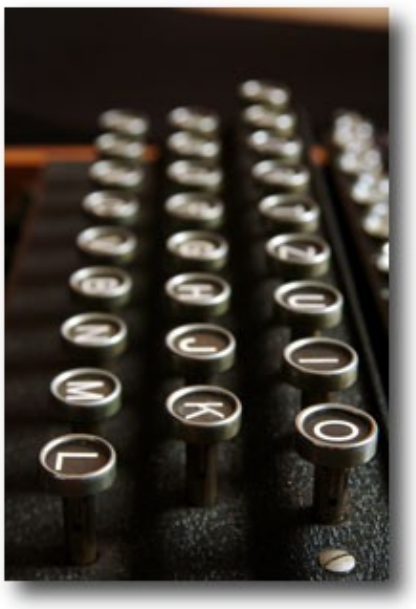
June 2008
Regulars

Puzzle page

The rail fence cipher



The Enigma machine was used by the Germans to encode messages in WW2.

This puzzle has been kindly donated to us by our sister project Enigma. Enigma travels the nation bringing a genuine WW2 Enigma machine into schools. It also publishes a code of the week on its website, giving you

the chance to win a signed copy of Simon Singh's Code Book. The Enigma website also has all the information you need to invite Enigma to your school. But now, let's get codebreaking.

The rail fence cipher involves writing messages so that alternate letters are written on separate upper and lower lines. To create the final encrypted message, the sequence of letters on the upper line is then followed by the sequence on the lower line. The code maker improves the security of the cipher by choosing more than two lines to encrypt the message.

Take the plaintext "pancakes for breakfast" for example. It can be enciphered using a shift of two by writing it as follows:

p	n	a	e	f		r	td>	td>	td>	td>
a	c	k	s	td>	td>	td>	td>	td>		t

The ciphertext is then created by reading across the rows as follows:

pnaefrra fsa cksobekat

In this case, a shift of two, in other words two lines, was used. In order to decipher it, the ciphertext must be split into two parts. If the shift was three, then the ciphertext must be split into three lines, four lines for a shift of four etc.

Here is your cypher text. You'll have to work out for yourself which shift was used. Happy puzzling!

TURNITYLNTHASMTITLRBAQEC.SONEASEBEWBMSASEB'BNODOENNIVH
MTTXRBLTIELTBHSAIOUSUWHITNURTQZEEOEBANODISEBLIMTTTXEEBW
YIURI.SSLNEANPNMTAAHITHLMTIUETNCNENULRCCCEVNOHWYMSNEESS
LIAITMEURT'ADEHSRISIEYBHSEDWTUURDNVUKUASENRAESO.

You can find out more about the rail fence cypher on Simon Singh's website.

The solution

The shift used in this text was 4, so the 212 characters in the cypher text must be split into four lines of 53 characters each:

TURNITYLNTHASMTITLRBAQEC.SONEASEBEWBMSASEB'BNODOENNIV
HMTTXRBLTIELTBHSAIOUSUWHITNURTQZEEOEBANODISEBLIMTTTXE
EBWYIURI.SSLNEANPNMTAAHITHLMTIUETNCNENULRCCCEVNOHWYS
NEESSLIAITMEURT'ADEHSRISIEYBHSEDWTUURDNVUKUASENRAESO.

Reading the text column−wise decodes the message as:

The number twenty six is truly brilliant. It is the smallest number that isn't a palindrome but has a square which is. It is the only number that is squeezed between two cube numbers and an unsolved rubicks cube can be solved in no more than twenty six moves.

Back to main puzzle page

Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the NRICH and MOTIVATE sites.