The mathematics of encryption grids

1 *To the 500th anniversary of the Girolamo Cardano.* [1]

1 Introduction

Figure 0

The 16th century had just begun when Girolamo Cardano (1501–1576), Italian mathematician, physicist, philosopher, physician (a real renaissance scholar) was born. His 1545 publication titled *Ars Magna* contains general formulae for the roots of the cubic equation. Today, it is these formulae that Cardan's name is most often associated with, though it is still uncertain whether these discoveries were his own.[2]

Very few of us recognize Cardan as one of the most outstanding figures of 16th-century cryptography. This is not so surprising, as it is natural that cryptography should be pursued inconspicuously. The strictly confidential correspondence of kings and warlords used various cipher systems. As the more complicated cipher techniques, and especially the decryption of messages often require advanced mathematical skills, it can be expected that the theoretical background should be established in a large part by famous mathematicians.

Cardan developed a cipher system, then completely unknown, that is now called Cardan's screen. The success of Cardan's encryption screen is best proved by the fact that is was still used 400 years later, in the middle of the 20th century, by the West-German intelligence service (BND = Federal Information Service.)

In this paper, after a short historical overview, we illustrate the principle of Cardan's encryption screen, and then discuss several generalizations and a few mathematical properties of the grid.

Torch telegraphy and interval cipher

Cardan conducted a thorough research of the cipher systems of the past, back to antiquity. He found a text by Polybius, a Greek historian of the 2nd century BC, in which the author describes an interesting and completely unusual technique.

Torch telegraphy by Polybius

Consider the 5 by 5 table in *Figure 1.*

	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	

Figure 1

The sender of the message needs 10 torches, 5 for each hand. He sends the message letter by letter, by holding up as many torches with his left hand as the number of the row, and with his right hand as the number of the column containing the letter to be sent. For example, in the case of the letter „s", he holds 3 torches in his left hand and 4 in his right hand. Polybius was very proud of his method:

„This method was invented by Cleoxenus and Democritus but it was enhanced by me", he wrote.

[1] See *Figure 0*

[2] According to historians, Scipione del Ferro (1465–1526) had found the general solution for cubic equations and showed it to his colleagues. That probably happened around 1515, when mathematical competitions were fashionable in Italy. A colleague of Ferro suggested to Niccolo Tartaglia (1500–1557), a mathematician of great learning, that they should solve cubic equations. Tartaglia solved the equations by the set deadline, but he did not reveal his technique. Cardan asked him so persistently for the method that finally, he confided the solution to Cardan, but he made Cardan swear to secrecy. Cardan broke his word and published the method in his *Ars Magna,* in 1545. A bitter dispute started between Tartaglia and Cardan, and it remains unsettled to this day.