0. ábra

Éppen csak elkezdődött a XVI. század, amikor Girolamo Cardano (1501–1576) olasz matematikus, fizikus, filozófus, orvos, (egyszóval igazi reneszánsz tudós) (*0. ábra*) megszületett. 1545-ben megjelent munkája, az Ars Magna képleteket tartalmaz az általános alakú harmadfokú egyenlet gyökeire. Az utókor számára Cardano nevével általában ezen eredményei kapcsolódnak össze, pedig a mai napig kétséges, hogy ezeket a képleteket valóban ő fedezte-e fel.[1]

Ugyanakkor kevesen ismerik Cardanot mint a XVI. századi kriptográfia egyik legjelentősebb alakját. Ez nem annyira meglepő, hiszen természeténél fogva a kriptográfiát (a titkosírást, vagy rejtjelezést) „zárt ajtók mögött" művelték. Királyok, hadvezérek szigorúan bizalmas levelezését bonyolították különböző módszerekkel titkosított levelekkel. Mivel a bonyolultabb rejtjelezési módszerek és főleg azok megfejtése legtöbbször komoly matematikai ismereteket igényel, így érthető, hogy többnyire neves matematikusok nevéhez fűződik a kriptográfia elméleti alapjainak megteremtése.

Cardano egy akkor egészen új rejtjelezést dolgozott ki, amelyet ma Cardano-rácsnak neveznek. A Cardano-rács sikerét mi sem bizonyítja jobban, mint hogy 400 évvel később, a XX. század közepén, a nyugatnémet hírszerző szerv (BND = Szövetségi Információs Szolgálat) még használta.

A következőkben rövid történeti áttekintés után bemutatjuk a Cardano-rács alapgondolatát, majd annak több irányú általánosítását és néhány matematikai tulajdonságát.

Fáklyatávíró és intervallum rejtjelezés

Cardano behatóan tanulmányozta az előző korok rejtjelezési technikáit egészen az ókorig visszatekintve. Így akadt

[1] A matematika-történészek szerint egy bizonyos Scipione del Ferro (1465–1526) megtalálta az általános alakú harmadfokú egyenlet megoldását, melyet közölt kollégáival. Ez 1515 körül történhetett, amikor Olaszországban gyakran tartottak matematikai versenyeket. Ferro egyik kollégája azt javasolta Niccolo Tartaglia (1500–1557) akkori nagyképzettségű matematikusnak, hogy oldjanak meg harmadfokú egyenleteket. Tartaglia a kijelölt határidő előtt megoldotta az egyenleteket, módszerét azonban titokban tartotta. Cardano kitartó érdeklődésére elmondta neki a megoldást, de megeskette, hogy hallgat róla. Cardano azonban nem tartotta meg esküjét és 1545-ben az Ars Magna-ban ismertette a harmadfokú egyenlet megoldásának módszerét. Így kezdődött a heves, ádáz vita Tartaglia és Cardano között, amelynek végére a matematika-történet a mai napig nem tudott pontot tenni.

rá az i.e. II. században élt Polübiosz nevű görög történész leírására, amelyben egy érdekes és az addig megszokottól merőben különböző eljárást ír le.

Polübiosz fáklyatávírója

Készítsük el az *1. ábrán* látható 5 sorból és 5 oszlopból álló táblázatot.

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

1. ábra

Az üzenetet küldőnél 10 fáklya van, 5-5 mindkét kezénél. Az üzenetet betűnként küldi el úgy, hogy a bal kezével annyi fáklyát emel föl, ahányadik sorban, a jobb kezével pedig annyit, ahányadik oszlopban helyezkedik el a küldendő betű a táblázatban. Például a „t" betű esetén a bal kezében 3, míg a jobb kezében 4 fáklya van.

„Ezt a módszert Cleoxenusz és Demokritosz találta ki, de én tökéletesítettem." – írja büszkén Polübiosz.

Joggal lehetett büszke, mert bár a fáklyával történő üzenet továbbítást már a régi kínaiak[2] is ismerték, az ő rendszere volt az első táblázatba foglalt rejtjelező eljárás, amelynek nagy előnye, hogy — a módszer megváltoztatása nélkül — könnyen cserélhető a táblázatbeli ABC, illetve a táblázatbeli betűk elhelyezése.

Kérdés: *A fenti* 22 *betűs ABC betűi hányféleképpen helyezhetők el a táblázatban? És ha kitöltjük mind a* 25 *betűhelyet a táblázatban?*

Ezt az eljárást fejlesztette tovább Cardano úgy, hogy az ABC betűinek megadásához csak két fáklyát használt (egyet-egyet mindkét kézben) és a fáklyák elhelyezkedése, illetve egymáshoz való viszonya kódolta a megfelelő sort és oszlopot.

Ez a módszer adhatta Cardanonak az ötletet, hogy megalkossa a táblázaton alapuló titkosírás két nagy családját. Az egyik az „intervallum rejtjelezés", amelyben az üzenet titkosítása a betűk közötti távolságokon alapul. A módszert az egyszerűség kedvéért egy példán mutatjuk be. Készítsük el a *2. ábrán* látható táblázatot.

Á	a	e	r	n	c	b
B	i	o	d	l	g	q
C	u	s	m	f	p	t

2. ábra

Legyen az üzenet: *csacsi*. (A lépéseket a *3. ábrákon* követhetjük.) Írjuk az üres levélpapír bal felső sarkába az Á, B, C betűk bármelyikét. Ez csupán a szöveg kezdetét jelöli (C). Helyezzük a táblázat üres négyzetét a megjelölt betűre, majd a *csacsi* első betűjét (c) tartalmazó, nagybetűvel jelzett mező jelét (Á) írjuk a papírra pontosan a c betű fölé (lásd *3.a) ábra*). Most helyezzük a táblázat üres négyzetét az utoljára felírt nagybetűre, és keressük ki a táblázatból a következő betűt, az „s"-et. Ezzel ugyanúgy járunk el, mint az előzőkben, azaz a táblázatbeli *s* betű fölé írjuk a papírra a mező jelét (C). A fenti lépéseket addig folytatjuk, amíg van hely a levélpapír adott sorában, majd a legelső lépést megismételve új sort nyitunk, és az eljárást folytatjuk a küldendő szöveg végéig. A megfejtő dolgát azzal nehezítjük meg, hogy az üresen maradt helyeket tetszőleges, Á, B, C-től különböző betűkkel töltjük ki (lásd *3.b) ábra*). (Még jobb, ha értelmes szöveggé tudjuk kiegészíteni a rejtett szöveget, de ez nem feltétlenül szükséges.)

[2] A Kínai Nagy Falon már 2000 évvel ezelőtt, száz méterenként felállított fáklyások útján tudtak több száz kilométerre, nagyon gyorsan (és pontosan) üzeneteket eljuttatni.