



© 1997–2004, Millennium Mathematics Project, University of Cambridge.

Permission is granted to print and copy this page on paper for non-commercial use. For other uses, including electronic redistribution, please contact us.

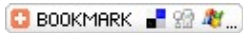
March 2005

Features



Exploring the Enigma

by Claire Ellis



Cryptography terminology

Plaintext: Everyday language; e.g. "This is plaintext"

Ciphertext: Enciphered language; e.g. "rgua ua xuogwerwzr"

A **code** is a system of secret communication in which each word in a message is replaced with another word, letter, sentence or symbol. For example:

Plaintext:	British	won (the)	battle (at Alam Halfa)
Ciphertext:	Dog	ate	rabbit

A **cipher** is a system of secret communication in which each letter in a message is replaced with another letter, word sentence or symbol. For example:

Plaintext:	s	h	i	p	s	s	a	i	l	e	d	t	o	d	a	y
Ciphertext:	r	g	h	o	r	r	z	h	k	d	c	s	n	c	z	x

There are two parts to every cipher, and in order to decipher messages you must know both parts:

$$\text{Cipher} = \text{Algorithm} + \text{Key},$$

Exploring the Enigma

where an "algorithm" is a general method of encryption, for example, "swap every letter for a symbol", or "jumble up all the letters in a word", and a "key" is the particular way a message has been enciphered that time, for example, "replace A by \$, B by or "move the last letter of every word to the front".

[Back to main article](#)



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