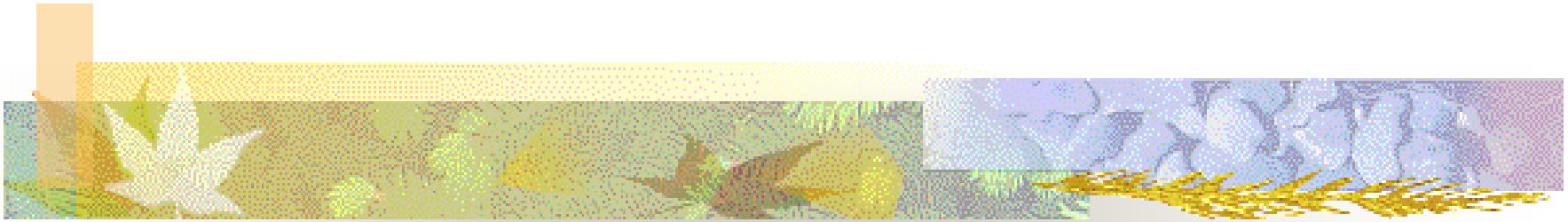
Kriptanalisis



Bahan kuliah

IF4020 Kriptografi

Kriptanalisis pada *Cipher* Abjad-Tunggal

- Jumlah kemungkinan kunci = 26!
- Tidak dapat menyembunyikan hubungan antara plainteks dengan cipherteks.
- Huruf yang sama dienkripsi menjadi huruf cipherteks yang sama
- Huruf yang sering muncul di dalam palinteks, sering muncul pula di dalam cipherteksnya.

- Oleh karena itu, cipherteks dapat didekripsi tanpa mengetahui kunci (*ciphertext-only attack*)

- Metode yang digunakan:

  1. Terkaan
  2. Statistik (analisis frekuensi)

- Informasi yang dibutuhkan:

  1. Mengetahui bahasa yang digunakan untuk plainteks
  2. Konteks plainteks

Metode Terkaan

Asumsi: - bahasa plainteks adalah B. Inggris
- spasi tidak dibuang

Tujuan: mereduksi jumlah kunci

Contoh 1. Cipherteks: **G WR W RWL**

Plainteks: I AM A MA*

I AM A MAN

Jumlah kunci berkurang dari 26! menjadi 22!

Contoh 2.

Cipherteks: **HKC**

Plainteks:

- lebih sukar ditentukan,
- tetapi tidak mungkin

  Z diganti dengan **H**,

  Q dengan **K**,

  K dengan **C**,

karena tidak ada kata “ZQC” dalam Bahasa Inggris

Contoh 3.

Cipherteks: **HATTPT**

Plainteks: salah satu dari **T** atau **P** merepresentasikan huruf vokal, misal

CHEESE

MISSES

CANNON

Contoh 4.

Cipherteks: **HATTPT**

Plainteks: diketahui informasi bahwa pesan tersebut adalah nama negara.

→ GREECE

- Proses menerka dapat menjadi lebih sulit jika cipherteks dikelompokkan ke dalam blok-blok huruf.
- Contoh:

CTBMN BYCTC BTJDS QXBNS GSTJC BTSWX CTQTZ CQVUJ
QJSGS TJQZZ MNQJS VLNSX VSZJU JDSTS JQUUS JUBXJ
DSKSU JSNTK BGAQJ ZBGYQ TLCTZ BNYBN QJSW

- Jika diberikan informasi bahwa cipherteks tersebut berasal dari perusahaan yang bergerak di bidang keuangan, maka proses menerka dapat lebih mudah

- Kata keuangan dalam Bahasa Inggris adalah FINANCIAL

- Ada dua buah huruf I yang berulang, dengan empat buah huruf lain di antara keduanya (NANC)
- Cari huruf berulang dengan pola seperti itu di dalam cipherteks (tidak termasuk spasi). Ditemukan pada posisi 6, 15, 27, 31, 42, 48, 58, 66, 70, 71, 76, dan 82

```
      6          15                 27
CTBMN BYCTC BTJDS QXBNS GSTJC BTSWX
CTQTZ CQVUJ QJSGS TJQZZ MNQJS VLNSX
VSZJU JDSTS JQUUS JUBXJ DSKSU JSNTK
BGAQJ ZBGYQ TLCTZ BNYBN  QJSW
```

- Hanya dua diantaranya, yaitu 31 dan 42 yang mempunyai huruf berikutnya yang berulang (berkoresponden dengan N
- Dan dari keduanya hanya pada posisi 31 huruf A berada pada posisi yang tepat
- Jadi ditemukan FINANCIAL pada posisi 30, yaitu untuk kriptogram **XCTQTZCQV**

CTBMN BYCTC BTJDS QXBNS GSTJC BTSWX
CTQTZ CQVUJ QJSGS TJQZZ MNQJS VLNSX
VSZJU JDSTS JQUUS JUBXJ DSKSU JSNTK
BGAQJ ZBGYQ TLCTZ BNYBN QJSW

- Diperoleh pemetaan:

X	→	f	**C**	→	i
T	→	n	**Q**	→	a
Z	→	c	**V**	→	l

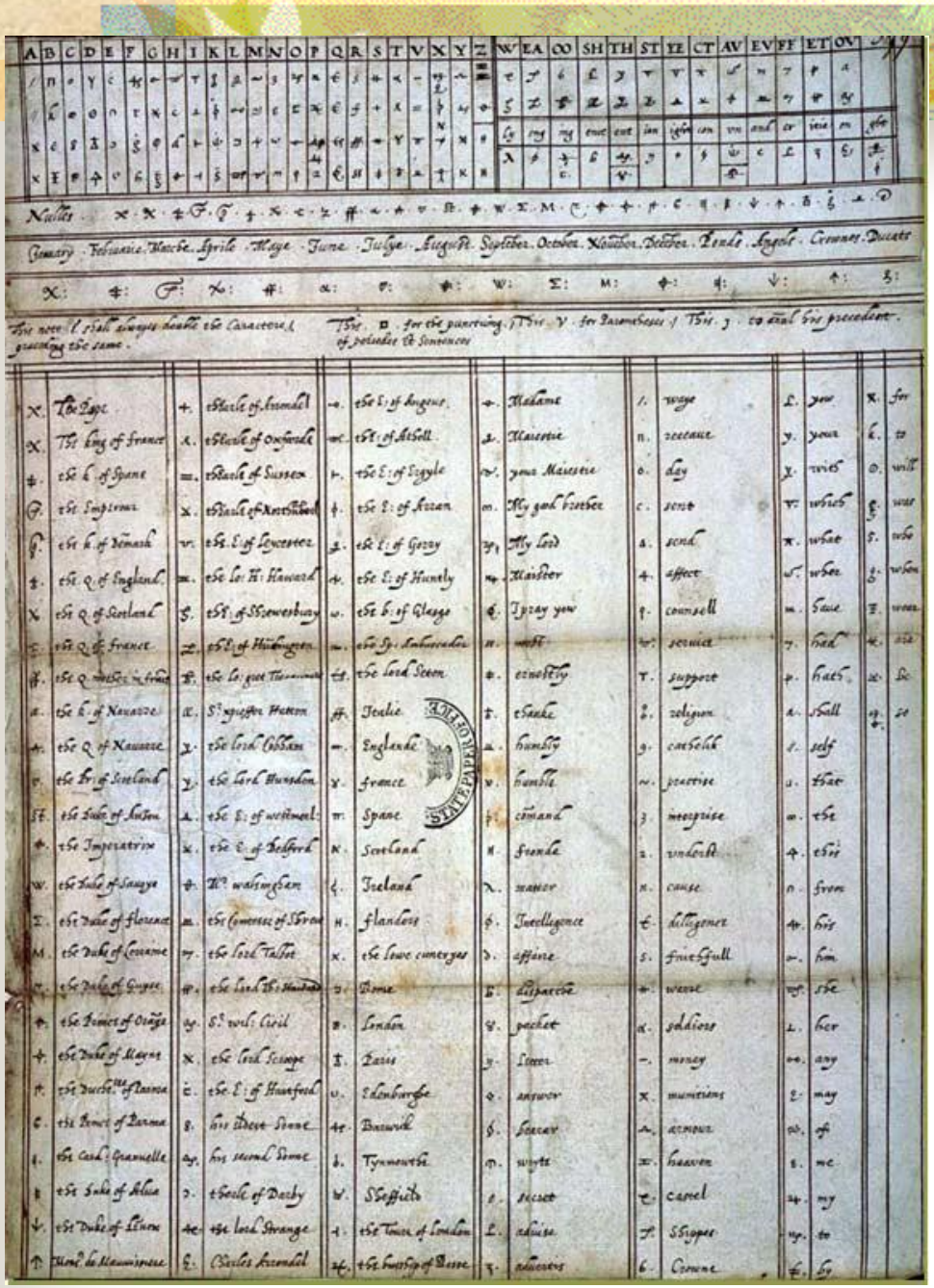
- Ganti semua huruf **X**, **C**, **T**, **Q**, **Z**, **V** dengan f, i, n, a, c, l:

CTBMN BYCTC BTJDS QXBNS GSTJC BTSWX CTQTZ CQVUJ
QJSGS TJQZZ MNQJS VLNSX VSZJU JDSTS JQUUS JUBXJ
DSKSU JSNTK BGAQJ ZBGYQ TLCTZ BNYBN QJSW

inBMN BYini BnJDS cfBNS GSnJi BnSWf inanc ialUJ
aJSGS nJacc MNaJS VLNSf VScJU JDSnS JaUUS JUBfJ
DSKSU JSNnK BGAaJ cBGYa nLinc BNYBN aJSW

- Jumlah kunci berkurang menjadi 20! Deduksi dapat diteruskan.

- Peristiwa yang menimpa Queen Mary of Scotland pada abad 18 karena menggunakan *cipher* abjad-tunggal yang mudah diterka ➔ mudah dipecahkan.

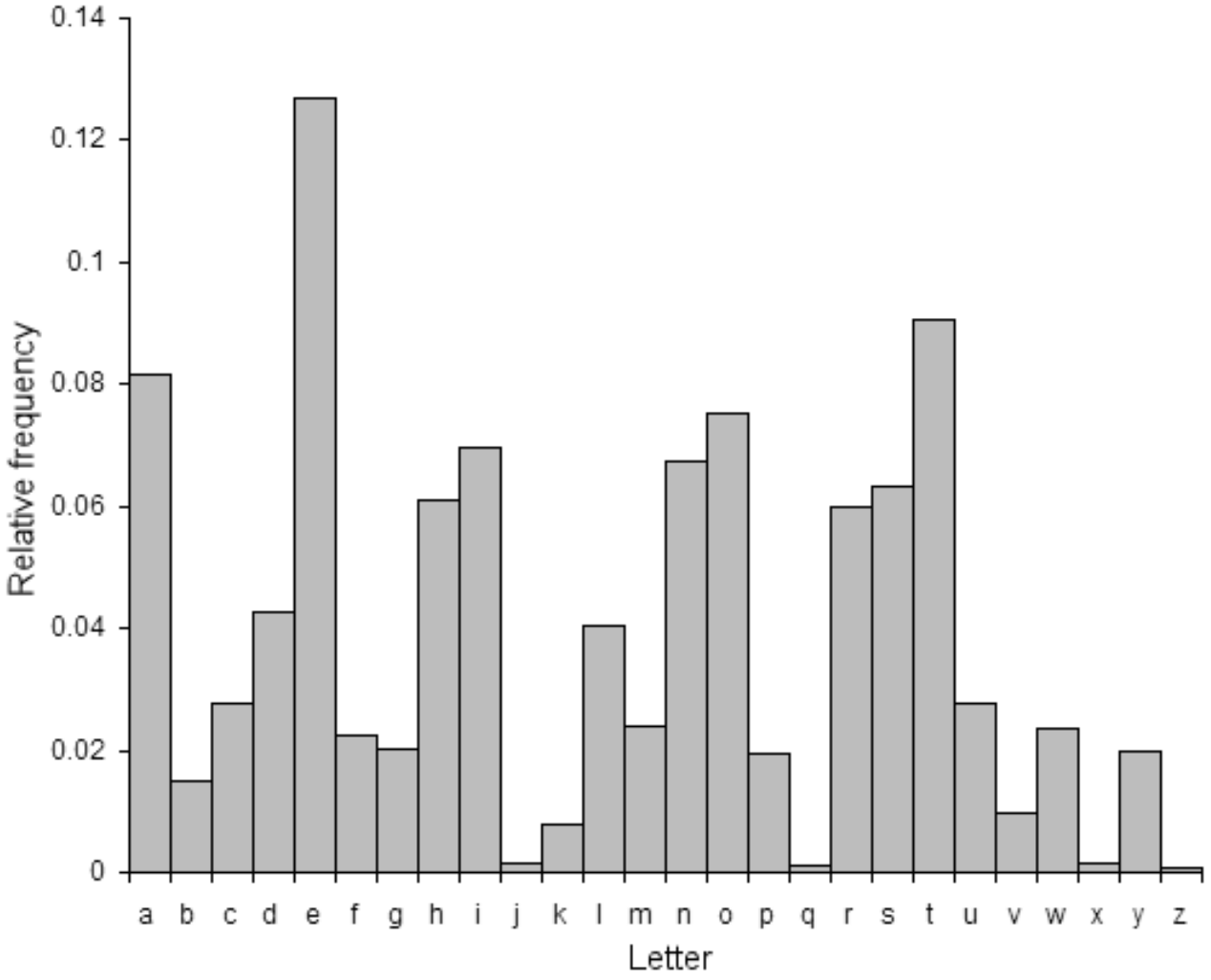


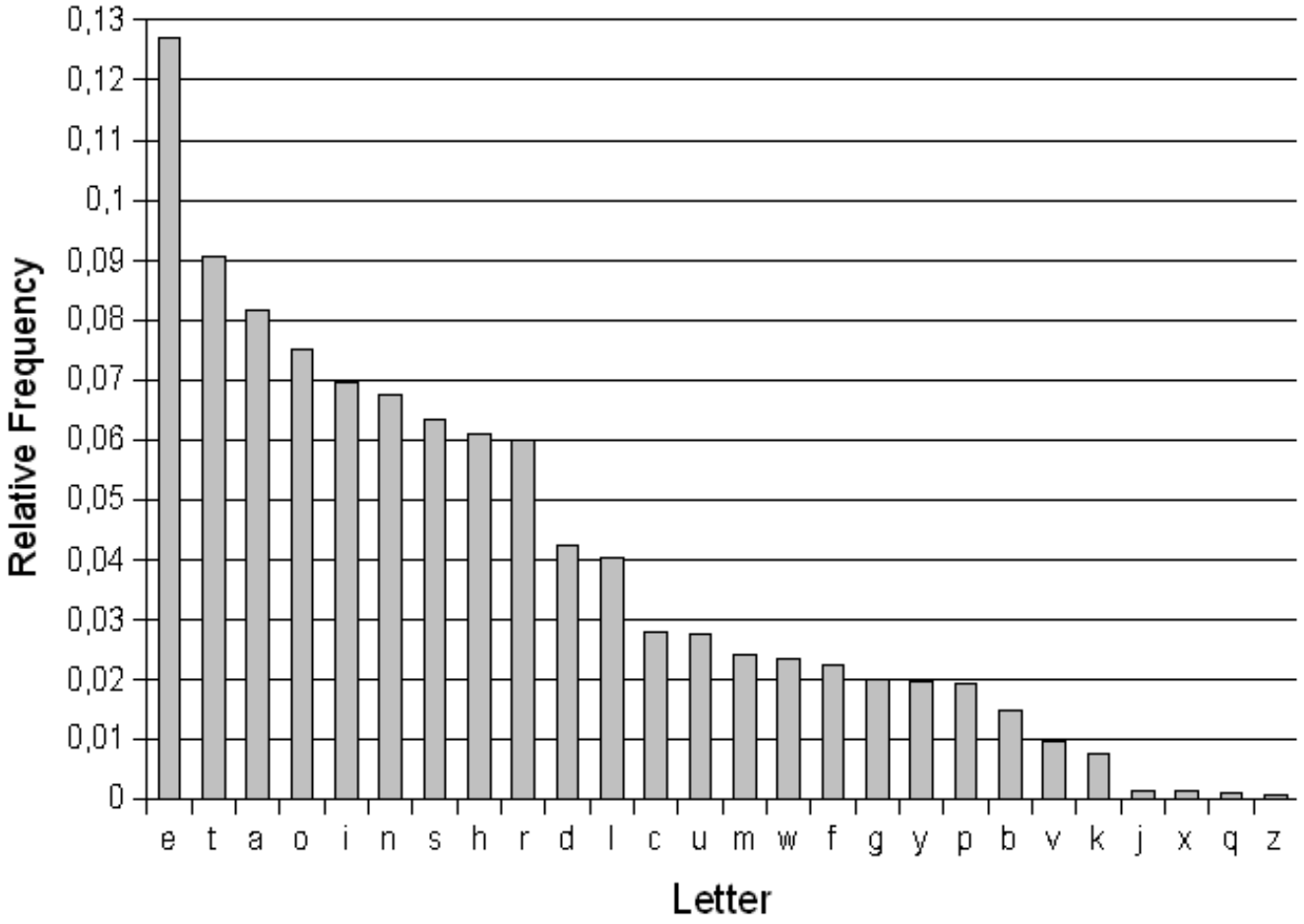
Cipher yang digunakan oleh *Mary Queen of Scott.*

Metode Analisis Frekuensi

Tabel 2. 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


0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
Relative frequency
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
Letter


Relative Frequency
0,13
0,12
0,11
0,1
0,09
0,08
0,07
0,06
0,05
0,04
0,03
0,02
0,01
0
e t a o i n s h r d l c u m w f g y p b v k j x q z
Letter

- *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

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

- Kemunculan huruf-huruf di dalam sembarang plainteks tercermin pada tabel tersebut.

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

Teknik analisis frekuensi dilakukan sebagai berikut:

1. Misalkan plainteks ditulis dalam Bahasa Inggris (plainteks dalam bahasa lain secara prinsip tidak jauh berbeda).
2. Asumsikan plainteks dienkripsi dengan *cipher* alfabat-tunggal.
3. Hitung frekuensi kemunculan relatif huruf-huruf di dalam cipherteks.
4. Bandingkan hasil langkah 3 dengan Tabel 2. Catatlah bahwa huruf yang paling sering muncul dalam teks Bahasa Inggris adalah huruf E. Jadi, huruf yang paling sering muncul di dalam cipherteks kemungkinan besar adalah huruf E di dalam plainteksnya.
5. Langkah 4 diulangi untuk huruf dengan frekeuensi terbanyak berikutnya.

- Contoh: Diberikan cipherteks berikut ini:

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

Lakukakan kriptanalisis dengan teknik analisis frekuensi untuk memperoleh plainteks. Asumsi: bahasa yang digunakan adalah Bahasa Inggris dan *cipher* yang digunakan adalah *cipher* abjad-tunggal.

- 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

- Huruf yang paling sering muncul di dalam cipherteks: huruf P dan Z.
- 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 sudah 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`

- 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 **Z** 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
```

- Analisis frekuensi tetap bisa dilakukan meskipun spasi dihilangkan:

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFE
MVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQL
MGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITR
EWHEXXLEXXMZITWAWSQWXSWEXTVEPMRXRSJGSTVRI
EYVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVIQ
IVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJXL
IKEGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQIVI
IBGIIHMWYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVE
WGISJKTVWMRLIHYSPHXLIQIMYLXSJXLIMWRIGXQER
OIVFVIZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGSWRM
HIVEXMSWMGSTPHLEVHPFKPEZINTCMXIVJSVLMRSCM
WMSWVIRCIGXMWYMX

- Hasil perhitungan frekuensi kemunculan huruf:
  - 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:

```
heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtatePFaMVaWHKVST
YhtZetheKeetPeJVSZaYPaRRGaReMWQhMGhMtQaReWGPSReHMt
QaRaKeaTtMJTPRGaVaKaeTRaWHatthattMZeTWAWSQWtSWatTV
aPMRtRSJGSTVReaYVeatCVMUeMWaRGMeWtMJMGCSMWtSJOMeQt
heVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtVeZMtFSJtheKaG
AaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFha
VHaWHYPSRRFQMthaPPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQ
eMYhtSJtheMWReGtQaROeVFVeZaVAaKPeaWHtaAMWYaPPthMWY
RMWtSGSWRMHeVatMSWMGSTPHhaVHPFKPaZeNTCMteVJSVhMRSC
MWMSWVeRCeGtMWYMt
```

- 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:

```
hereTCSWPeYraWHarSseQithaYraOeaWHstatePFairaWHKrST
YhtmetheKeetPeJrSmaYPassGaseiWQhiGhitQaseWGPSseHit
QasaKeaTtiJTPsGaraKaeTsaWHatthattimeTWAWSQWtSWatTr
aPistsSJGSTrseaYreatCriUeiWasGieWtiJiGCSiWtSJOieQt
hereQeretQSrSTWHKPaGAsCStsWearSWeeBtremitFSJtheKaG
AaWHaPSWYSWeWeartheStherthesGaPesQereeBGeeHiWYPFha
rHaWHYPSssFQithaPPtheaCCearaWGeSJKTrWisheHYSPHtheQ
eiYhtSJtheiWseGtQasOerFremarAaKPeaWHtaAiWYaPPthiWY
siWtSGSWsiHeratiSWiGSTPHharHPFKPameNTCiterJSrhisSC
iWiSWresCeGtiWYit
```

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

- Hasil iterasi 3:

```
hereuponlegrandarosewithagraveandstatelyairandbrou
ghtmethebeetlefromaglasscaseinwhichitwasenclosedit
wasabeautifulscarabaeusandatthattimeunknowntonatur
alistsofcourseagreatprizeinascientificpointofviewt
hereweretworoundblackspotsnearoneextremityofthebac
kandalongoneneartheotherthescaleswereexceedinglyha
rdandglossywithalltheappearanceofburnishedgoldthew
eightoftheinsectwasveryremarkableandtakingallthing
sintoconsiderationicouldhardlyblamejupiterfor*hiso
pinionrespectingit
```

- 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.

Metode Kasiski

- Kembali ke *Vigenere cipher*…

- Friedrich Kasiski adalah orang yang pertama kali memecahkan *Vigènere cipher* pada Tahun 1863 .

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

- Metode Kasiski membantu menemukan panjang kunci *Vigenere cipher*.

- Metode Kasiski memanfaatkan keuntungan bahwa bahasa Inggris tidak hanya mengandung perulangan huruf,

- tetapi juga perulangan pasangan huruf atau tripel huruf, seperti `TH`, `THE`, dsb.

- Perulangan kelompok huruf ini ada kemungkinan menghasilkan kriptogram yang berulang.

- Contoh 1:

Plainteks : `CRYPTO IS SHORT FOR CRYPTOGRAPHY`
Kunci : `abcdab cd abcda bcd abcdabcdabcd`
Cipherteks : **`CSASTP`** `KV SIQUT GQU` **`CSASTP`**`IUAQJB`

- Pada contoh ini, `CRYPTO` dienkripsi menjadi kriptogram yang sama, yaitu **`CSATP`**.

- Tetapi kasus seperti ini tidak selalu demikian, misalnya pada contoh berikut ini….

- Contoh 2:

Plainteks	: `CRYPTO IS SHORT FOR CRYPTOGRAPHY`
Kunci	: `abcdef ab cdefa bcd efabcdefabcd`
Cipherteks	: **`CSASXT`** `IT UKWST GQU` **`CWYQVR`**`KWAQJB`

- Pada contoh di atas, `CRYPTO` tidak dienkripsi menjadi kriptogram yang sama.

- Mengapa bisa demikian?

- Secara intuitif: jika jarak antara dua buah *string* yang berulang di dalam plainteks merupakan kelipatan dari panjang kunci,

- maka *string* yang sama tersebut akan muncul menjadi kriptogram yang sama pula di dalam cipherteks.

- Pada Contoh 1,
  - kunci = `abcd`
  - panjang kunci = 4
  - jarak antara dua `CRYPTO` yang berulang = 16
  - 16 = kelipatan 4

  ∴ `CRYPTO` dienkripsi menjadi kriptogram yang sama

- Pada Contoh 2,
  - kunci = `abcdf`
  - panjang kunci = 6
  - jarak antara dua `CRYPTO` yang berulang = 16
  - 16 bukan kelipatan 6

∴ `CRYPTO` tidak dienkripsi menjadi kriptogram yang sama

- Goal metode Kasiski: mencari dua atau lebih kriptogram yang berulang untuk menentukan panjang kunci.

Langkah-langkah metode Kasiski:

1. Temukan semua kriptogram yang berulang di dalam cipherteks (pesan yang panjang biasanya mengandung kriptogram yang berulang).
2. Hitung jarak antara kriptogram yang berulang
3. Hitung semua faktor (pembagi) dari jarak tersebut (faktor pembagi menyatakan panjang kunci yang mungkin).
4. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut . Nilai tersebut mungkin adalah panjang kunci.

- Contoh:

DYDUXRMHTVDV**NQD**QNW**DYDUXRMH**ARTJGW**NQD**

Kriptogram yang berulang: **DYUDUXRM** dan **NQD**.

Jarak antara dua buah perulangan **DYUDUXRM** = 18.
Semua faktor pembagi 18 : {18, 9, 6, 3, 2}

Jarak antara dua buah perulangan **NQD** =20.
Semua faktor pembagi 20 : {20, 10, 5, 4, 2}.

Irisan dari kedua buah himpunan tersebut adalah 2
Panjang kunci kemungkinan besar adalah 2.

- Setelah panjang kunci diketahui, maka langkah berikutnya menentukan kata kunci

- Kata kunci dapat ditentukan dengan menggunakan *exhaustive key serach*

- Jika panjang kunci = *p*, maka jumlah kunci yang harsu dicoba adalah 26^p

- Namun lebih mangkus menggunakan teknik analisis frekuensi.

Langkah-langkahnya sbb:

1. Misalkan panjang kunci yang sudah berhasil dideduksi adalah *n*. Setiap huruf kelipatan ke-*n* pasti dienkripsi dengan huruf kunci yang sama. Kelompokkan setiap huruf ke-*n* bersama-sama sehingga kriptanalis memiliki *n* buah "pesan", masing-masing dienkripsi dengan substitusi alfabet-tunggal (dalam hal ini *Caesar cipher*).

2. Tiap-tiap pesan dari hasil langkah 1 dapat dipecahkan dengan teknik analisis frekuensi.

3. Dari hasil langkah 3 kriptanalis dapat menyusun huruf-huruf kunci. Atau, kriptanalis dapat menerka kata yang membantu untuk memecahkan cipherteks

- Contoh:

1 2 3

LJVBQ STNEZ LQMED **LJV**MA MPKAU FAVAT **LJV**DA YYVNF
JQLNP **LJV**HK VTRNF **LJV**CM LKETA **LJV**HU YJVSF KRFTT
WEFUX VHZNP

4 5 6

Kriptogram yang berulang adalah **LJV**.

Jarak **LJV** ke-1 dengan **LJV** ke-2 = 15

Jarak **LJV** ke-2 dengan **LJV** ke-3 = 15

Jarak **LJV** ke-3 dengan **LJV** ke-4 = 15

Jarak **LJV** ke-4 dengan **LJV** ke-5 = 10

Jarak **LJV** ke-5 dengan **LJV** ke-6 = 10

Faktor pembagi 15 = {3, 5, 15}

Faktor pembagi 10 = {2, 5, 10}

Irisan kedua himpunan ini = 5. Jadi, panjang kunci diperkirakan = 5

- Kelompokkan “pesan” setiap kelipatan ke-5, dimulai dari huruf cipherteks pertama, kedua, dan seterusnya.

LJVBQ STNEZ LQMED **LJV**MA MPKAU FAVAT **LJV**DA YYVNF
JQLNP **LJV**HK VTRNF **LJV**CM LKETA **LJV**HU YJVSF KRFTT
WEFUX VHZNP

Kelompok	Pesan	Huruf paling sering muncul
1	LSLLM FLYHL VLLLY KWV	L
2	JTQJP AJYQJ TJKJJ REH	J
3	VNMVK VVVLV RVEVV FFZ	V
4	BEEMA ADNNH NCTHS TUN	N
5	QZDAU TAFPK FMAUF TXP	A

- Dalam Bahasa Inggris, 10 huruf yang yang paling sering muncul adalah E, T, A, O, I, N, S, H, R, dan D,

- Triplet yang paling sering muncul adalah THE. Karena **LJV** paling sering muncul di dalam cipherteks, maka dari 10 huruf tsb semua kemungkinan kata 3-huruf dibentuk dan kata yang yang cocok untuk **LJV** adalah `THE`.

- Jadi, kita dapat menerka bahwa **LJV** mungkin adalah `THE`.

- Dari sini kita buat tabel yang memetakan huruf plainteks dengan cipherteks dan huruf-huruf kuncinya (ingatlah bahwa setiap nilai numerik dari huruf kunci menyatakan jumlah pergeseran huruf pada *Caesar cipher*):

Kelompok	Huruf plainteks	Huruf cipherteks	Huruf kunci
1	T	L	S (=18)
2	H	J	C (=2)
3	E	V	R (=17)
4	N	N	A (=0)
5	O	A	M (=12)

Jadi, kuncinya adalah SCRAM

- Dengan menggunakan kunci SCRAM cipherteks berhasil didekripsi menjadi:

```
THEBE ARWEN TOVER THEMO UNTAI NYEAH
THEDO GWENT ROUND THEHY DRANT THECA
TINTO THEHI GHEST SPOTH ECOUL DFIND
```

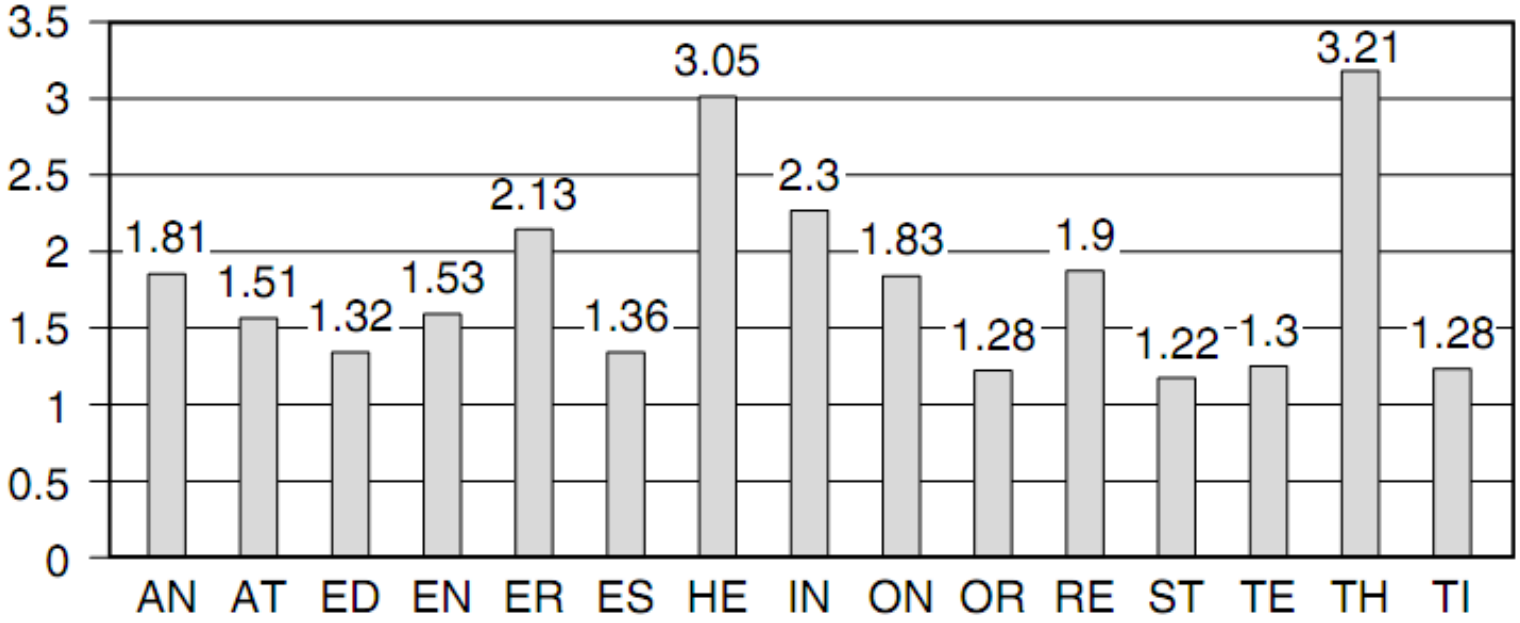
- atau dalam kalimat yang lebih jelas:

```
THE BEAR WENT OVER THE MOUNTAIN YEAH
THE DOG WENT ROUND THE HYDRANT THE CAT
INTO THE HIGHEST SPOT HE COULD FIND
```

Kriptanalisis Playfair Cipher

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

- *Playfair cipher* dapat dipecahkan dengan analisis frekuensi pasangan huruf, karena terdapat tabel frekuensi kemunculan pasangan huruf dalam Bahasa Inggris.


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

- 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.

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