Académie de Toulouse – classes européennes mathématiques-anglais – session 2013

Sujet n°24

You can write on the subject paper but don't forget to give back the examination paper at the end of the test

CIPHER

The Caesar Cipher, named for Julius Caesar who used it in his military campaigns, is one of the simplest and easiest substitution ciphers in the world.

Julius Caesar used a substitution cipher with a left shift of three letters in his military campaigns. While there are a few older ciphers in the world, this was the first recorded use of any encryption technique. It not only helped Caesar in his military campaigns, but it left a lasting influence on cryptology. Among the public, the Caesar cipher is still the most popular method of encryption in use.

Specific techniques to crack encoded messages were not invented until the 9th century. Two of these techniques are as simple as the cipher itself. The first involves frequency analysis. One can break a substitution cipher by matching the letters that appear most frequently in the message with the letters that appear most frequently in the language.
For english, the table of relative frequencies (in %) is just given below :

a	b	c	d	e	f	g	h	i	j	k	l	m
8.05	1.62	3.2	3.65	12.31	2.28	1.61	5.14	7.18	0.1	0.52	4.03	2.25
n	o	p	q	r	s	t	u	v	w	x	y	z
7.19	7.94	2.29	0.2	6.03	6.59	9.59	3.1	0.93	2.03	0.2	1.88	0.09

This is an encrypted message using a shift of some letters you have to find and then decrypt !

Encrypted message :
OCZ HVOCZHVODXVG XJINOVIO KD DN PIYZM OCMZVO AMJH V BMJPK JA YZOMVXOJMN RCJ RDGG WZ HVMFDIB OVP YVT JI OPZNYVT ORZIOT-ZDBCO JA EPIZ.

1. Fill in the table to find frequencies of each encrypted letters.

A	B	C	D	E	F	G	H	I	J	K	L	M
3	3	5	6	1	1	3	4	7	8		0	7
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4		5	0	3		3	0	11	1	3	4	10

2. What are the five most frequent letters in the coded message ?
3. Using the table of relative frequencies previously given, what should be the most common letters in the English plain text ?
4. Try to crack the code and find the hidden « mathematical » message.

Tip : here the most frequent letter is not E but …
NB : plain text = message décrypté ou message avant le codage