

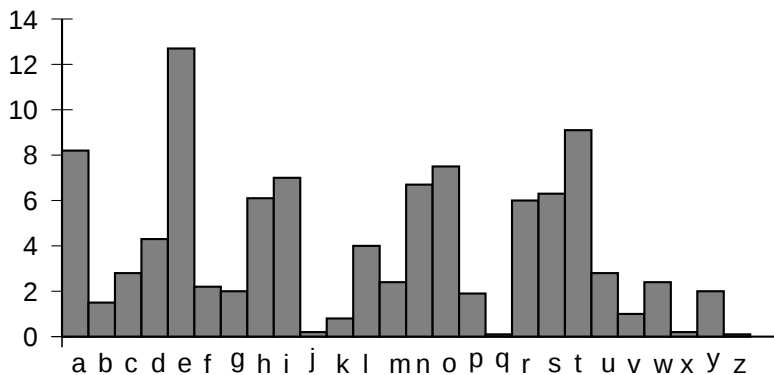
Session 14 – The Vigenère cipher

European section – Season 03

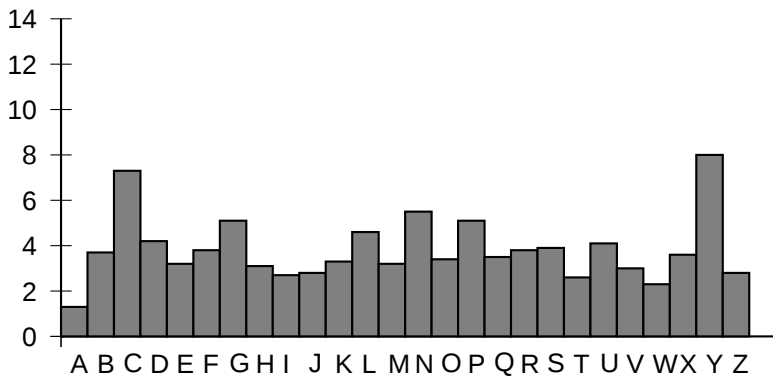
A cipher text

EBGIQ LSVRY ENJON CIUZC NNQPZ PCPQF LHIOB THVRC XITXG YAEYL NYDPD LNGCY
XUPCK THFGM YXGBD FFNIS YZQBR FHDCD WSYRY ENJOK THFSL PPKDY MFAMM
YWGXR CUVOQ ZHKCR SUVSL EBGWM CHKXE TNYSJ WVGSL LVQNW EBCDG DAQSL
RNQLC SUPQC ONJOK LHIYG YAVYZ PBCXE PXJKB MYGXL LGGNK ZCUdT ZHNSN HCILW
OIVSL RCHL HCUON LLGXR DVWDF PQCCL ZNIYG YAVYC XVCBP LMUDF PHCWC THUYD
LLCCR SUVGY DMVSJ WJQCQ TVNOZ JVGSL RBWXE FHFOP TNVYR SYYYP WXXKE
PHGBY WUPNN LLVSA FFCBJ JIPDF LNSDR ZKDI YIYXY DNJOB PUVRU LLTKL EBGGY
DUNPP PXUZY YANOP LHFRC EIQUY XITON ZMKDG GYCZN CICMF EIVRC DCVEY ECQXY
YXJKB NIPMC YNTRK PXJSQ XCPNM YNION CIUZC NNQPL ZNDOG YAJKL RYFSL EBGWM
CHKXE LHFWM DNRKP ECEEJ LLNIM YNION CIUZC NNQPP PGQFG YACVJ EBGMP FGDVG
YAOYP EUTPP ZGCBM FHFQK EIPOG YBKCA PFNGY WFYSR SUUZM ZHUYD LLVRC HITUF
LXVKI PHJSK QCXOU PYMCY YXTOB FWGNR SYUZM ZHVVQ ZGGDF THIVG VYCYX TFHSJ
PZQBR FHDCD WSPYM YYGFC CWCWC EIERY YAGDF PVGNB THIRC CYQBC WMGDF
PSYYS WXJKT PXKCA ZPGBC ONJOU ZLNNQ SYCFG PMVWY ENTOQ DCVGY DUNKP
RYCXB SYCFW DNQXC EBCDU LMEEP CYPDJ JNJOM MDGMR ZZJSQ LNVOL ECQXQ
LHFKR DIOON ZCPDY SOIOQ EURVC SUFLC PHJKK XYTOB THVYG EUUKL LHERM CZQBK
LHCMJ PMOYG DNUKR OIYXD LWKXE EBGGY WFIBG AJGMR SYKBM YLKXE THDYR SBCXB
DVTKA PXJSQ WYICY RUKXQ ENJOQ EIPOQ ZHGSR SYTCG OYCXB SYCFC OBKCQ SIWVB
PLUMY FAJDD TLGKL OUTOB XCUDD TFNOB SCUFG DCQXZ FNVRC MFQMI DFKNM FNYSR
SUHKG YNCXB THCZN CIRBG LNGDG YENSL RHQSQ PGQSQ EGCXY RYFDM PUUOG
EUYKW QLQWR SYJYJ PUPNN PYTOB THUSB PUVDF PZCBC YXYKQ LHQDF PLDVM
NECXB EBGWM CNBY CIWXB TNNYM VYFCS DJKMG ZOUVW DNTYL RUPND CYURH
FMVSL QLQXR ZZKDU LMCXC HMRYM YCVGY DMJSL JUURC DNWNG PXKDF PBGKP
ONJOA WURZG YADOF THFRG XBGDS CHGNF TMJOY ONGXB ZHUU LHISL RUNSR
EFGBG QZQPY RIPIY YXUKU DYXOP LFQPR SYYKP OYPCU LNERG YAJSK EBTYS RBVRC
MUTC

Standard frequencies in English



Frequencies in the cipher



What we notice

What we notice

- No frequency less than 1.3%.

What we notice

- No frequency less than 1.3%.
- No frequency more than 10%.

What we notice

- No frequency less than 1.3%.
- No frequency more than 10%.
- C and Y could stand for e, but just as well for a, h, i, m, o, r, s, t.

What we notice

- No frequency less than 1.3%.
- No frequency more than 10%.
- C and Y could stand for e, but just as well for a, h, i, m, o, r, s, t.
- The global shape of the histogram.

What we can conclude

- Not in English ? But,

What we can conclude

- Not in English ? But,
 - we know it's in English ;

What we can conclude

- Not in English ? But,
 - we know it's in English ;
 - no language has such standard letter frequency histogram.

What we can conclude

- Not in English ? But,
 - we know it's in English ;
 - no language has such standard letter frequency histogram.
- Not a simple Caesar Cipher.

What we can conclude

- Not in English ? But,
 - we know it's in English ;
 - no language has such standard letter frequency histogram.
- Not a simple Caesar Cipher.
- Not a monoalphabetic substitution cipher.

What we can conclude

- Not in English ? But,
 - we know it's in English ;
 - no language has such standard letter frequency histogram.
- Not a simple Caesar Cipher.
- Not a monoalphabetic substitution cipher.
- Frequency analysis is not enough.

Blaise de Vigenère (1523 – 1596)



La cifra del Sig. Giovan Battista Belaso – Venetia 1553

AB	a b c d e f g h i l m n o p q r f t u x y z
CD	a b c d e f g h i l m t u x y z n o p q r f
EF	a b c d e f g h i l m z n o p q r f t u x y
GH	a b c d e f g h i l m f t u x y z n o p q r
IL	a b c d e f g h i l m y z n o p q r f t u x
MN	a b c d e f g h i l m r f t u x y z n o p q
OP	a b c d e f g h i l m x y z n o p q r f t u
QR	a b c d e f g h i l m q r f t u x y z n o p
ST	a b c d e f g h i l m p q r f t u x y z n o
VX	a b c d e f g h i l m u x y z n o p q r f t
YZ	a b c d e f g h i l m o p q r f t u x y z n

The tabula recta

	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

How to encipher a message

t h e w o r l d i s
R A D I O R A D I O

.

a f l a t d i s c
R A D I O R A D I

.

How to encipher a message

t h e w o r l d i s
R A D I O R A D I O
K

a f l a t d i s c
R A D I O R A D I
.

How to encipher a message

t h e w o r l d i s
R A D I O R A D I O
K H

a f l a t d i s c
R A D I O R A D I
.

How to encipher a message

t h e w o r l d i s
R A D I O R A D I O
K H H E C I L G Q G

a f l a t d i s c
R A D I O R A D I
R F O I H U I V S

How to decipher a message

K H H E C I L G Q G
R A D I O R A D I O
.

R F O I H U I V S
R A D I O R A D I
.

How to decipher a message

K H H E C I L G Q G

R A D I O R A D I O

t

R F O I H U I V S

R A D I O R A D I

.

How to decipher a message

K H H E C I L G Q G

R A D I O R A D I O

t h

R F O I H U I V S

R A D I O R A D I

.

How to decipher a message

K H H E C I L G Q G
R A D I O R A D I O
t h e w o r l d i s

R F O I H U I V S
R A D I O R A D I
a f l a t d i s c

Encode and decode a
quote about mathematics

Modular arithmetic

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv$

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv 9 [26]$

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv 9 [26]$
- $47 \equiv$

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv 9 [26]$
- $47 \equiv 21 [26]$

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv 9 [26]$
- $47 \equiv 21 [26]$
- $260 \equiv$

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv 9 [26]$
- $47 \equiv 21 [26]$
- $260 \equiv 0 [26]$

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv 9 [26]$
- $47 \equiv 21 [26]$
- $260 \equiv 0 [26]$
- $12 \equiv$

Definition

Two numbers a and b are congruent modulo n if their difference is a multiple of n . Then, we write

$$a \equiv b[n].$$

- $35 \equiv 9 [26]$
- $47 \equiv 21 [26]$
- $260 \equiv 0 [26]$
- $12 \equiv 12 [26]$

Modular arithmetic in cryptography

Each letter is associated to a two-digit number : 00 to A, 01 to B and so on until 25 to Z, This correspondance lets us transform any message into a string of two-digit numbers.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19

The Caesar cipher

A shift of 4 is modeled as

The Caesar cipher

A shift of 4 is modeled as addition by 4 :

$$L = I + 4.$$

The Caesar cipher

A shift of 4 is modeled as addition by 4 :

$$L = I + 4.$$

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19

The Caesar cipher

A shift of 4 is modeled as addition by 4 :

$$L = I + 4.$$

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19
23	11	08	26	18	21	15	07	12	22	09	15	04	23

The Caesar cipher

A shift of 4 is modeled as addition by 4 :

$$L = I + 4.$$

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19
23	11	08	26	18	21	15	07	12	22	09	15	04	23
23	11	08	00	18	21	15	07	12	22	09	15	04	23

The Caesar cipher

A shift of 4 is modeled as addition by 4 :

$$L = I + 4.$$

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19
23	11	08	26	18	21	15	07	12	22	09	15	04	23
23	11	08	00	18	21	15	07	12	22	09	15	04	23
X	L	I	A	S	V	P	H	M	W	J	P	E	X

Affine ciphers

Choose two numbers a , b and apply the transformation :

$$L = al + b.$$

Make sure that two different letters will be coded by two different letters.

Affine ciphers

Choose two numbers a , b and apply the transformation :

$$L = aI + b.$$

Make sure that two different letters will be coded by two different letters.

Code a message with the formula $L = 3I + 12$.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19

Affine ciphers

Choose two numbers a , b and apply the transformation :

$$L = aI + b.$$

Make sure that two different letters will be coded by two different letters.

Code a message with the formula $L = 3I + 12$.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19
57	21	12	66	42	51	33	09	24	54	15	33	00	57

Affine ciphers

Choose two numbers a , b and apply the transformation :

$$L = aI + b.$$

Make sure that two different letters will be coded by two different letters.

Code a message with the formula $L = 3I + 12$.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19
57	21	12	66	42	51	33	09	24	54	15	33	00	57
69	33	24	78	54	63	45	21	36	66	27	45	12	69

Affine ciphers

Choose two numbers a , b and apply the transformation :

$$L = aI + b.$$

Make sure that two different letters will be coded by two different letters.

Code a message with the formula $L = 3I + 12$.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19
57	21	12	66	42	51	33	09	24	54	15	33	00	57
69	33	24	78	54	63	45	21	36	66	27	45	12	69
17	07	24	00	02	11	19	21	10	14	01	19	12	17

Affine ciphers

Choose two numbers a , b and apply the transformation :

$$L = aI + b.$$

Make sure that two different letters will be coded by two different letters.

Code a message with the formula $L = 3I + 12$.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
19	07	04	22	14	17	11	03	08	18	05	11	00	19
57	21	12	66	42	51	33	09	24	54	15	33	00	57
69	33	24	78	54	63	45	21	36	66	27	45	12	69
17	07	24	00	02	11	19	21	10	14	01	19	12	17
R	H	Y	A	C	L	T	V	K	O	B	T	M	R

The Vigenère cipher in modular arithmetic

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
R	A	D	I	O	R	A	D	I	O	R	A	D	I

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
R	A	D	I	O	R	A	D	I	O	R	A	D	I
19	07	04	22	14	17	11	03	08	18	05	11	00	19

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
R	A	D	I	O	R	A	D	I	O	R	A	D	I
19	07	04	22	14	17	11	03	08	18	05	11	00	19
17	00	03	08	14	17	00	03	08	14	17	00	03	08

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
R	A	D	I	O	R	A	D	I	O	R	A	D	I
19	07	04	22	14	17	11	03	08	18	05	11	00	19
17	00	03	08	14	17	00	03	08	14	17	00	03	08
36	14	07	30	28	34	11	06	16	32	22	11	03	27

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
R	A	D	I	O	R	A	D	I	O	R	A	D	I
19	07	04	22	14	17	11	03	08	18	05	11	00	19
17	00	03	08	14	17	00	03	08	14	17	00	03	08
36	14	07	30	28	34	11	06	16	32	22	11	03	27
10	14	07	04	02	08	11	06	16	06	22	11	03	01

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
R	A	D	I	O	R	A	D	I	O	R	A	D	I
19	07	04	22	14	17	11	03	08	18	05	11	00	19
17	00	03	08	14	17	00	03	08	14	17	00	03	08
36	14	07	30	28	34	11	06	16	32	22	11	03	27
10	14	07	04	02	08	11	06	16	06	22	11	03	01
K	O	H	E	C	I	L	G	Q	G	W	L	D	B

The Vigenère cipher in modular arithmetic

To apply the key to a message, just add the two numbers together.

t	h	e	w	o	r	l	d	i	s	f	l	a	t
R	A	D	I	O	R	A	D	I	O	R	A	D	I
19	07	04	22	14	17	11	03	08	18	05	11	00	19
17	00	03	08	14	17	00	03	08	14	17	00	03	08
36	14	07	30	28	34	11	06	16	32	22	11	03	27
10	14	07	04	02	08	11	06	16	06	22	11	03	01
K	O	H	E	C	I	L	G	Q	G	W	L	D	B

The true Vigenère cipher

t h e w o r l d i s
R A D I O T H E W O
K H H E C K S H E G

a f l a t d i s c
R L D I S A F L A
R O O I L D N D C