

Algoritma Kriptografi Klasik (Bagian 1)




Bahan kuliah
IF4020 Kriptografi



Pendahuluan

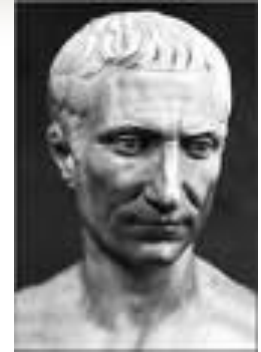
- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Tiga alasan mempelajari algoritma klasik:
 1. Memahami konsep dasar kriptografi.
 2. Dasar algoritma kriptografi modern.
 3. Memahami kelemahan sistem *cipher*.

- 
- Algoritma kriptografi klasik disusun oleh dua teknik dasar:
 1. Teknik substitusi: mengganti huruf plainteks dengan huruf cipherteks.
 2. Teknik transposisi: mengubah susunan/posisi huruf plainteks ke posisi lainnya.

 - Oleh karena itu, dikenal dua macam algoritma kriptografi klasik:
 1. *Cipher* Substitusi (*Substitution Ciphers*)
 2. *Cipher* Transposisi (*Transposition Ciphers*)

Cipher Substitusi

- Contoh: *Caesar Cipher*
- Tiap huruf alfabet digeser 3 huruf ke kanan



p_i : 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
 c_i : 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

- Contoh:
Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX
Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**





■ *Caesar wheel*

- 
- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:

Semula: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

Menjadi: **DZDV LDVW HULA GDQW HPDQ QBAR EHOL A**

- Atau membuang semua spasi:

DZDVL DVWHULAGDQWHPDQQBAREHOLA

- Tujuannya agar kriptanalisis menjadi lebih sulit

- Misalkan, $A = 0,$
 $B = 1,$
 $C = 2,$
...
 $Z = 25$

maka, Caesar Cipher dirumuskan secara matematis:

$$\text{Enkripsi: } c_i = E(p_i) = (p_i + 3) \bmod 26$$

$$\text{Dekripsi: } p_i = D(c_i) = (c_i - 3) \bmod 26$$

Ket: p_i = karakter plainteks ke-i
 c_i = karakter cipherteks ke-i



Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

- $p_1 = 'A' = 0 \rightarrow c_1 = E(0) = (0 + 3) \bmod 26 = 3 = 'D'$
- $p_2 = 'W' = 22 \rightarrow c_2 = E(22) = (22 + 3) \bmod 26 = 25 = 'Z'$
- $p_3 = 'A' = 0 \rightarrow c_3 = E(0) = (0 + 3) \bmod 26 = 3 = 'D'$
- $p_4 = 'S' = 18 \rightarrow c_4 = E(18) = (18 + 3) \bmod 26 = 21 = 'V'$
- $p_5 = 'I' = 8 \rightarrow c_4 = E(8) = (8 + 3) \bmod 26 = 11 = 'L'$
- dst...

Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

ENKRIPSI

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

- $p_1 = 'A' = 0 \rightarrow c_1 = E(0) = (0 + 3) \bmod 26 = 3 = 'D'$
- $p_2 = 'W' = 22 \rightarrow c_2 = E(22) = (22 + 3) \bmod 26 = 25 = 'Z'$
- $p_3 = 'A' = 0 \rightarrow c_3 = E(0) = (0 + 3) \bmod 26 = 3 = 'D'$
- $p_4 = 'S' = 18 \rightarrow c_4 = E(18) = (18 + 3) \bmod 26 = 21 = 'V'$
- $p_5 = 'I' = 8 \rightarrow c_4 = E(8) = (8 + 3) \bmod 26 = 11 = 'L'$
- dst...

Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

DEKRIPSI

Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

- $c_1 = 'D' = 3 \rightarrow p_1 = D(3) = (3 - 3) \bmod 26 = 0 = 'A'$
- $c_2 = 'Z' = 25 \rightarrow p_2 = D(22) = (25 - 3) \bmod 26 = 22 = 'W'$
- $c_3 = 'D' = 3 \rightarrow p_3 = D(3) = (3 - 3) \bmod 26 = 0 = 'A'$
- ...
- $c_{12} = 'A' = 0 \rightarrow p_{12} = D(0) = (0 - 3) \bmod 26 = -3 \bmod 26 = 23 = 'X'$ Keterangan: $-3 \bmod 26$ dihitung dengan cara $|-3| \bmod 26 = 3$, sehingga $-3 \bmod 26 = 26 - 3 = 23$
- **Plainteks:** AWASI ASTERIX DAN TEMANNYA OBELIX

- 
- Jika pergeseran huruf sejauh k , maka:

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 26$

Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 26$

k = kunci rahasia

- Untuk 256 karakter ASCII, maka:

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 256$

Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 256$

k = kunci rahasia



Kelemahan:

Caesar cipher mudah dipecahkan dengan *exhaustive key search* karena jumlah kuncinya sangat sedikit (hanya ada 26 kunci).

Contoh: kriptogram XMZVH

Tabel 1. Contoh *exhaustive key search* terhadap cipherteks XMZVH

Kunci (k) <i>ciphering</i>	'Pesan' hasil dekripsi	Kunci (k) <i>ciphering</i>	'Pesan' hasil dekripsi	Kunci (k) <i>ciphering</i>	'Pesan' hasil dekripsi
0	XMZVH	17	GVIEQ	8	PERNZ
25	YNAWI	16	HWJFR	7	QFSOA
24	ZOBXJ	15	IXKGS	6	RGTPB
23	APCYK	14	JYLHT	5	SHUQC
22	BQDZL	13	KZMIU	4	TIVRD
21	CREAM	12	LANJV	3	UJWSE
20	DSFBN	11	MBOKW	2	VKXTF
19	ETGCO	10	NCPLX	1	WLYUG
18	FUHDP	9	ODQMY		

Plainteks yang potensial adalah CREAM dengan $k = 21$.

Kunci ini digunakan untuk mendekripsikan cipherteks lainnya.

PHHW PH DIWHU WKH WRJD SDUWB

KEY

1 oggv og chvgt vjg vqic rctva

2 nffu nf bgufs uif uphb qbsuz

3 **meet me after the toga party**

4 Ldds ld zesdq sgd snfz ozqsx

5 kccr kc ydrpc rfc rmey nyprw

6 ...

21 ummb um inbmz bpm bwoi xizbg

22 tlla tl hmaly aol avnh whyaf

23 skkz sk glzkx znk zumg vgxze

24 rjjy rj fkyjw ymj ytlf ufwyd

25 qiix qi ejxiv xli xske tevxc

Cipherteks: VIVBQ SQBI SMBMUC LQ ICTI

k	Hasil dekripsi
0	vivbq sqbi smb muc lq icti
1	uhuap rpah rlaltb kp hbsh
2	tgtzo qozg qkzksa jo garg
3	sfsyn pnyf pjyjrz in fzqf
4	rerxm omxe oixiqy hm eyep
5	qdqwl nlwd nhwhpx gl dxod
6	pcpuk mkvc mgvgow fk cwnc
7	obouj ljub lfufnu ej bvmb
8	nanti kita ketemu di aula
9	mzmsj jhsz jdsdlt ch ztkz
10	lylrg igry icrcks bg yszy
11	kxkqf hfqx hbqbjr af xriz
12	jwjpe gepw gapaiq ze wqhw
13	iviod fdov fzozhp yd vpgv
14	huhnc ecnu eynygo xc uofu
15	gtgmb dbmt dxmxfn wb tnet
16	fsfla calc cwlwem va smds
17	erekz bzkr bvkvdn uz rlcw
18	dqdjy ayjq aujuck ty qkbq
19	cpcix zxip ztitbj sx pjap
20	bobhw ywho yshsai rw oizo
21	anagv xvgn xrfqyg pu mgxm
22	xmzfu wufm wqfqyg pu mgxm
23	ylyet vtcl vpepxf ot lfwl
24	xkxds usdk uodowe ns kevk
25	wjwcr trcj tncnvd mr jduj



Contoh: Misalkan kriptogram **HSPPW** menghasilkan dua kemungkinan kunci yang potensial, yaitu:

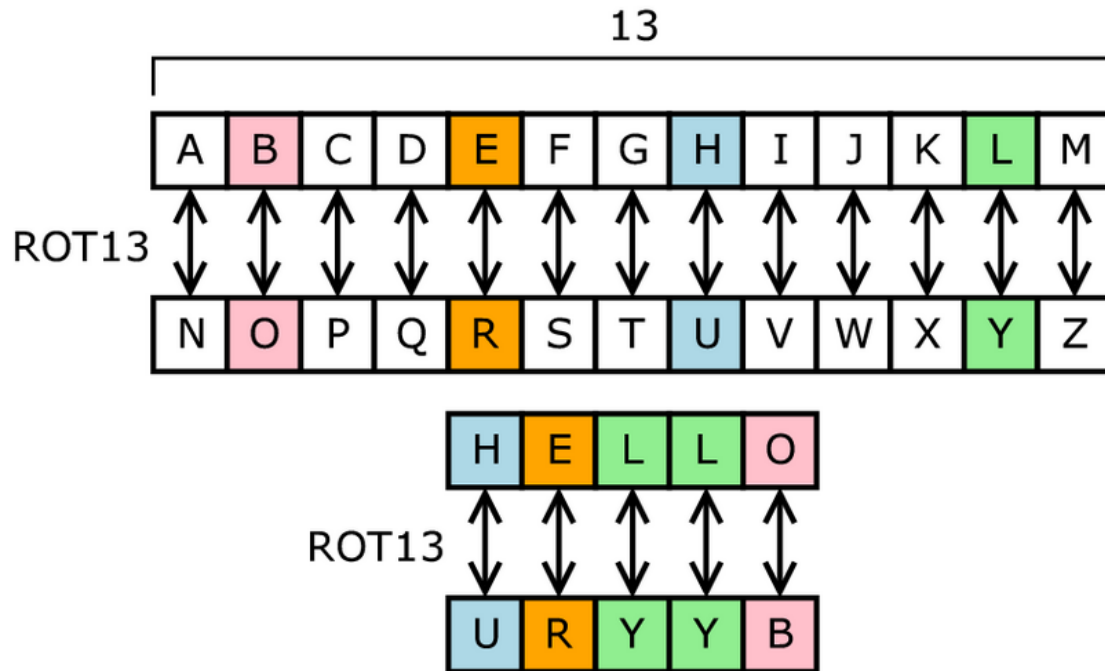
$k = 4$ menghasilkan pesan DOLLS


$k = 11$ menghasilkan WHEEL.

Nilai k mana yang benar?

Jika kasusnya demikian, maka lakukan dekripsi terhadap potongan cipherteks lain tetapi cukup menggunakan $k = 4$ dan $k = 11$ agar dapat disimpulkan kunci yang benar.

- Di dalam sistem operasi Unix, ROT13 adalah fungsi menggunakan *Caesar cipher* dengan pergeseran $k = 13$



- 
- Contoh: ROT13 (ROTATE) = EBGNGR
 - Nama “ROT13” berasal dari *net.jokes*
(<http://groups.google.com/group/net.jokes>) (tahun 1980)
 - ROT13 biasanya digunakan di dalam forum *online* untuk menyandikan jawaban teka-teki, kuis, canda, dsb
 - Enkripsi arsip dua kali dengan ROT13 menghasilkan pesan semula:
$$P = \text{ROT13}(\text{ROT13}(P))$$

sebab
$$\text{ROT}_{13}(\text{ROT}_{13}(x)) = \text{ROT}_{26}(x) = x$$
 - Jadi dekripsi cukup dilakukan dengan mengenkripsi cipherteks kembali dengan ROT13



Jenis-jenis *Cipher* Substitusi

1. ***Cipher* abjad-tunggal** (*monoalphabetic cipher*)
2. ***Cipher* substitusi homofonik** (*Homophonic substitution cipher*)
2. ***Cipher* abjad-majemuk** (*Polyalphabetic substitution cipher*)
3. ***Cipher* substitusi poligram** (*Polygram substitution cipher*)

***Cipher* abjad-tunggal** (*monoalphabetic cipher*)

- Satu huruf di plainteks diganti dengan satu huruf yang bersesuaian.

Contoh: *Caesar Cipher*

- Jumlah kemungkinan susunan huruf-huruf cipherteks yang dapat dibuat pada sembarang *cipher* abjad-tunggal adalah sebanyak

$$26! = 403.291.461.126.605.635.584.000.000$$

- Tabel substitusi dapat dibentuk secara acak:

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

- Atau dengan kalimat yang mudah diingat:

Contoh: we hope you enjoy this book

Buang duplikasi huruf: wehopyunjttisbkc

Sambung dengan huruf lain yang belum ada:

wehopyunjttisbkcacdfglmqrvxz

Tabel substitusi:

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

Cipher Substitusi Homofonik

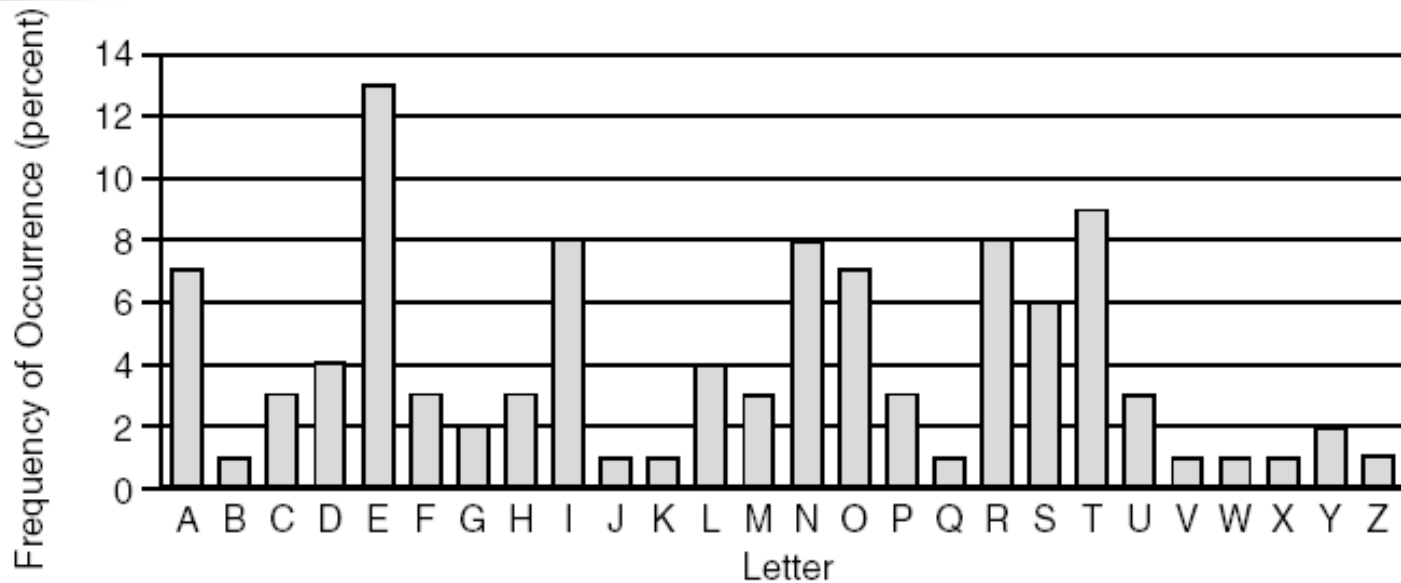
(*Homophonic substitution cipher*)

- Setiap huruf plainteks dipetakan ke dalam salah satu huruf atau pasangan huruf cipherteks 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, TX, YR, MB, OP, TF, QA
B	ER, FY
C	IU, CW, PL
D	NQ, VT, OA, GP
E	ZX, BR, JO, EW, HT, KC, ND, SO, BO, VE, KL, JU, HR
F	EP, MS
G	TW, HL
H	OU, HE, JK, AT, KY, IQ
I	GT, UA, CN, HI, WO, ZF, FI
J	OC
K	LV
L	TY, JO, DR, ML
M	GR, KU
N	BE, TF, XO, LG, PS, CD, IE
O	YA, HU, VS, KP, BD, JZ, OL
P	IR, JA
Q	SP
R	UL, XP, TA, RL, LW, DO
S	EQ, IF, TK, PN, GL, TA
T	SI, GD, KI, MA, EL, ET, MS, MT, TL
U	FA, BI, SF
V	GM
W	TG, AS
X	FI, TM
Y	SR, DS
Z	AR

- 
- Unit cipherteks mana yang dipilih diantara semua homofon ditentukan secara acak.

- Contoh:

Plainteks: K R I P T O

Cipherteks: **DI CE AX AZ CC DX**

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

Cipher Abjad-Majemuk

(*Polyalphabetic substitution cipher*)

- *Cipher* abjad-tunggal: satu kunci untuk semua huruf plainteks
- *Cipher* abjad-majemuk: setiap huruf menggunakan kunci berbeda.
- *Cipher* abjad-majemuk dibuat dari sejumlah *cipher* abjad-tunggal, masing-masing dengan kunci yang berbeda.
- Contoh: Vigenere Cipher (akan dijelaskan pada kuliah selanjutnya)

- 
- 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 ekuivalen dengan *cipher* abjad-tunggal.

Contoh: (spasi dibuang)

P : KRIPTOGRAFIKLASIKDENGANCIPHERALFABETMAJEMUK

K : LAMPIONLAMPIONLAMPIONLAMPIONLAMPIONLAMPIONL

C : **VRUEBCTCARXSZNDIWSMBTLNOXXVRCAXUIPREMMYMAHV**

Perhitungan:

$$(K + L) \bmod 26 = (10 + 11) \bmod 26 = 21 = \mathbf{V}$$

$$(R + A) \bmod 26 = (17 + 0) \bmod 26 = 17 = \mathbf{R}$$

$$(I + M) \bmod 26 = (8 + 12) \bmod 26 = 20 = \mathbf{U}$$

dst

Contoh 2: (dengan spasi)

P: SHE SELLS SEA SHELLS BY THE SEASHORE

K: KEY KEYKE YKE YKEYKE YK EYK EYKEYKEY

C: CLC CIJ VW QOE QRIJ VW ZI XFO WCKWFYVC

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 (*biigram*), jika 3 huruf disebut ternari-gram, dst
- Tujuannya: distribusi kemunculan poligram menjadi *flat* (datar), dan hal ini menyulitkan analisis frekuensi.
- Contoh: Playfair cipher (akan dijelaskan pada kuliah selanjutnya)



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 TEKNIK INFORMATIKA ITB

Enkripsi:

DEPART

EMENTE

KNIKIN

FORMAT

IKAITB

Cipherteks: (baca secara vertikal)

DEKFIEMNOKPEIRAANKMIRTIATTENTB

DEKF IEMN OKPE IRAA NKMI RTIA TTEN TB



Dekripsi: Bagi panjang cipherteks dengan kunci.

(Pada contoh ini, $30 / 6 = 5$)

DEKFI

EMNOK

PEIRA

ANKMI

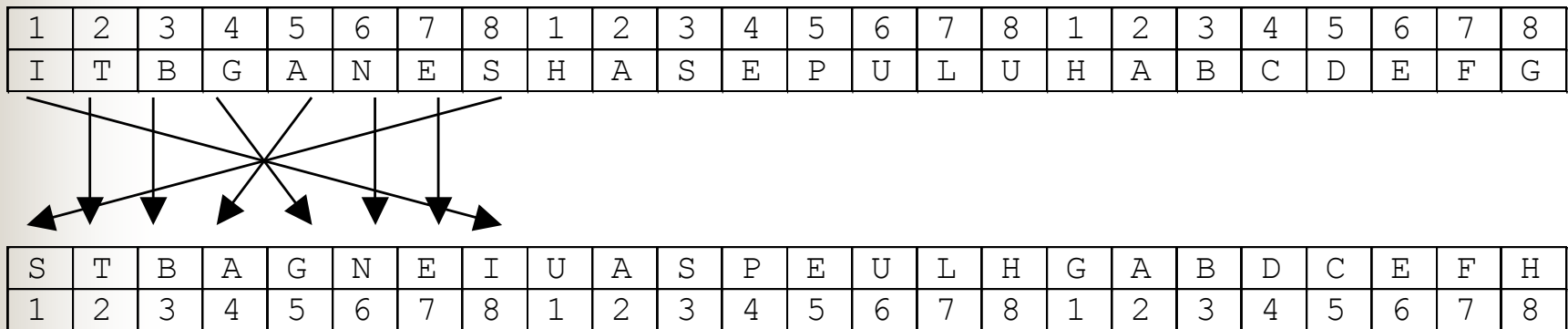
RTIAT

TENTB

Plainteks: (baca secara vertikal)

DEPARTEMEN TEKNIK INFORMATIKA ITB

- Contoh lain: Plainteks: ITB GANESHA SEPULUH
- Bagi menjadi blok-blok 8-huruf. Jika < 8 , tambahkan huruf palsu.



- Cipherteks: **STBAGNEIUASPEULHGABDCEFH**

Contoh lain. 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

CTAAAEIRPORPYNDTSCRITYGHDAUY

Super-enkripsi

- Menggabungkan *cipher* substitusi dengan *cipher* transposisi.
 - **Contoh.** Plainteks HELLO WORLD
 - 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**