POLYBIUS

Polybius was the name of the Greek who invented a system of converting alphabetic characters into numeric characters.

"*Greece would not have fallen had it obeyed Polybius in everything, and when Greece did meet disaster, its only help came from him*" Pausanias, 8.37.2, Inscription on the Temple of Despoina near Arakesion.

It was devised to enable messages to be easily signalled using torches.

	1.	2.	3.	4.	5.
1.	a	f	l	q	v
2.	b	g	m	r	x
3.	c	h	n	s	y
4.	d	i	o	t	z
5.	e	k	p	u	

Each letter may be represented by two numbers by looking up the row the letter is in and the column. For instance h=23 and r=42.

The idea was that a message may be transmitted by holding different combinations of torches in each hand. The chequerboard has other important characteristics, namely the reduction in the number of different characters, the conversion to numbers and the reduction of a symbol into two parts which are separately manipulable. As such chequerboards form the basis for many more ciphers.

Varients of this idea are used to convert a single character into units which may be manipulated seperately, this can lead to some very strong ciphers, for instance the Adfgvx cipher.

[Excerpt from "Classical Cryptography" by ThinkQuest Team 27158]