BREAKING THE CODE ! (part 1)

Faire lire le début de la fiche. Demander aux élèves de dire oralement ce qu'ils ont compris.
Présenter le codage de César et les faire déchiffrer. On peut utiliser un système de double disque (voir annexe). On peut utiliser le site suivant pour vérifier :
http://www.counton.org/explorer/codebreaking/caesar-cipher.php

Pour déchiffrer quand on connaît le décalage on utilise les deux disques, reliés entre eux par une attache parisienne. Sinon on peut utiliser des bandelettes (on aligne les lettres du message et on regarde si cela donne un mot connu sur une autre ligne).
Par groupe, les élèves écrivent un message codé et le transmettent à un autre groupe qui doit le déchiffrer sans connaître le décalage choisi (avec les bandelettes). → prévoir des enveloppes et des feuilles pour faire passer le message.

Présenter le second codage (affine), les faire coder leur nom. Essayer plusieurs codages.
Les faire déchiffrer.
C'est plus facile quand la table est complétée. On peut ne pas donner la table (juste quelques exemples) pour compliquer.

Pour le codage affine (ax + b) il faut que a et 26 soient premiers entre eux (ce qui assure que deux lettres différentes sont codées par deux nombres différents).
On pourra utiliser le tableur pour trouver la table qui permet de réaliser le codage.

Par groupe, les élèves écrivent un message codé et le transmettent à un autre groupe qui doit le déchiffrer.
→ prévoir des enveloppes et des feuilles pour faire passer le message.
On peut compliquer en donnant avant à chaque groupe un codage (multiplier par 5 puis retirer 1, etc.) ou bien les laisser choisir le codage affine qu'ils veulent… dans ce cas certains codages ne fonctionneront pas. On pourra alors discuter de ce problème et essayer de le comprendre avec les élèves.

Après plusieurs séances, un élève (ou un binôme) peut présenter un codage et son décryptage à la classe en 5 min.

Pour aborder le thème du codage :
http://www.simonsingh.net/media/online-videos/cryptography/the-science-of-secrecy-going-public/
(une vidéo de Simon Singh)

Pour montrer des codes utilisés (navigation, braille…) :
http://www.quadibloc.com/crypto/intro.htm

BREAKING THE CODE ! (part 1)

When you think of ***spies and secret agents***, you might think of lots of things; nifty gadgets, foreign travel, dangerous missiles, fast cars and being shaken but not stirred. You probably wouldn't think of mathematics. But you should.
Cracking codes and unravelling the true meaning of secret messages involves loads of maths, from simple addition and subtraction, to data handling and logical thinking.
In fact, ***some of the most famous code breakers in history have been mathematicians*** who have been able to use quite simple maths to uncovered plots, identify traitors and influence battles.

The Roman Geezer

Let me give you an example. Nearly 2000 years ago, Julius Caesar was busy taking over the world, invading countries to increase the size of the Roman Empire. He needed a way of communicating his battle plans and tactics to everyone on his side without the enemy finding out. So ***Caesar would write messages to his generals in code***.
Instead of writing the letter 'A', he would write the letter that comes three places further on in the alphabet, the letter 'D'. Instead of a 'B', he would write an 'E', instead of a 'C', he would write an 'F' and so on. When he got to the end of the alphabet, however, he would have to go right back to the beginning, so instead of an 'X', he would write an 'A', instead of a 'Y', he'd write a 'B' and instead of 'Z', he'd write a 'C'.

Complete the table to find out how Caesar would encode the following message:

Caesar's message	**A**	**T**	**T**	**A**	**C**	**K**		**A**	**T**		**D**	**A**	**W**	**N**
	B	U			D	L								
	C	V			E	M								
Coded message	D	W	W	D	F	N		D	W		G	D	Z	Q

When Caesar's generals came ***to decipher the messages***, they knew that all they had to do was go back three places in the alphabet.
Have a go at trying to work out these messages which could have been sent by Caesar or his generals:

HQHPB DSSURDFKLQJ	WKLUWB GHDG	UHWUHDW WR IRUHVW
ENEMY APPROACHING	THIRTY DEAD	RETREAT TO FOREST

Easy as 1, 2, 3
This all seems very clever, but so far it's all been letters and no numbers. So where's the maths? The maths comes if you think of the letters as numbers from 0 to 25 with A being 0, B being 1, C being 2 etc. Then encoding, shifting the alphabet forward three places, is the same as adding three to your starting number :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For example, encoding the letter 'A' is 0+3=3, which is a 'D'.
Coding 'I' is: 8 + 3=11, which is 'L'.
However, you do have to be careful when you get to the end of the alphabet, because there is no letter number 26, so you have to go back to number 0. In maths we call this 'MOD 26', instead of writing 26, we go back to 0.

Have a go at coding your name by adding 3 to every letter : ....

Then have a go at coding your name by shifting the alphabet forward by more places by adding greater numbers eg adding 5... ...then adding 10.

....

Then have a go at decoding. If your letters are numbers and encoding is addition, then decoding is subtraction, so if you've coded a message by adding 5, you will have to decode the message by subtracting 5.

HTSLWFYZQFYNTSX

CONGRATULATIONS

Let’s try another code

Let’s use a more difficult operation to encode a message. For instance, multiply each number by 3 and then add 2.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25
C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

Find the encoded message for : MATHS ARE EASY !

MCHXD CBO OCDW

BREAKING THE CODE ! (part 2)

Follow the explanations to make a key to Caesar’s code :

“ Draw a circle with a radius of 6cm. Cut it off . With the same center, draw a circle with a radius of 5 cm. Divide the side of this disc into 26 equal parts (1 for each letter). Write the alphabet all around this disc.
Do it again with a smaller disc : the first with a radius of 5 cm and the second with a radius of 4 cm. Write the alphabet all around.
Fasten the two centers with a brass fastener.”

Give each group a message to decipher.
Write it and choose the shifting of the alphabet (ex : H → A):
http://www.counton.org/explorer/codebreaking/caesar-cipher.php

“Here is a message coded by Caesar : can you deciffer it ?

MABL VHWX BL MHH XTLR MH UKXTD → *This code is too easy to break*

PX ATOX MH YBGW T GXP PTR HY VHWBGZ → *We have to find a new way of coding* ”

Ancient Runes
Let the students look for how it works…
Each drawing give the position of the letter in the table :
W → 5th row and 3rd column
A → 1st row and 1st column *Be careful : Row first and Column in second position !*
S → 4th row and 4th column
So the message to decipher is : LOOK UNDER THE STONE
Let the students write a message to you !

BREAKING THE CODE ! (part 3)

Treason!

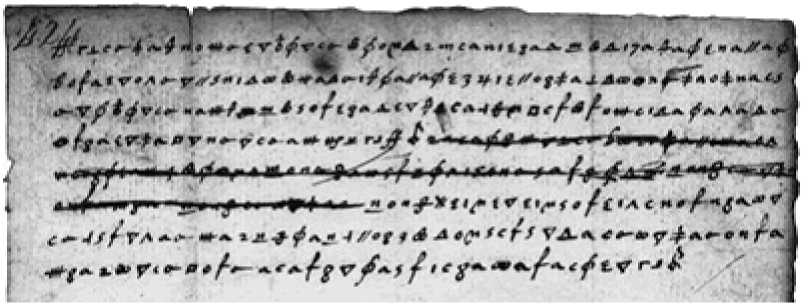
If you've got the hang of coding messages by shifting the alphabet forward, then you might have realised that it is actually pretty simple to crack this type of code. It can easily be done just ***by trial and error****. An enemy code breaker would only have to try out* ***25 different possible shifts*** *before they were able to read your messages, which means that your messages wouldn't be secret for very long.*
So, what about coding messages another way ? Instead of writing a letter, we could write ***a symbol****, or draw a picture. Instead of an 'A' we could write *, instead of a 'B' write + etc. For a long time, people thought this type of code would* ***be really hard to crack****. It would take the enemy far too long to figure out what letter of the alphabet each symbol stood for just by trying all the possible combinations of letters and symbols. There are 400 million billion billion possible combinations!*

This type of code was used by Mary Queen of Scots when she was plotting against Elizabeth the First. Mary wanted to kill Elizabeth so that she herself could become Queen of England and was sending coded messages of this sort to her co-conspirator Anthony Babington.

Elisabeth The First

Mary Queen of Scots

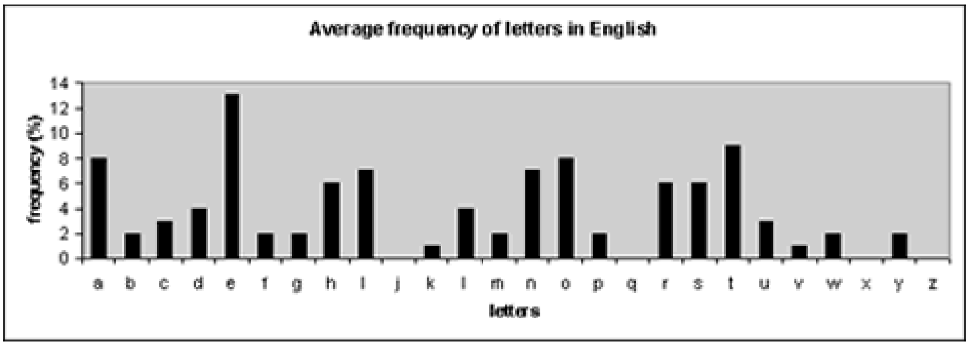
Unfortunately for Mary, there is a very simple way of cracking this code that doesn't involve trial and error, but which does involve… surprise… surprise... **maths** !



Letter sent by Mary Queen of Scots to her co-conspirator Anthony Babington. Every symbol stands for a letter of the alphabet.

Letters in a language are pretty unusual because some get used more often than other letters. An easy experiment you can do to test this out is to get everyone in your class to raise their hand if they have the letter 'E' in their name. Then get all those with a 'Z' to raise their hand, then a 'Q', then an 'A'. You will probably find that 'E' and 'A' are more common than 'Z' and 'Q'.

The graph below shows the average frequency of letters in English. To compile the information, people looked through thousands and thousands of books, magazines and newspapers, and counted the number of times each letter came up.



In English, which is the most commonly used letter ? E

In any piece of writing, on average, how often do we use E ? 13 %

Which is the second most common letter ? T and the third most commonly used letter ? A

Let’s complete the table below : ***Average Frequency of letters in English***

Letters	E	T	A, O	I, N	H, R, S	D, L	C, U	B, F, G, M, P, W, Y	K, V	J, Q, X, Z
Frequency (%)	13	9	8	7	6	4	3	2	1	0

Lettre	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
Indice de fréquence en Anglais	8.08	1.67	3.18	3.99	**12.56**	2.17	1.80	5.27	7.24	0.14	0.63	4.04	2.60	7.38	7.47	1.91	0.09	6.42	6.59	9.15	2.79	1.00	1,89	0,21	1,65	0,07

This information that can help you to crack codes.

All Elizabeth the First's Spy-Master had to do to crack Mary's code, was to look through the coded message and count the number of times each symbol came up. The symbol that came up the most would probably stand for the letter 'E'.

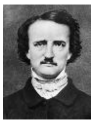
When you crack codes like this, by looking for the most common letter, it's called **'frequency analysis'**, and it was this clever method of cracking codes that resulted in Mary having her head cut off !

J’ai montré ensuite aux élèves les répétitions courantes en anglais sur le site :
http://www.counton.org/explorer/codebreaking/frequency-analysis.php

Ensuite j’ai montré (10 min) une video de Simon Singh :
http://simonsingh.net/media/online-videos/cryptography/the-science-of-secrecy-going-public/
cela parle d’une nouvelle façon de crypter les messages découverte dans les années 70, les chercheurs expliquent leur découverte.

BREAKING THE CODE ! (part 4)

Let us follow the story of <u>*The Gold Bug*</u> by Edgar Allan Poe.



Here is the message found on a parchment :

53‡‡+305))6*;4826)4‡.)4‡);806*;48+8¶60))85;1‡(;:‡*8
+83(88)5*+;46(;88*96*?;8)*‡(;485);5*+2:*‡(;4956*2(5*—
4)8¶8*;4069285);)6+8)4‡‡;1(‡9;48081;8:8‡1;48+85;4)485
+528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

Cracking this code will allow the narrator to find a treasure ! Let's follow him to decipher the enigma…

1st step : Guessing the language in which the enigma is written → ***English*** for sure !

2nd step : Find all the characters used in the message. Count them all and find their frequency in it.

Character	8	;	4	‡	*	5	6	(	+	0	9	:	?	¶	—
				)					1		2	3			.
Times	33	26	19	16	13	12	11	10	8	6	5	4	3	2	1

As the most frequent letter in English is E, we shall guess that '8' represents E.
To verify this supposition, let's observe that the '8' is seen often in couples (for E is doubled with great frequency in English).

3rd step : The most frequent word in English is THE. Therefore find a repetition of three characters in the same order, the last of them being '8' : ; 4 8

Now you can guess which symbol represents T, and the one representing H.
Write it in the table and replace all these symbols in the message.

4th step : Let's find a new word in the message. Look at this part of the message THE T(EETH . As we can't find any letter to complete the word *t..eeth*,we shall think that the last 'th' is the beginning of the following word. Can you find the missing letter in *t..ee* ? Try all the letters !
Now you can guess which letter stands for (.

5th step : Let the pupils work by group and try to deciffer the message. Let them argue in their group. Each group can present his findings to the others.

A way of deciphering (according to <u>*The Gold Bug*</u>) :
We now can read : "*the tree th……..h the*" with three letters missing. Which word do you think it is ? through.
So you can guess which letter stands for ‡, ? and 3.
At the beginning of the second line, we can see : +EGREE Guess the letter which is missing.
Now you know which letter stands for +.
Fours letters beyond this word, we notice the combination : TH6RTEE* which suggests the word '*th...rtee..*'.
We have found two more letters !
At the beginning of the message we observe : 5GOOD , this means probably two words : '.. good'. Which letter do you think 5 stands for ? A
Now we have guessed most of the letters.
Look at those parts of the message : THIRTEEN 9INUTE) 1ROM FORT : SE¶ENTH
Now complete the following table :

Characters	8	;	4	‡	)	*	5	6	(	+	1	0	9	2	:	3	?	¶	—	.
Letters	E	T	H	O	S	N	A	I	R	D	F	L	M	B	Y	G	U	V	C	P

Now you can decipher the message :

53‡‡+305))6*;4826)4‡.)4‡);806*;48+8¶60))85;1‡(;:‡*8
A GOOD GLASS IN THE BISHOP’S HOSTEL IN THE DEVIL’S SEAT FORTY-ONE

+83(88)5*+;46(;88*96*?;8)*‡(;485);5*+2:*‡(;4956*2(5*—
DEGREES AND THIRTEEN MINUTES NORTH EAST AND BY NORTH MAIN BRANC

4)8¶8*;4069285);)6+8)4‡‡;1(‡9;48081;8:8‡1;48+85;4)485
H SEVENTH LIMB EAST SIDE SHOOT FROM THE LEFT EYE OF THE DEATH’S HEA

+528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;
D A BEE-LINE FROM THE TREE TROUGH THE SHOT FIFTY FEET OUT.

On pourra mettre en ligne sur e-lyco des informations complémentaires :

- extrait original en anglais
- traduction en français
- lien aux explications données sur wikipedia

Printed from : *http://fr.wikipedia.org/wiki/Le_Scarab%C3%A9e_d%27or*

Le Scarabée d'or (*The Gold Bug*) est une nouvelle d'Edgar Allan Poe, parue en juin 1843 dans le journal de Philadelphie *Dollar Newspaper*.

Poe a gagné un concours organisé par le journal et reçu un prix de 100 dollars, ce qui représente le montant le plus élevé que l'écrivain ait touché pour une nouvelle publiée[1]. C'est également le texte le plus largement lu du vivant de l'auteur[2].

La nouvelle popularisa la cryptographie auprès du grand public tout en établissant la réputation de cryptographe hors pair de l'écrivain aux yeux de ses contemporains[3]. Elle a été reprise dans de nombreux journaux et publications et fut traduite en français par Charles Baudelaire et publiée dans le recueil des *Histoires extraordinaires*.

Dans cette nouvelle, William Legrand, trouve un magnifique scarabée doré sur l'île Sullivan en Caroline du Sud où ce fils de bonne famille déchu est venu fuir la misère. Apparemment en or massif, le scarabée va tourmenter son esprit jusqu'à l'obsession.

Accompagné par son fidèle serviteur Jupiter et suivi par son ami narrateur, Legrand se lance, après de multiples péripéties engendrées par la découverte du scarabée, à la poursuite du trésor du célèbre Cap'tain Kidd dans une étrange chasse préfigurant *L'Île au trésor* de Stevenson. La découverte d'un message mystérieux sur une esquisse griffonnée sur un vieux parchemin engendre pour les protagonistes une séries de rebondissements qui mêle suspense et cryptologie.

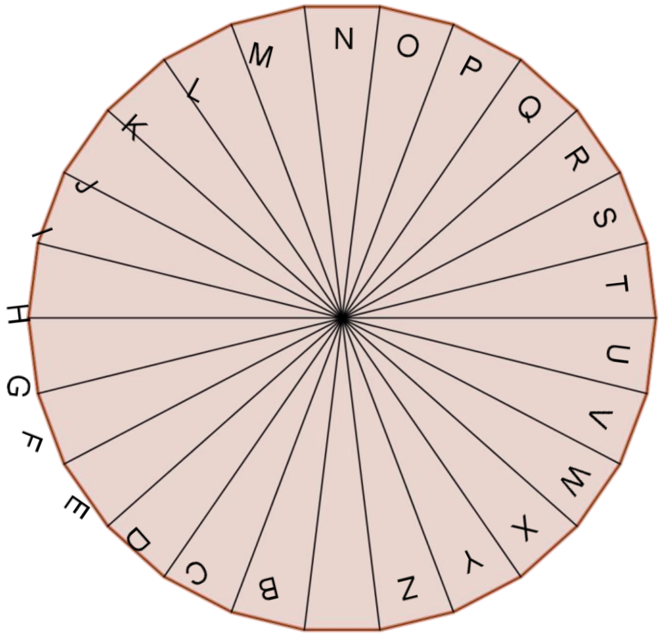
http://fr.wikipedia.org/wiki/La_cryptologie_dans_le_scarab%C3%A9e_d%27or

Commentaires :

Cette séquence a été testée en 3ème et en 2de. La première partie peut être menée sur une ou deux séances.

On pourra présenter d'autres types de codages : pigpen, vigenère

(voir : http://www.counton.org/explorer/codebreaking/index.php) codes barres, codages RSA... selon le niveau des élèves.



Impossible d'afficher l'image.

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

V	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**
W	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**	**W**
X	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Y	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
Z	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**	**Z**