The Vigenère cipher	Season	03
	Episode	14
	Time frame	1 period

Prerequisites : What is a monoalphabetic cipher and how to decipher it.

Objectives :
- Introduce a stronger, polyalphabetic, cipher.
- See the problem it involves for decryption.

Materials :
- *Text ciphered with a Vigenère square, along with its frequency analysis.*
- *Lesson.*
- *Tabula recta.*
- *Sentences to encipher.*
- *Beamer.*

1 – A new cipher text — 20 min

A cipher text is shown to the class, along with its frequency analysis. The problems that this cipher presents are highlighted, mainly the fact that frequency analysis is not working.

2 – The Vigenère cipher — 20 mins

The Vigenère square is described and a example is shown.

3 – Enciphering and deciphering — 20 mins

Each student picks up a sentence and choses a key word to encipher it. It is then sent to someone else in the class, along with the key, to be deciphered.

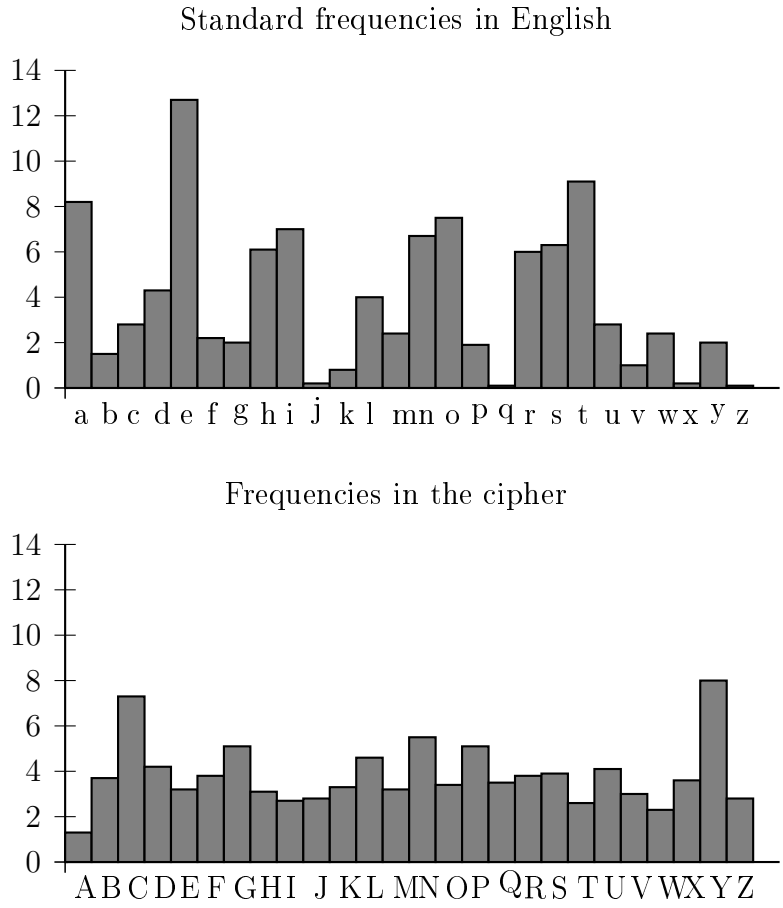
4 – Can you break it ? — 15 mins

Brainstorming session : how to break the Vigenère cipher ?

The cipher

EBGIQ LSVRY ENJON CIUZC NNQPZ PCPQF LHIOB THVRC
XITXG YAEYL NYPDP LNGCY XUPCK THFGM YXGBD FFNIS
YZQBR FHCDC 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 RCHEL
HCUON LLGXR DVWDF PQCCL ZNIYG YAVYC XVCBP LMUDF
PHCWC THUYD LLCCR SUVGY DMVSJ WJQCQ TVNOZ JVGSL
RBWXE FHFOP TNVYR SYYYP WXKXE PHGBY WUPNN LLVSA
FFCBJ JIPDF LNDSR ZZKDI YIYXY DNJOB PUVRU LLTKL
EBGGY DUNPP PXUZY YANOP LHFRC EIQUY XITON ZMKDG
GYCZN CICMF EIVRC DCVEY ECQXY YXJKB NIPMC YNTKR
PXJSQ XCPNM YNJON CIUZC NNQPL ZNDOG YAJKL RYFSL
EBGWM CHKXE LHFWM DNRKP ECEEJ LLNIM YNJON CIUZC
NNQPP PGQFG YACVJ EBGMP FGDVG YAOYP EUTPP ZGCBM
FHFKQ EIPOG YBKCA PFNGY WFYSR SUUZM ZHUYD LLVRC
HITUF LXVKI PHJSK QCXOU PYMCY YXTOB FWGNR SYUZM
ZHVYQ ZGGDF THIVG VYCXY TFHSJ PZQBR FHCDC 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 AJGNR 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 CNCBY 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 ZHUDU LHISL RUNSR EFGBG QZQPY RIPIY
YXUKU DYXOP LFQPR SYYKP OYPCU LNERG YAJSK EBTYS
RBVRC MUTC

Letter frequencies



Analysis

What we notice

- No letter has a frequency less than 1.3%, which is inconsistant with the letter frequencies in English.
- No letter has a frequency more than 10%, so there's no obvious candidate for e. It could be C' or Y, but these two letters could just as well be a, h, i, m, o, r, s, t.
- The histogram doesn't look at all like the standard histogram.

What we can conclude

- The language used could be something else then English, but
  - ◇ we know that the original text was in English ;
  - ◇ no language has such standard letter frequency histogram.
- It's obviously not a simple Caesar Cipher.
- It doesn't seem to be a monoalphabetic substitution cipher.
- A simple frequency analysis is not enough to break it.

History and concept

The Vigenère cipher was first described by Giovan Battista Bellaso in a book published in 1553. It is also known as "Le Chiffre Indéchiffrable", as it seemed for a long time that it was unbreakable. In the 19th century, it was mistakenly attributed to Blaise de Vigenère, a French diplomat and cryptographer from the 16th century. Vigenère did not invent the so-called Vigenère cipher, but he did devise a stronger autokey based on the same table.

Messages are encrypted with the help of a tabula recta, also called Vigenère square, or Vigenère table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.

	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

At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

Plain text : The world is a flat disk. **Code word :** RADIO

Encryption process :

- The first letter is enciphered using the line of the letter R : t is coded into K.
- For the second letter, we use the line of the letter A : h is coded into H.
- For the third letter, we use the line of the letter D : e is coded into H.
- For the fourth letter, we use the line of the letter I : w is coded into E.
- For the fifth letter, we use the line of the letter O : o is coded into C.
- For the sixth letter, we use the line of the letter R : r is coded into I.
- For the seventh letter, we use the line of the letter A : l is coded into L.
- And so on...

It's interesting to notice that the letters h and e have both been enciphered into H ! So the most common letter in English has been enciphered with the same letter as another one, much less common. On another hand, another e in the text may not be enciphered into H.

Spaces and punctuation marks are normally not considered before encryption, and the plain text may be given in groups of 5 letters, to make decryption even harder, as words of one or two letters are easy to spot in English.

Below is a practical way to present this process, with the cipher text in the last row.

t	h	e	w	o	r	l	d	i	s	a	f	l	a	t	d	i	s	c
R	A	D	I	O	R	A	D	I	O	R	A	D	I	O	R	A	D	I
K	H	H	E	C	I	L	G	Q	G	R	F	O	I	H	U	I	V	S

How to decipher a message

To decipher a message encrypted with this method, you need to know the key. Write down the encrypted message and, below, repeat the key word as many times as needed. In a third row, we will write he deciphered message. The table is the same as the one used for encryption, but *upside down*.

K	H	H	E	C	I	L	G	Q	G	R	F	O	I	H	U	I	V	S
R	A	D	I	O	R	A	D	I	O	R	A	D	I	O	R	A	D	I
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?

To decode the first letter, look up in the tabula recta the letter K in the row R. You find the letter t. For the second letter, look up the letter H in the row A. You find the letter h, and so on.

A mathematical view

The Vigenère cipher can be implemented easily using numbers instead of letters and *modular arithmetic*.

In modular arithmetic, we only consider positive integers stricly lower than a given number, called the *modulus*. For example, if the modulus is 26, we will only use the integers from 0 to 25. Any whole number n is *congruent* to one of these integers : the remainder of the division of n by the modulus. For example, if we divide 47 by 26, the remainder is 21, as $47 = 1 \times 26 + 21$. We say that 47 and 21 are congruent, and write

$$47 \equiv 21 \ [26].$$

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	a	f	l	a	t	d	i	s	c
19	07	04	22	14	17	11	03	08	18	00	05	11	00	19	03	08	18	10

The key is also written as a string of numbers : RADIO becomes 17 00 03 08 14.

To encipher the message, write the numerical version in a table and, in a second row, write down the numerical key repeatedly, as we did previously with the alphabetical messages. Then, is a third row, simply add the numbers in each column, reducing the results modulo 26.

19	07	04	22	14	17	11	03	08	18	00	05	11	00	19	03	08	18	10
17	00	03	08	14	17	00	03	08	14	17	00	03	08	14	17	00	03	08
10	07	07	04	02	08	11	06	16	06	17	05	14	08	07	20	08	21	18

The numerical encypted message could then be turned back into an alphabetical one, but it's useless. Sending a numerical message is just as secure as an alphabetical one.

Advantages and drawbacks

The so-called Vigenère cipher offered a higher level of secrecy than the monoalphabetic ciphers. It was considered unbreakable for a few centuries, as straightforward frequency analysis didn't work on it. Still, it was never widely used because it was too time-consuming to implement. When a lot of messages had to be sent in a short time, for example during a war, armies could not afford the time needed to encipher and decipher.

The Vigenère cipher was in fact broken by some cryptanalists as soon as in the 16th century. Around 1830, Charles Babbage broke the so-called Vigenère cipher as well as the stronger auto-key cipher actually devised by Vigenère. As his discovery was kept secret by the British government, it was mistakenly attributed to Friedrich Kasiski, a Prussian infantry officer, who made the same discovery some years after Babbage.

It still took a large amount of time, intuition and luck to break it, so it was still a quite secure system. With the advent of computers, breaking a Vigenère cipher has become much easier and quicker. It's interesting to note that Charles Babbage, one of the first to break the Vigenère cipher, also introduced the main concepts that would lead to computers.

An important weakness of this cipher is the repetition of the key. This creates a periodic use of the same monoalphabetic cipher. A soon as the length of the key is known, the cipher text can be divided according to the period, and each group of letters treated with frequency analysis. This is the basis of the method to break the Vigenère cipher.

The *real* Vigenère auto-key cipher

VIGENÈRE DIDN'T INVENT THE CIPHER THAT BEARS HIS NAME, but he did devise a stronger one, with no repetition of the key, and therefore no periodicity in the encryptement, making it really immune to frequency analysis.

The trick is to use the key only to encrypt the first few letters of the message, and then to use the message itself, hence the name *auto-key*.

Using the same example as before, we will encrypt the first five letters using the letters of the key RADIO, and will then use the letters of the message itself, as shown in the following table :

t	h	e	w	o	r	l	d	i	s	a	f	l	a	t	d	i	s	c
R	A	D	I	O	T	H	E	W	O	R	L	D	I	S	A	F	L	A
K	H	H	E	C	K	S	H	E	G	R	O	O	I	L	D	N	D	C

To decrypt the cipher message, we must first use the letters of the key. When we reach the end of the key, we use the the letters of the plain text, in the same order as they were decrypted.

The Vigenère cipher

Season 03
Episode 14
Document 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

Document 1 Sentences to encipher

A mathematician is a machine for turning coffee into theorems.
(Paul Erdös)

Perfect numbers like perfect men are very rare. (René Descartes)

Mathematicians are born, not made. (Henri Poincaré)

It is impossible to be a mathematician without being a poet in soul.
(Sofia Kovalevskaya)

The search for truth is more precious than its possession. (Albert Einstein)

If there is a God, he's a great mathematician. (Paul Dirac)

Math is like love – a simple idea but it can get complicated. (R. Drabek)

God made the integers ; all the rest is the work of man.
(Leopold Kronecker)

There are three types of people in this world : Those who can count, and those who can't. (Anonymous)

The essence of mathematics is not to make simple things complicated, but to make complicated things simple. (S. Gudder)

The human mind has never invented a labor-saving machine equal to algebra. (Anonymous)

Go down deep enough into anything and you will find mathematics.
(Dean Schlicter)

Mathematics is as much an aspect of culture as it is a collection of algorithms. (Carl Boyer)

Music is the pleasure the human mind experiences from counting without being aware that it is counting. (Gottfried Leibniz)

Mathematics is the supreme judge ; from its decisions there is no appeal. (Tobias Dantzig)

I used to love mathematics for its own sake, and I still do, because it allows for no hypocrisy and no vagueness. (Stendhal)

If there is a God, he's a great mathematician. (Paul Dirac)

Philosophy is a game with objectives and no rules. Mathematics is a game with rules and no objectives. (Anonymous)

Mathematics consists in proving the most obvious thing
in the least obvious way. (George Polya)

Obvious is the most dangerous word in mathematics. (E.T. Bell)

Arithmetic is being able to count up to twenty
without taking off your shoes. (Mickey Mouse)

I have hardly ever known a mathematician who was capable of reasoning. (Plato)

You know we all became mathematicians for the same reason :
we were lazy. (Max Rosenlicht)

These days, even the most pure and abstract mathematics is in danger to be applied. (Anonymous)

What is a rigorous definition of rigor ? (Anonymous)

Only two things are infinite, the universe and human stupidity, and I'm not sure about the former. (Albert Einstein)

There are 10 kinds of people in the world, those who understand binary math, and those who don't. (Anonymous)

Statistics : the mathematical theory of ignorance. (Morris Kline)

Most people use statistics the way a drunk uses a lamp post, more for support than enlightenment. (Anonymous)

Geometry is the science of correct reasoning on incorrect figures. (George Polya)

Without geometry life is pointless. (Anonymous)

Inspiration is needed in geometry, just as much as in poetry. (Aleksandr Pushkin)

Calculus has its limits. (Anonymous)

Mathematics is the science which uses easy words for hard ideas. (Anonymous)

A mathematician who is not also a poet will never be a complete mathematician. (Karl Weierstrass)

To ask the right question is harder than to answer it. (Georg Cantor)
