04 – Kriptanalisis Sederhana

Oleh: Rinaldi Munir

Cipher abjad-tunggal (*monoalphabetic cipher*)

- Pada *cipher* abjad-tunggal, satu huruf plainteks diganti dengan satu huruf cipherteks yang bersesuaian.

- *Caesar cipher* adalah salah satu *cipher* yang tergolong ke dalam *cipher* abjad-tunggal dengan tabel substitusi berupa hasil dari pergeseran tiga huruf ke kanan.

- Secara umum, kita dapat membentuk tabel subtitusi sembarang. Jumlah kemungkinan tabel substitusi yang dapat dibuat pada sembarang *cipher* abjad-tunggal adalah sebanyak

  26! = 403.291.461.126.605.635.584.000.000

  karena ada 26! cara mempermutasikan 26 huruf alfabet.

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

- Atau berdasarkan kalimat yang mudah diingat:

  Contoh: `di bawah sinar bulan purnama hati resah jadi senang`

  Buang duplikasi huruf menjadi: `dibawhsnrulpmtejg`

  Sambung dengan huruf lain yang belum ada:

  `dibawhsnrulpmtejgcfkoqvwxyz`

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

Kriptanalisis *Cipher* Abjad-Tunggal

- *Cipher* abjad-tunggal (*monoalphabetic cipher*) memetakan sebuah huruf plainteks ke sebuah huruf cipherteks. Contoh: Caesar Cipher

- Kelemahan *cipher* abjad-tunggal: tidak dapat menyembunyikan hubungan statistik antara plainteks dengan cipherteks.
  - Huruf yang sama dienkripsi menjadi huruf cipherteks yang sama
  - Huruf yang sering muncul di dalam plainteks, sering muncul pula di dalam huruf cipherteks yang berkoesponden.

- Oleh karena itu, cipherteks dapat didekripsi tanpa mengetahui kuncinya

- *Cipher* abjad-tunggal dapat dipecahkan dengan menggunakan:
  1. teknik terkaan
  2. metode analisis frekuensi
  3. gabungan 1 dan 2

- Informasi yang dibutuhkan di dalam kriptanalisis:
  1. Mengetahui bahasa yang digunakan di dalam plainteks
  2. Konteks plainteks tentang apa

Contoh dengan metode terkaan.

Diberikan cipherteks hasil enkripsi dengan cipher abjad-tunggal sebagai berikut:

```
CTBMNBYCTCBTJDSQXBNSGSTJCBTSWXCTQTZCQVUJQJSGSTJQZZMNQJS
VLNSXVSZJUJDSTSJQUUSJUBXJDSKSUJSNTKBGAQJZBGYQTLCTZBNYBN
QJSW
```

- Jika diberikan informasi bahwa cipherteks tersebut plainteksnya berbahasa Inggris dan pesan berasal dari perusahaan yang bergerak di bidang keuangan, maka

  - konteks: keuangan

  - kata keuangan dalam Bahasa Inggris adalah `financial`

- Di dalam kata financial ada dua buah huruf i yang berulang, dengan empat buah huruf lain di antara keduanya (nanc) → inanci

- Cari enam huruf dengan pola seperti itu di dalam cipherteks. Ditemukan pada posisi ke-6, 15, 27, 31, 42, 48, 58, 66, 70, 71, 76, dan 82

```
      6          15                27   31              42      58

CTBMNBYCTCBTJDSQXBNSGSTJCBTSWXCTQTZCQVUJQJSGSTJQZZMNQJS
VLNSXVSZJUJDSTSJQUUSJUBXJDSKSUJSNTKBGAQJZBGYQTLCTZBNYBN
QJSW
```

- Hanya dua diantaranya, yaitu 31 dan 42 yang mempunyai huruf berikutnya yang berulang (berkoresponden dengan n) → inanci

- Dan dari keduanya hanya pada posisi 31 huruf a berada pada posisi yang tepat

- Jadi ditemukan `financial` pada posisi 30, yaitu untuk kriptogram `XCTQTZCQV`

```
CTBMNBYCTCBTJDSQXBNSGSTJCBTSWXCTQTZCQVUJQJSGSTJQZZMNQJS
VLNSXVSZJUJDSTSJQUUSJUBXJDSKSUJSNTKBGAQJZBGYQTLCTZBNYBN
QJSW
```

- Diperoleh pemetaan huruf:

X → f	C → i
T → n	Q → a
Z → c	V → l

- Ganti semua huruf `X`, `C`, `T`, `Q`, `Z`, `V` di dalam cipherteks dengan `f`, `i`, `n`, `a`, `c`, `l`:

```
CTBMNBYCTCBTJDSQXBNSGSTJCBTSWXCTQTZCQVUJ
QJSGSTJQZZMNQJSVLNSXVSZJUJDSTSJQUUSJUBXJ
DSKSUJSNTKBGAQJZBGYQTLCTZBNYBNQJSW
                    ↓
inBMNBYiniBnJDScfBNSGSnJiBnSWfinancialUJ
aJSGSnJaccMNaJSVLNSfVScJUJDSnSJaUUSJUBfJ
DSKSUJSNnKBGAaJcBGYanLincBNYBNaJSW
```

- Jumlah kunci berkurang menjadi 20!

- Deduksi huruf-huruf lain dapat diteruskan. Misalnya:

  incBNYBNaJSW → incorporate

- Diperoleh pemetaan huruf berikutnya:

  B → o J → t

  N → r S → e

  Y → p

- Tabel substitusi sementara

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
Q		Z		S	X			C			V		T	B	Y		N		J						

- Teruskan dengan mengganti B dengan o, N dengan r, Y dengan p, J dengan t dan S dengan e sampai diperoleh tabel subtsitusi yang lengkap

Metode Analisis Frekuensi

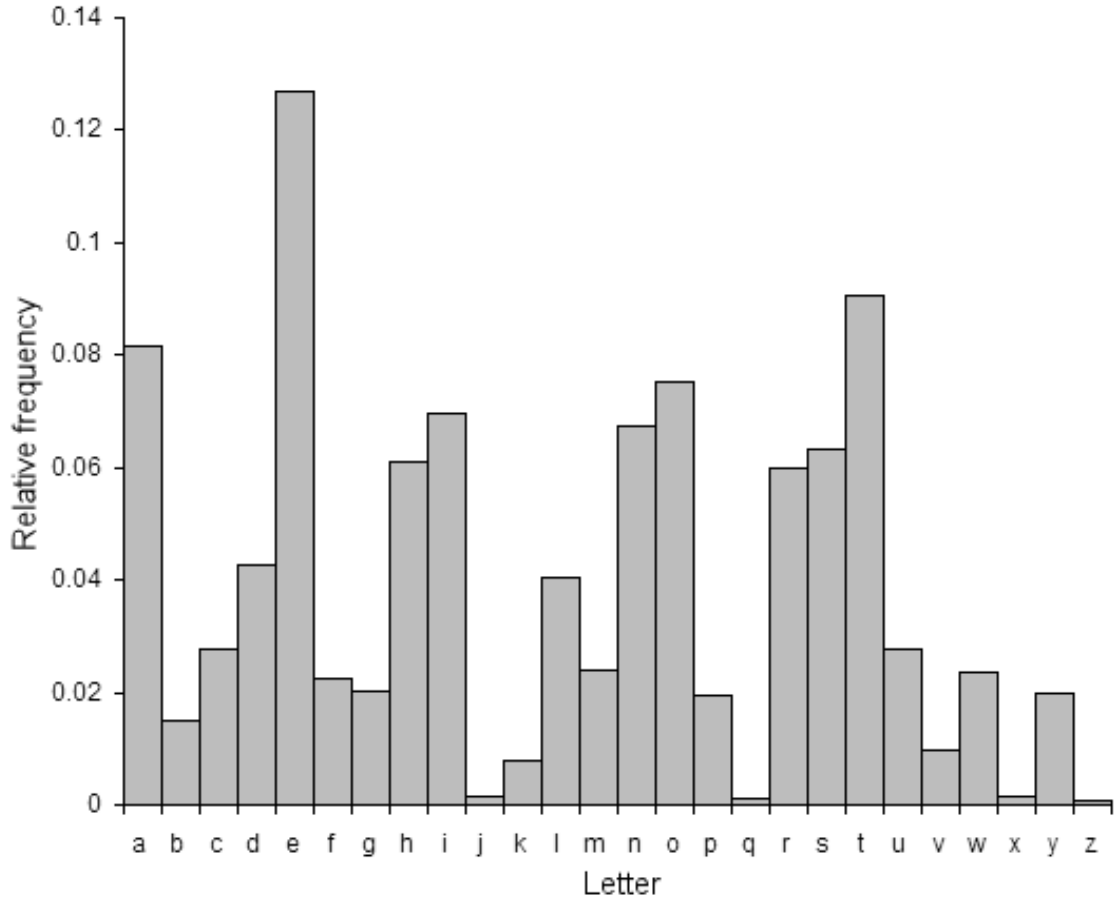
- Perulangan huruf di dalam plainteks tercermin pula pada perulangan huruf yang berkoresponden di dalam cipherteksnya.

- Hubungan statistik antara huruf-huruf di dalam plainteks dengan huruf-huruf di dalam cipherteks menjadi peluang bagi kriptanalis untuk memecahkan cipherteks.

- Dengan memanfaatkan frekuensi kemunculan huruf, atau pasangan huruf (bigram), atau tiga huruf (trigram) di dalam suatu bahasa natural, kriptanalis dapat menemukan plainteks dengan mudah.

Tabel Frekuensi kemunculan (relatif) huruf-huruf dalam teks Bahasa Inggris (sampel mencapai 300.000 karakter di dalam sejumlah novel dan suratkabar

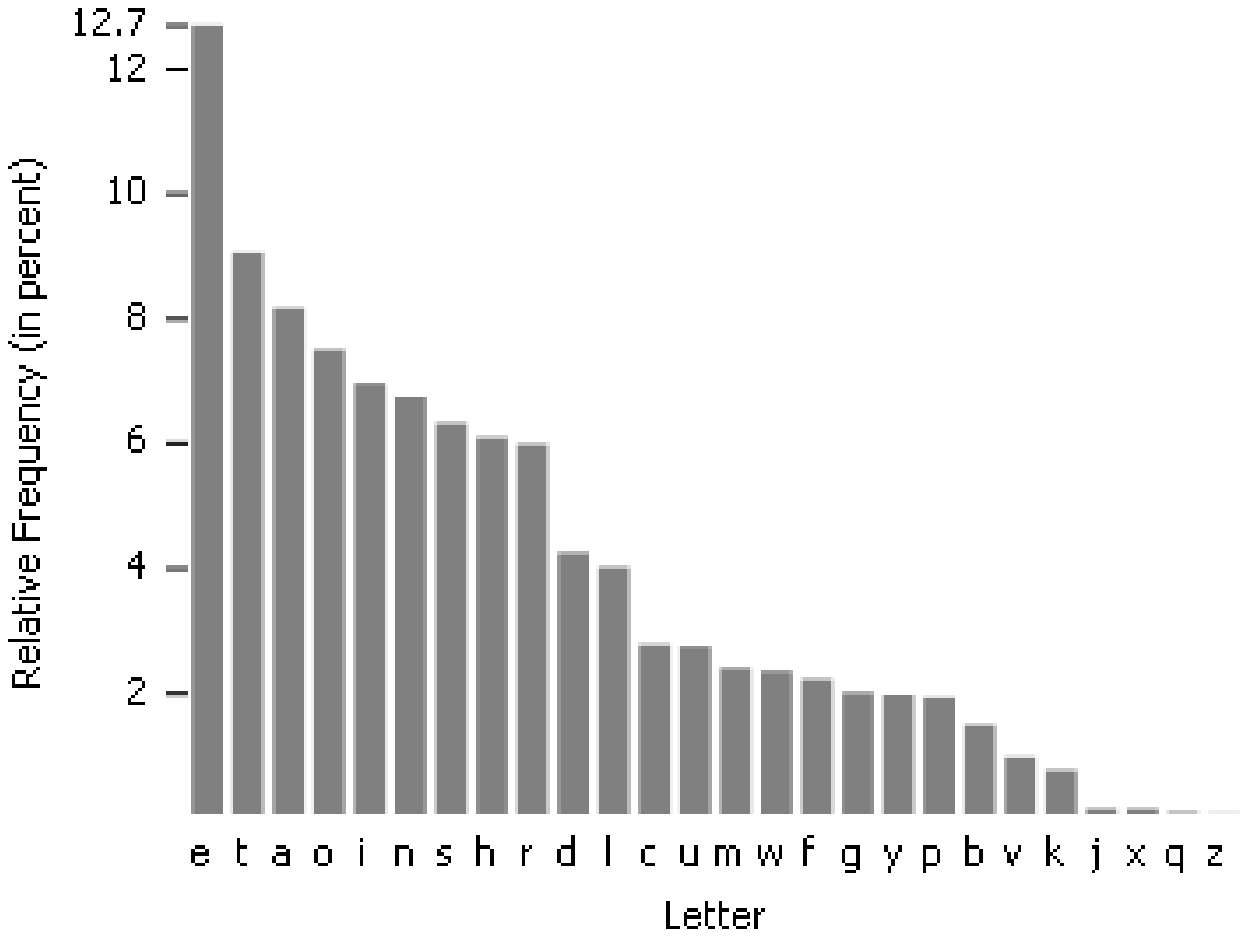
Huruf	%	Huruf	%
A	8,2	N	6,7
B	1,5	O	7,5
C	2,8	P	1,9
D	4,2	Q	0,1
E	12,7	R	6,0
F	2,2	S	6,3
G	2,0	T	9,0
H	6,1	U	2,8
I	7,0	V	1,0
J	0,1	W	2,4
K	0,8	X	2,0
L	4,0	Y	0,1
M	2,4	Z	0,1



- *Top* 10 huruf yang sering muncul dalam teks Bahasa Inggris: E, T, A, O, I, N, S, H, R, D, L, U

- Top 10 huruf *bigram* yang sering muncul dalam teks B. Inggris: TH, HE, IN, EN, NT, RE, ER, AN, TI, dan ES

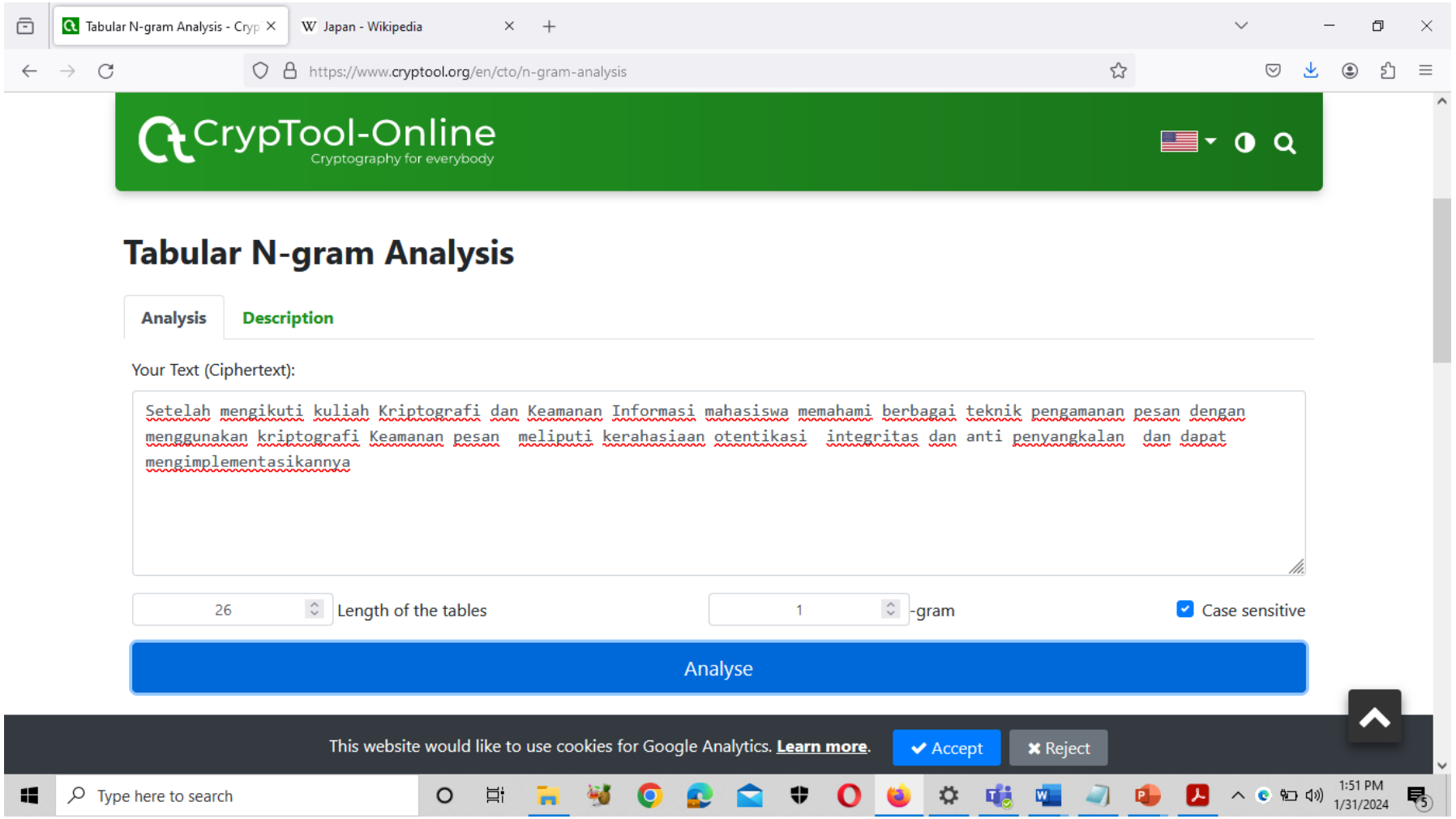
- Top 10 huruf *trigram* yang sering muncul dalam teks B. Inggris: THE, AND, THA, ENT, ING, ION, TIO, FOR, NDE, dan HAS



- Top 10 huruf yang paling sering muncul dalam Bahasa Indonesia:

Huruf	Peluang (%)
A	17,50
N	10,30
I	8,70
E	7,50
K	5,65
T	5,10
R	4,60
D	4,50
S	4,50
M	4,50

- Kakas online untuk menghitung frekuensi kemunculan huruf, bigram, trigram dsb: https://www.cryptool.org/en/cto/n-gram-analysis



CrypTool-Online
Cryptography for everybody

N-gram tables

Rank	1-gram	Abs.	Rel.
1	a	44	19.298
2	n	31	13.596
3	i	22	9.649
4	e	21	9.211
5	m	14	6.140
6	t	13	5.702
7	g	11	4.825
8	k	10	4.386
9	p	9	3.947
10	s	9	3.947
11	r	8	3.509

- Kriptanalis menggunakan tabel frekuensi kemunculan huruf dalam B. Inggris sebagai kakas bantu melakukan dekripsi.

- Misalnya, jika huruf “R” paling sering muncul di dalam cipherteks, maka kemungkinan besar itu adalah huruf “E” di dalam plainteksnya.

Langkah-langkah kriptanalisis dengan metode analisis frekuensi adalah sbb:

1. Hitung frekuensi kemunculan relatif huruf-huruf di dalam cipherteks.

2. Bandingkan hasil langkah 1 dengan Tabel frekuensi kemunculan huruf, tabel kemunculan bigram, trigram, dsb. Mengingat huruf yang paling sering muncul dalam teks Bahasa Inggris adalah huruf E, maka huruf yang paling sering muncul di dalam cipherteks kemungkinan besar adalah huruf E di dalam plainteksnya.

3. Langkah 2 diulangi untuk huruf dengan frekeuensi terbanyak berikutnya. (biasanya hanya terpakai untuk 3 sampai 5 huruf pertama di dalam tabel frekuensi).

- Contoh: Diberikan cipherteks berikut ini (Stalling, 2011):

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
```

Kita akan makukakan kriptanalisis dengan metode analisis frekuensi untuk memperoleh plainteks.

Asumsi: bahasa yang digunakan adalah Bahasa Inggris dan *cipher* yang digunakan adalah *cipher* abjad-tunggal.

Hitung frekuensi kemunculan huruf di dalam cipherteks tersebut:

Huruf	%	Huruf	%
P	13,33	Q	2,50
Z	11.67	T	2,50
S	8,33	A	1,67
U	8,33	B	1,67
O	7,50	G	1,67
M	6.67	Y	1,67
H	5,83	I	0,83
D	5,00	J	0,83
E	5,00	C	0,00
V	4,17	K	0,00
X	4,17	L	0,00
F	3,33	N	0,00
W	3,33	R	0,00

- Dua huruf yang paling sering muncul di dalam cipherteks: huruf P dan Z.
- Dua huruf yang paling sering muncul di dalam B. Inggris: huruf E dan T.
- Kemungkinan besar,
  - P adalah pemetaan dari e
  - Z adalah pemetaan dari t
- Tetapi kita belum dapat memastikannya sebab masih diperlukan cara *trial and error* dan pengetahuan tentang Bahasa Inggris.
- Tetapi ini adalah langkah awal yang bagus.

Iterasi 1:

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
 t           e   e te    t  t  e e             t

VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
   e t    t  t    e  ee    e   t     t

EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
 e  e e t t  e    t e   et
```

- ZWP dan ZWSZ dipetakan menjadi t*e dan t**t
- Kemungkinan besar W adalah pemetataan dari H sehingga kata yang mungkin untuk ZWP dan ZWSZ adalah the dan that

Iterasi 1:

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
 t           e   e te    t  t  e e              t

VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
   e t    t  t    e  ee    e  t     t

EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
 e  e e t t  e    t e  et
```

- ZWP dan ZWSZ dipetakan menjadi t*e dan t**t
- Kemungkinan besar W adalah pemetataan dari H sehingga kata yang mungkin untuk ZWP dan ZWSZ adalah the dan that

- Diperoleh pemetaan:

  P → e

  Z → t

  W → h

  S → a

- **Iterasi 2:**

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
 t  a         e   e te  a  that  e e a        a    t

VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
   e t    ta t  ha e  ee   a e   th     t  a

EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
 e  e e tat  e     the   et
```

- `WSFP` dipetakan menjadi `ha*e`.

- Dalam Bahasa Inggris, kata yang mungkin untuk `ha*e` hanyalah `have`, `hate`, `hale`, dan `haze`

- Dengan mencoba mengganti semua `F` di dalam cipherteks dengan `v`, `t`, `l`, dan `z`, maka huruf yang cocok adalah `v` sehingga `WSFP` dipetakan menjadi `have`

- Dengan mengganti `F` menjadi `v` pada kriptogram `EPYEPOPDZSZUFPO` sehingga menjadi `*e*e*e*tat*ve*`, maka kata yang cocok untuk ini adalah `representatives`

- Diperoleh pemetaan:

  E → r Y → p

  U → I O → s

  D → n

- Hasil akhir bila diselesaikan:

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

- Tabel substitusi yang dihasilkan:

- Analisis frekuensi tetap bisa dilakukan meskipun spasi dihilangkan.

- Contoh:

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIX
LIKIIXPIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJT
PRGEVEKEITREWHEXXLEXXMZITWAWSQWXSWEXTVEPMRXRSJGSTVRIEYVI
EXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCS
XRWIEVSWIIBXVIZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLIVXLIRGE
PIRQIVIIBGIIHMWYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVEWGISJKTV
WMRLIHYSPHXLIQIMYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWY
EPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZINTCMXIVJSVLMR
SCMWMSWVIRCIGXMWYMX

- Hasil perhitungan frekuensi kemunculan huruf, bigram, dan trigram:
  - huruf I paling sering muncul,
  - XL adalah bigram yang paling sering muncul,
  - XLI adalah trigram yang paling sering muncul.

Ketiga data terbanyak ini menghasilkan dugaan bahwa

I berkoresponden dengan huruf plainteks e,

XLI berkoresponden dengan the,

XL berkoresponden dengan th

Pemetaan:

I → e

X → t

L → h

- XLEX dipetakan menjadi th*t.
- Kata yang cocok untuk th*t. adalah that.
- Jadi kita memperoleh: E → a
- Hasil iterasi pertama:

heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtatePFaMVaWHKVSTYhtZe
theKeetPeJVSZaYPaRRGaReMWQhMGhMtQaReWGPSReHMtQaRaKeaTtM
JTPRGaVaKaeTRaWHatthattMZeTWAWSQWtSWatTVaPMRtRSJGSTVRea
YVeatCVMUeMWaRGMeWtMJMGCSMWtSJOMeQtheVeQeVetQSVSTWHKPaG
ARCStRWeaVSWeeBtVeZMtFSJtheKaGAaWHaPSWYSWeWeaVtheStheVt
heRGaPeRQeVeeBGeeHMWYPFhaVHaWHYPSRRFQMthaPPtheaCCeaVaWG
eSJKTVWMRheHYSPHtheQeMYhtSJtheMWReGtQaROeVFVeZaVAaKPeaW
HtaAMWYaPPthMWYRMWtSGSWRMHeVatMSWMGSTPHhaVHPFKPaZeNTCMt
eVJSVhMRSCMWMSWVeRCeGtMWYMt

- Selanjutnya,

  `Rtate` mungkin adalah `state`,

  `atthattMZE` mungkin adalah `atthattime`,

  `heVe` mungkin adalah `here`.

- Jadi, kita memperoleh pemetaan baru:

  `R` → `s`

  `M` → `i`

  `Z` → `m`

  `V` → `r`

- Hasil iterasi ke-2:

```
hereTCSWPeYraWHarSseQithaYraOeaWHstatePFairaWHKrSTYhtm
etheKeetPeJrSmaYPassGaseiWQhiGhitQaseWGPSseHitQasaKeaT
tiJTPsGaraKaeTsaWHatthattimeTWAWSQWtSWatTraPistsSJGSTr
seaYreatCriUeiWasGieWtiJiGCSiWtSJOieQthereQeretQSrSTWH
KPaGAsCStsWearSWeeBtremitFSJtheKaGAaWHaPSWYSWeWeartheS
therthesGaPesQereeBGeeHiWYPFharHaWHYPSssFQithaPPtheaCC
earaWGeSJKTrWisheHYSPHtheQeiYhtSJtheiWseGtQasOerFremar
AaKPeaWHtaAiWYaPPthiWYsiWtSGSWsiHeratiSWiGSTPHharHPFKP
ameNTCiterJSrhisSCiWiSWresCeGtiWYit
```

- Teruskan, dengan menerka kata-kata yang sudah dikenal, misalnya `remarA` mungkin `remark`, dsb

- Hasil iterasi 3:

```
hereuponlegrandarosewithagraveandstatelyairandbr
oughtmethebeetlefromaglasscaseinwhichitwasenclos
editwasabeautifulscarabaeusandatthattimeunknownt
onaturalistsofcourseagreatprizeinascientificpoin
tofviewthereweretworoundblackspotsnearoneextremi
tyofthebackandalongoneneartheotherthescalesweree
xceedinglyhardandglossywithalltheappearanceofbur
nishedgoldtheweightoftheinsectwasveryremarkablea
ndtakingallthingsintoconsiderationicouldhardlybl
amejupiterfor*hisopinionrespectingit
```

- Tambahkan spasi, tanda baca, dll

Here upon Legrand arose, with a grave and stately air, and brought me the beetle from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at that time, unknown to naturalists—of course a great prize in a scientific point of view. There were two round black spots near one extremity of the back, and a long one near the other. The scales were exceedingly hard and glossy, with all the appearance of burnished gold. The weight of the insect was very remarkable, and, taking all things into consideration, I could hardly blame Jupiter for his opinion respecting it.