

**BACCALAURÉAT GENERAL
EPREUVE SPECIFIQUE DES SECTIONS EUROPENNES
MATHEMATIQUES – ANGLAIS**

SUJET 3

**Information security and privacy
Thème : cryptographie**

Sujet comportant deux pages. L'usage de tout modèle de calculatrice, avec ou sans mode examen est autorisé.

Terrorism has cost many innocent lives so far this century, and mathematics has a role to play in stopping terrorist acts before they happen. Terrorists are able to commit these acts because they can plan and communicate in secret. Government intelligence agencies all over the world try to intercept terrorist computer e-mails and decode them.

- 5 All encryption is based on a key, which is a word or a number. These keys give the information needed to decode or decrypt the message. The keys currently most commonly used to encrypt e-mails are numbers that are the products of two prime numbers. To crack the code, you have to work out the original two prime numbers. When the numbers involved are very large, this is almost impossible to do because there are so
- 10 many possibilities.

Governments are hoping that in the future quantum computers that can process calculations simultaneously will be able to find the two prime numbers quickly and enable them to crack the terrorists' codes. Breaking an encryption code is called decryption.

Source : <http://hi.com.au/mathszonesas/pdf/MZQSA01b.pdf>

1. Explain what the text deals with and comment on it.

Exercise

Here is a CODING table for the alphabet.

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

X	Y	Z	Space	!	?	@
24	25	26	27	28	29	30

To code a message, you would simply replace the letters of the message with the numbers from the table. Computers use a system like this to capture text as numeric data.

Encryption changes the coding of the letters according to a particular rule; hopefully the rule is only known by the person intended to receive the message.

For instance with the rule $f(x)=4x+15$ the letter 'A' becomes '19'.

Answer the following questions

1) Encrypt the text "LINEAR CIPHER" with the encrypting function $f(x) = x + 3$

2) Here is a secret message from me.

13 49 46 25 58 7 64 67 40 7 64 31 49 46

a) Assuming that the first letter of the plaintext is "C" and the last one is "N", find the ENCRYPTING FUNCTION.

b) Find a method to decrypt the message.

Helpful tip: the encoding function is a linear function.