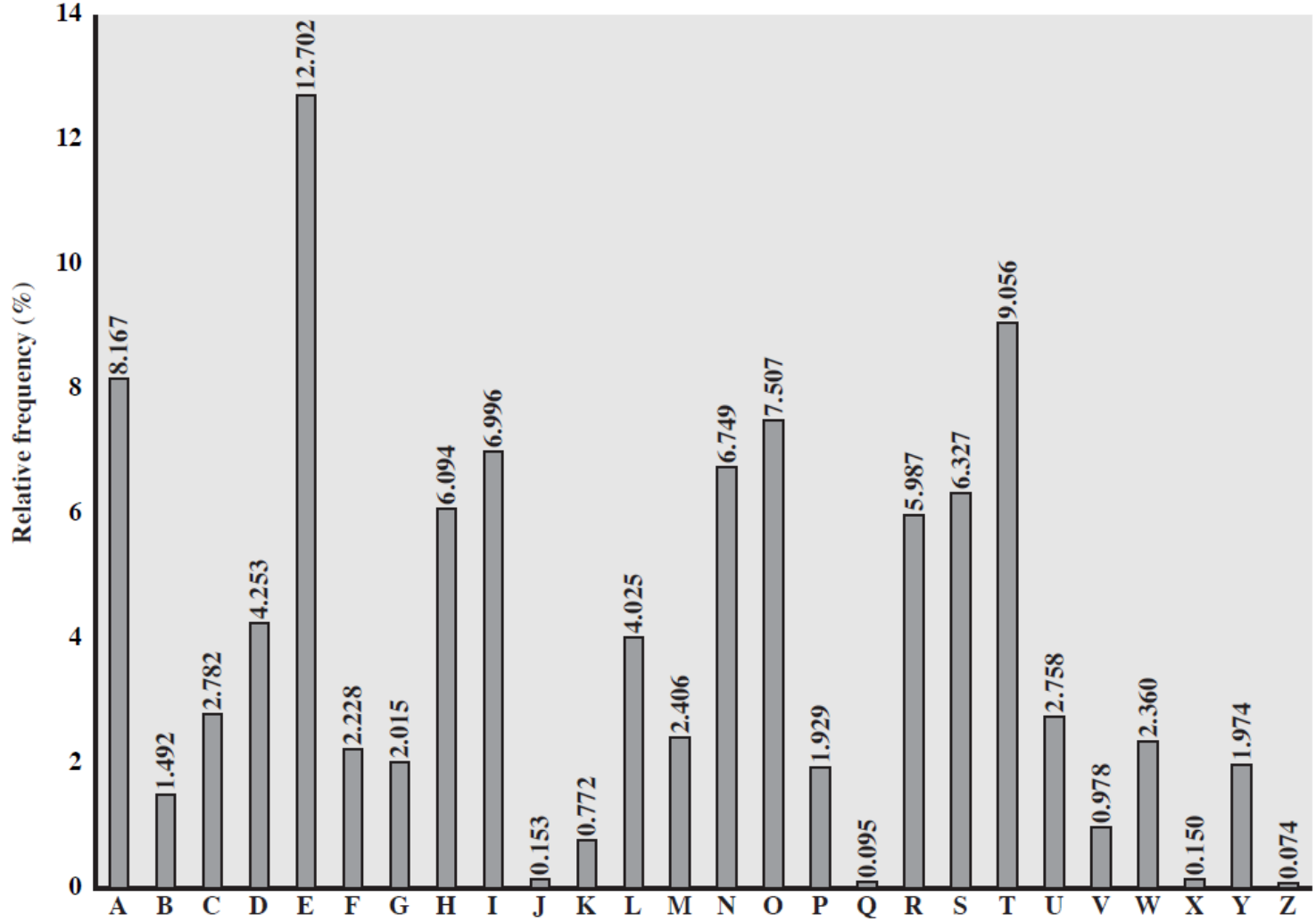
Plain letters: abcdefghijklmnopqrstuvwxyz
Cipher letters: DKVQFIBJWPESCXHTMYAUOLRGZN

- **Akan terdapat 26! Kemungkinan kunci**
- **Masalah: karakteristik bahasa**
- **Dapat dipecahkan dengan analisis frekuensi:**
  - Frekuensi huruf
  - Frekuensi bigram (kombinasi 2 huruf)

STATISTIK BAHASA DAN KRIPTOANALISIS

- **Bahasa manusia tidak random.**
- **Huruf-huruf tidak digunakan dengan frekuensi yang sama.**
- **Dalam bahasa Inggris, E adalah huruf yang paling banyak dipakai, diikuti T, A, O, dst.**
- **Huruf-huruf lain seperti Z, J, K, Q, X jarang digunakan.**
- **Terdapat tabel frekuensi untuk huruf tunggal, ganda, dan triple dari berbagai macam bahasa**

FREKUENSI HURUF BAHASA INGGRIS



- **Statistik untuk huruf ganda dan triple (dari yang paling sering digunakan)**
  - Huruf ganda :

    th he an in er re es on, …
  - Triple letters:

    the and ent ion tio for nde, …

KRIPTOANALISIS UNTUK MONOALPHABETIC CIPHER

- **Monoalphabetic substitution tidak mengubah frekuensi relatif dari huruf-huruf**
- **Untuk melakukan serangan:**
  - Hitung frekuensi huruf pada ciphertext
  - Bandingkan distribusi ini dengan distribusi yang sudah diketahui

CONTOH KRIPTOANALISIS

- **Ciphertext yang diberikan:**

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- **Hitung frekuensi relatif huruf pada ciphertext**

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

- **Tebakan {P, Z} = {e, t}**
- **Dari huruf ganda, ZW memiliki frekuensi tertinggi, maka dapat ditebak ZW = th sehingga ZWP = the**
- **Dengan trial and error, diperoleh:**

  it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

PERBAIKAN UNTUK MONOALPHABETIC CIPHER

- **Penyandian substitusi homofon: 1 huruf dapat diganti dengan sejumlah cipher, dipakai secara bergantian.**
- **Untuk meningkatkan efisiensi:**
  - Multiple letter encryption, misal: playfair cipher

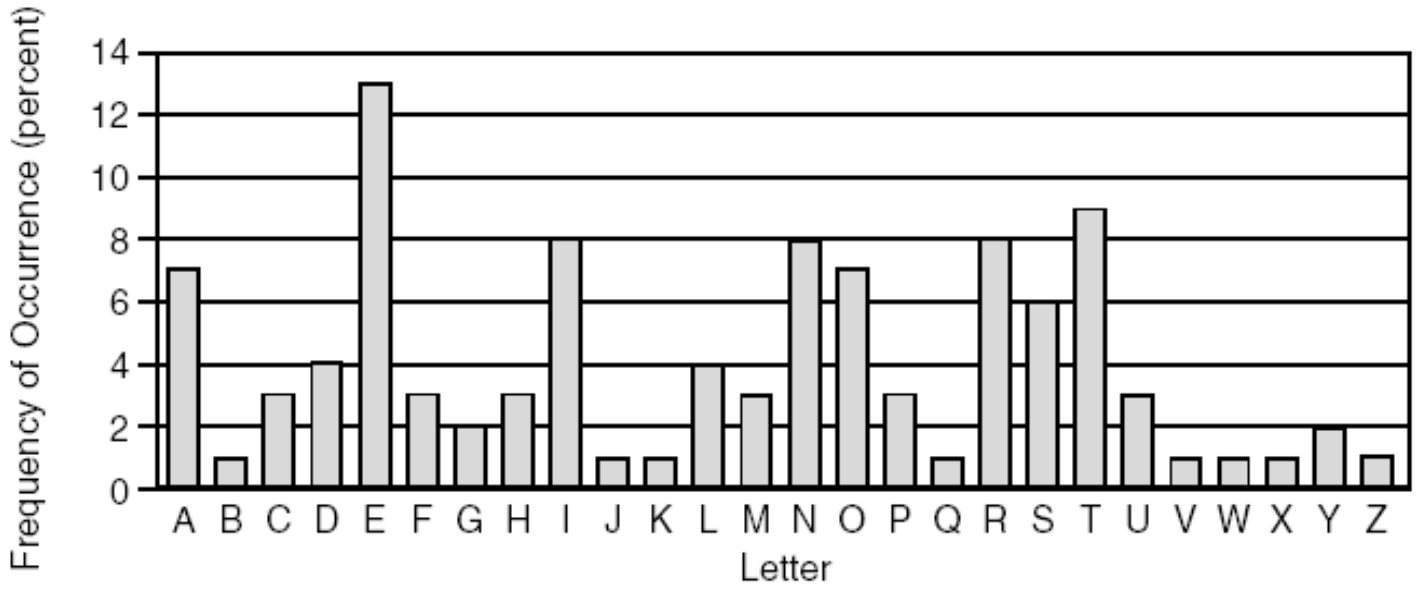
CIPHER SUBSTITUSI HOMOFONIK (*HOMOPHONIC SUBSTITUTION CIPHER*)

- **Merupakan perbaikan dari penyandian monoalfabetik**
- **Setiap huruf plainteks dipetakan ke dalam salah satu huruf atau pasangan huruf ciphertext yang mungkin.**
- **Tujuan: menyembunyikan hubungan statistik antara plainteks dengan cipherteks**
- **Fungsi *ciphering* memetakan satu-ke-banyak (*one-to-many*).**

Misal: huruf `E` → `AB`, `TQ`, `YT`, `UX` (homofon)

huruf `B` → `EK`, `MF`, `KY` (homofon)

- **Contoh: Sebuah teks dengan frekuensi kemunculan huruf sbb:**



- **Huruf E muncul 13 % → dikodekan dengan 13 huruf homofon**

Huruf

Plainteks	**Pilihan untuk unit cipherteks**												
A	BU	CP	AV	AH	BT	BS	CQ						
B	AT												
C	DL	BK	AU										
D	BV	DY	DM	AI									
E	DK	CO	AW	BL	AA	CR	BM	CS	AF	AG	BO	BN	BE
F	BW	CM	CN										
G	DN	BJ											
H	AS	CL	CK										
I	DJ	BI	AX	CJ	AB	BP	CU	CT					
J	BX												
K	DI												
L	AR	BH	CI	AJ									
M	DH	BG	AY										
N	BY	DG	DF	CH	AC	BR	DU	DT					
O	DZ	BF	DX	AK	CG	BQ	DR						
P	BZ	DE	AZ										
Q	DD												
R	AQ	DC	DQ	AL	CE	CF	CV	DS					
S	AP	AN	AO	CD	DW	DV							
T	CB	DB	DP	CC	AD	CY	CW	CX	AE				
U	CA	AM	BA										
V	BB												
W	CZ												
X	BD												
Y	DO	DA											
Z	BC												

- **Unit ciphertext mana yang dipilih di antara semua homofon ditentukan secara acak.**
- **Contoh:**

  Plainteks: `KRIPTO`

  Cipherteks: `DI CE AX AZ CC DX`

- **Enkripsi: satu-ke-banyak**
- **Dekripsi: satu-ke-satu**
- **Dekripsi menggunakan tabel homofon yang sama.**

AFFINE CIPHER

- **Merupakan bentuk khusus dari substitution cipher**
- **Menggunakan affine function:**

  $f(x) = (ax + b) \bmod 26$, di mana $a, b \in Z_{26}$

  Catatan: jika a = 1, akan menjadi shift cipher
- **Agar dekripsi bisa dilakukan, f(x) harus merupakan fungsi injektif. Ini dipenuhi jika a relatif prima terhadap 26.**
- **Affine cipher:**
  - Enkripsi: $C = E(P) = (aP + b) \bmod 26$, di mana $a, b \in Z_{26}$, dan $fpb(a, 26) = 1$
    - P adalah urutan huruf plaintext pada alfabet, C adalah urutan dari huruf ciphertext di alfabet.
  - Dekripsi: $P = E(C) = a^{-1} (C - b) \bmod 26$
    - a^{-1} adalah invers perkalian dari a pada operasi (mod 26).

CIPHER SUBSTITUSI POLIGRAM (POLYGRAM SUBSTITUTION CIPHER)

- **Blok huruf plainteks disubstitusi dengan blok cipherteks.**
- **Misalnya `AS` diganti dengan `RT`, `BY` diganti dengan `SL`**
- **Jika unit huruf plainteks/cipherteks panjangnya 2 huruf, maka ia disebut digram (*bigram*), jika 3 huruf disebut ternari-gram, dst**
- **Tujuannya: distribusi kemunculan poligram menjadi *flat* (datar), dan hal ini menyulitkan analisis frekuensi.**
- **Contoh: Playfair**

PLAYFAIR CIPHER

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

  25!=15.511.210.043.330.985.984.000.000

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

- **Plaintext dienkripsi 2 huruf sekali waktu**

  dengan aturan:

  - Plaintext yang berulang dipisahkan dengan suatu huruf, misal: x
    - balloon → balxloon
  - Jika jumlah huruf ganjil, tambahkan huruf khusus, misal huruf x, di akhir
  - 2 huruf pada baris yang sama diganti dengan huruf berikutnya

    ar → RM
  - 2 huruf pada kolom yang sama diganti dengan huruf di bawahnya

    mu → CM
  - Jika tidak, suatu huruf diganti dengan huruf yang ada pada barisnya dan pada kolum yang sama dengan huruf pasangannya

    hs → BP, ea → IM atau JM
- **Kelemahan: masih menggunakan plaintext.**

- Jumlah kemungkinan kunci:

  25!=15.511.210.043.330.985.984.000.000

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

S	T	A	N	D	S
E	R	C	H	B	E
K	F	G	I/J	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

Contoh:

Plainteks: `GOOD BROOMS SWEEP CLEAN`

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

GO OD BR OX OM SZ SW EZ EP CL EA NX

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 OX OM SZ SW EZ EP CL EA NX

Cipherteks:

FP UT EC PW PO DV TV BV CM BG CS YA

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	

- 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 mendapatkan 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.

HILL CIPHER

- **Menggunakan matriks K berukuran m x m.**
- **Mengambil m huruf sekali waktu untuk dienkripsi.**
- **C = E(K, P) = PK mod 26**
  - C: ciphertext
  - P: plaintext sebanyak m huruf
  - K: matriks kunci berukuran m x m
- **Misal:**
  - Plaintext: 'paymoremoney'
  - K = 17 17 5
    21 18 21
    2 2 19
  - P = (15 0 24)
  - Untuk 3 huruf pertama:
    C =PK mod 26 = (303 303 531) mod 26 = (17 17 11) = RRL
  - C = RRLMWBKASPDH
- **Algoritma dekripsi: $P = D(K, C) = CK^{-1} \bmod 26$**

LATIHAN

1. **Tentukan ciphertext dari 'hari kemerdekaan indonesia' menggunakan metode Caesar cipher dengan kata kunci "security".**
2. **Bangunlah penyandian affine dan lakukan enkripsi untuk kata "enkripsi".**
3. **Buatlah matriks Playfair dengan kunci 'largest'. Enkripsi pesan 'The enemy must be stopped at all cost' dengan matriks tersebut.**
4. **Enkripsi pesan 'meet me at the usual place' dengan algoritma Hill cipher menggunakan key: 9 4**

   5 7

1B. CIPHER ABJAD-MAJEMUK (POLYALPABETIC SUBSTITUTION CIPHER)

- ***Cipher* abjad-tunggal: satu kunci untuk semua huruf plainteks**
- ***Cipher* abjad-majemuk: setiap huruf menggunakan kunci berbeda → Setiap huruf plaintext memiliki beberapa huruf ciphertext.**
- ***Cipher* abjad-majemuk dibuat dari sejumlah *cipher* abjad-tunggal, masing-masing dengan kunci yang berbeda.**
  - Sekuens dari monoalphabetic ciphers (M_1, M_2, M_3, ..., M_k) digunakan bergantian untuk mengenkripsi.
  - Kunci menentukan sekuens mana yang digunakan.
- **Contoh: Vigenere cipher, Vernam cipher, one-time pad**
- **Kriptoanalisis lebih sulit karena distribusi frekuensi tidak tergambarkan.**

- **Plainteks:**

$$P = p_1 p_2 \cdots p_m p_{m+1} \cdots p_{2m} \cdots$$

- **Cipherteks:**

$$E_k(P) = f_1(p_1)\, f_2(p_2) \cdots f_m(p_m)\, f_{m+1}(p_{m+1}) \cdots f_{2m}(p_{2m}) \cdots$$

- **Untuk $m = 1$, *cipher*-nya ekivalen dengan *cipher* abjad-tunggal.**

Contoh: (spasi dibuang)

P : KRIPTOGRAFIKLASIKDENGANCIPHERALFABETMAJEMUK

K : LAMPIONLAMPIONLAMPIONLAMPIONLAMPIONLAMPIONL

C : VRUEBCTCARXSZNDIWSMBTLNOXXVRCAXUIPREMMYMAHV

Perhitungan:

(K + L) mod 26 = (10 + 11) mod 26 = 21 = V

(R + A) mod 26 = (17 + 0) mod 26 = 17 = R

(I + M) mod 26 = (8 + 12) mod 26 = 20 = U

dst

Contoh 2: (dengan spasi)

P: SHE SELLS SEA SHELLS BY THE SEASHORE

K: KEY KEYKE YKE YKEYKE YK EYK EYKEYKEY

C: CLC CIJVW QOE QRIJVW ZI XFO WCKWFYVC

VIGÈNERE CIPHER

Termasuk ke dalam *cipher* abjad-majemuk (*polyalpa 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.
- *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 $1 \leq i \leq m$ menyatakan jumlah pergeseran pada huruf ke-*i*.

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

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

VIGENERE CIPHER TANPA MELIHAT TABEL

- **$C = C_0, C_1, \ldots C_{n-1} = E(K, P) = E[(k_0,k_1, \ldots,k_{m-1}), (p_0,p_1, \ldots,p_{n-1})]$ $= (p_0 + k_0)$ mod 26, ….**
- **Contoh:**

  Key : deceptivedeceptivedeceptive

  Plaintext : wearedescoveredsaveyourself

  Ciphertext : ZICVTWQNGRVTWAVZHCQYGLMGJ
- **Rumus enkripsi: $C_i = (p_i + k_{i \bmod m})$ mod 26**
- **Rumus dekripsi: $p_i = (C_i - k_{i \bmod m})$ mod 26**

- 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.

- *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*.

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.

VERNAM CIPHER DAN ONE-TIME PAD

- **Vernam Chiper** : $C_i = p_i$ XOR k_i
  - Lebih cocok untuk data biner
- **One-time pad vigenere cipher:** penggunaan key sepanjang message, sehingga key tidak perlu diulang.
  - Tidak bisa dipecahkan (unconditionally secure encryption).
  - Kelemahan: tidak praktis, masalah distribusi key.

2. CIPHER TRANSPOSISI

- **Cipherteks diperoleh dengan mengubah posisi huruf di dalam plainteks.**
- **Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian huruf di dalam plainteks.**
- **Nama lain untuk metode ini adalah permutasi, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.**

Contoh: Misalkan plainteks adalah

DEPARTEMEN ILMU KOMPUTER

Enkripsi:

DEPART

EMENIL

MUKOMP

UTERYZ

Cipherteks: (baca secara vertikal)

DEMUEMUTPEKEANORRIMYTLPZ

Dekripsi: Kelompokkan cipherteks sepanjang kunci.

(Pada contoh ini, 24 / 6 = 4)

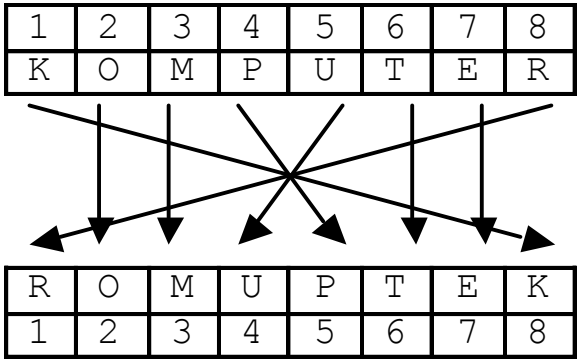
```
DEMU
EMUT
PEKE
ANOR
RIMY
TLPZ
```

Plainteks: (baca secara vertikal)

```
DEPARTEMEN ILMU KOMPUTER YZ
```

Teknik lain:

- **Bagi menjadi blok-blok 8-huruf. Jika < 8, tambahkan huruf palsu.**
- **Ubah susunan hurufnya dengan cara tertentu.**



Teknik lain: rail fence
Misalkan plainteks adalah

```
CRYPTOGRAPHY AND DATA SECURITY
```

Plainteks disusun menjadi 3 baris ($k = 3$) seperti di bawah ini:

```
C       T       A       A       A       E       I
 R   P   O   R   P   Y   N   D   T   S   C   R   T
   Y       G       H       D       A       U       Y
```

maka cipherteksnya adalah

```
CTAAAEIRPORPYNDTSCRTYGHDAUY
```

- **Contoh lain:**
  - Plaintext ditulis secara diagonal .
  - Contoh:

m e m a t r h t g p r y
e t e f e t e o a a t

- **Cara lain: menulis pesan dalam baris-baris, kemudian dibaca dari kolom ke kolom, tetapi tidak terurut.**
  - Urutan kolom menjadi key.
  - Contoh: key : 4 3 1 2 5 6 7
    plaintext : a t t a c k p
    o s t p o n e
    d u n t i l t
    w o a m x y z
    ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
- **Untuk meningkatkan keamanan: dilakukan enkripsi secara berulang.**

SUPER ENKRIPSI

- **Menggabungkan *cipher* substitusi dengan *cipher* transposisi.**
- **Lebih sulit untuk dipecahkan daripada hanya substitusi atau transposisi**
- **Merupakan penghubung antara penyandian klasik dan modern.**
- **Contoh: Plainteks `HELLO WORLD`**
- **Akan dienkripsi dengan *caesar cipher* menjadi `KHOOR ZRUOG`**

  Kemudian hasil enkripsi ini dienkripsi lagi dengan *cipher* transposisi ($k = 4$):

  - `KHOO`
  - `RZRU`
  - `OGZZ`

  Cipherteks akhir adalah: `KROHZGORZOUZ`

STEGANOGRAFI KLASIK

- **Metode untuk menyembunyikan keberadaan pesan.**
- **Contoh:**
  - Menulis surat yang sebenarnya berisi pesan rahasia.
    - Huruf pertama dari kata-kata.
    - Subset dari kata-kata.
- **Macam-macam teknik:**
  - Character marking
  - Invisible ink
  - Typewriter correction ribbon
- **Kelemahan:**
  - Memerlukan usaha lebih besar
  - Ketika dapat dipecahkan, sistem menjadi tidak berguna
- **Keuntungan:**
  - Cocok untuk pihak yang merahasiakan komunikasinya

LATIHAN

1. **Enkripsi kata ‘kriptografi vs kriptoanalisis’ dengan kata kunci ‘enkripsi’ menggunakan Vigenere chiper.**
2. **Enkripsi pesan ‘musuh sedang berada di timur sungai’ dengan metode transposisi, yaitumenulis pesan dalam baris-baris, kemudian dibaca dari kolom ke kolom, tetapi tidak terurut, dengan kunci berturut-turut ‘432165’ dan ‘246531’.**

ROTOR

- **Merupakan penyandian kompleks yang paling banyak digunakan sebelum adanya penyandian modern.**
- **Banyak digunakan dalam Perang Dunia 2.**
- **Menggunakan serangkaian silinder yang dapat diputar.**
- **Mengimplementasikan penyandian substitusi polialfabetik dengan periode K.**
- **Dengan 3 silinder, $K = 26^3 = 17{,}576$.**
- **Dengan 5 silinder, $K = 26^5 = 12 \times 10^6$.**

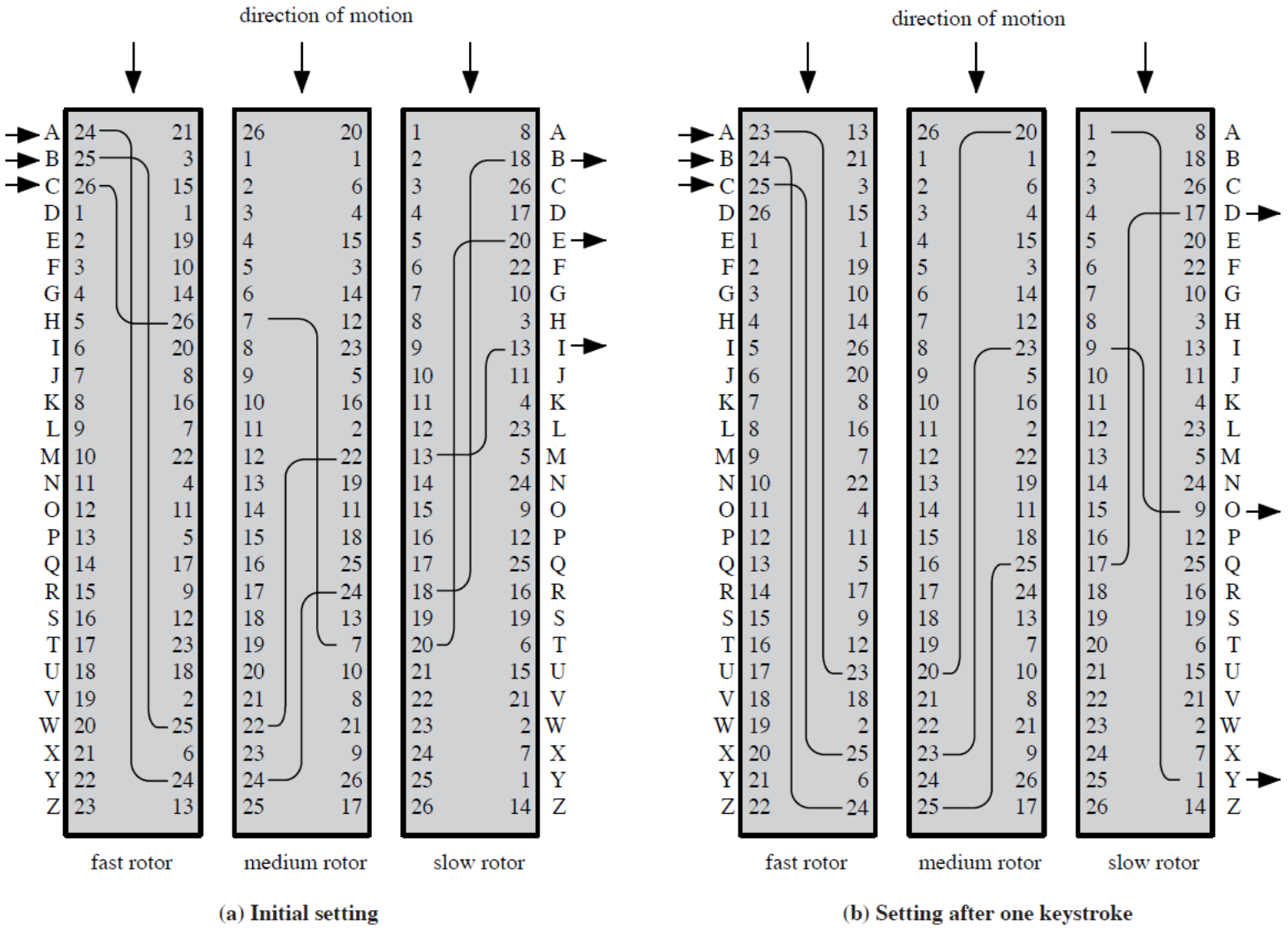


Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts

LEMBAR SETTING RAHASIA JERMAN

Geheim! Secret indeed! This is an example of the setting shee

Geheim!

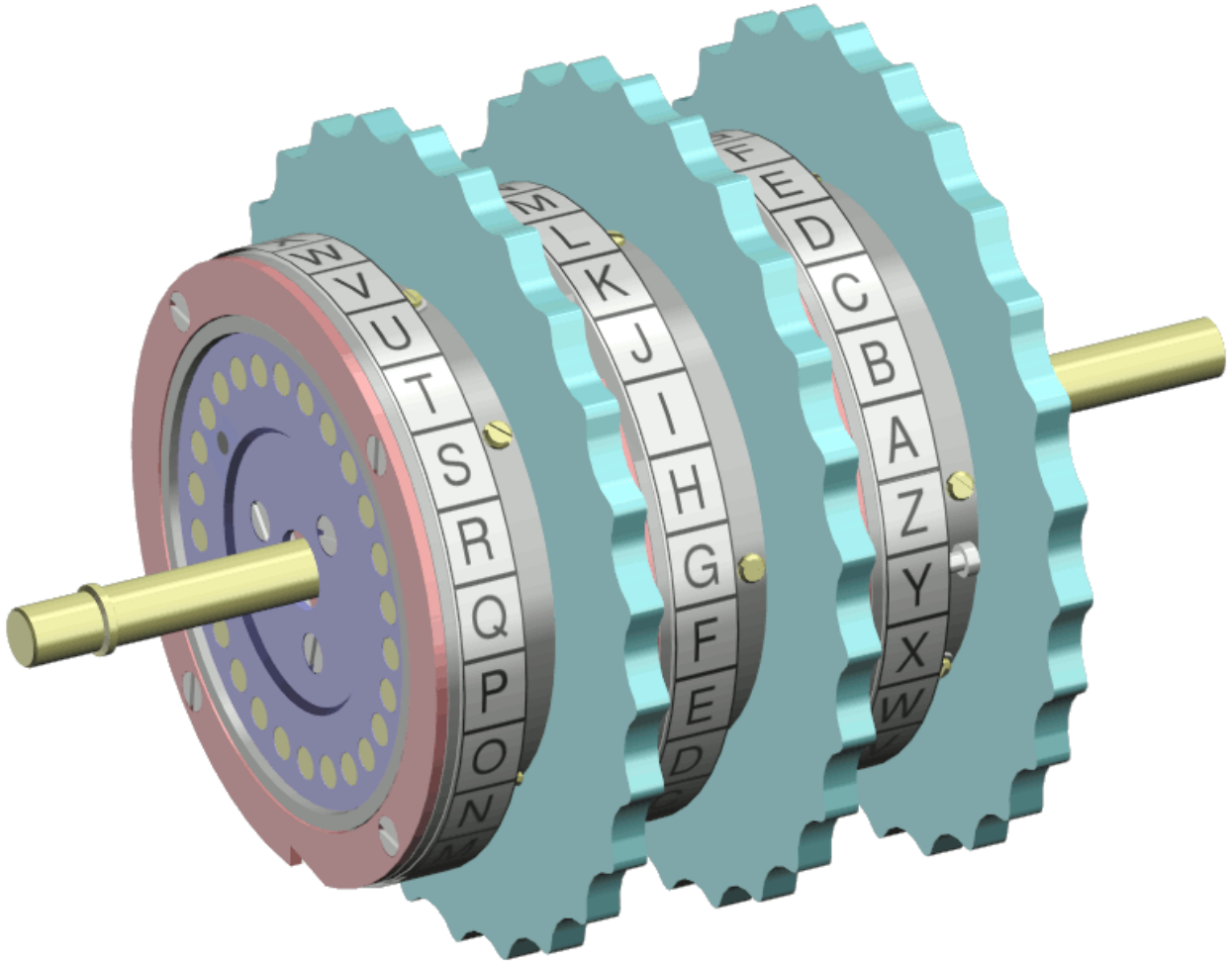
Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen
31.	I V III	06 20 24	UA PF RQ SO NI EY BG HL TX ZJ
30.	V II III	01 07 12	GF KV JM IB UW LX TD QS NA ZH
29.	IV I V	11 17 26	CI OK PV ZL HX NB AW DJ FE ST

Tanggal
Rotor yang mana yang digunakan (ada10 rotor)
Setting ring
SettingpPlugboard

ROTOR



MESIN ROTOR ENIGMA