Az ó-és középkori titkosírások és feltörésük matematikai vonatkozásai.

Készítette: Sabján Attila

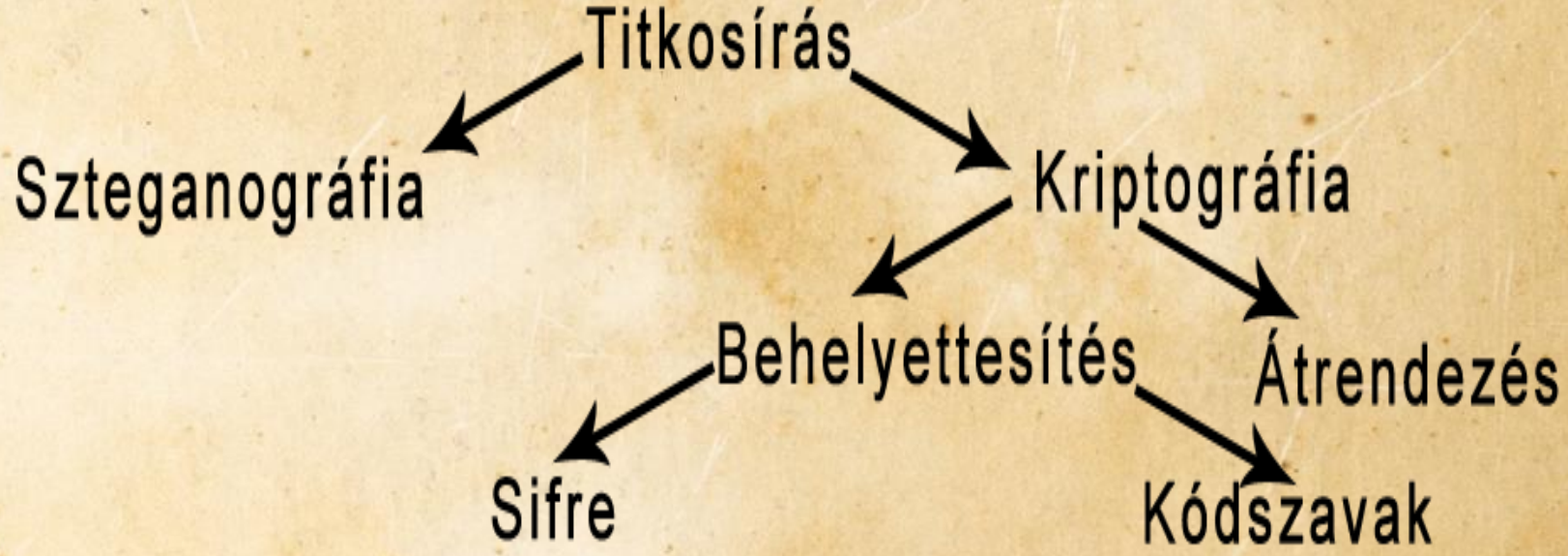
2020.04.13

A kriptográfia története

- A titkosírás (kriptográfia) abból a célból jött létre, hogy az egymástól távol lévő emberek bizalmasan tudjanak kommunikálni.
- Egy titkosírás akkor jó, ha idegen számára a megfejtés lehetetlen, és a feladó rövid idő alatt kényelmesen tudja kódolni, a címzett pedig rövid idő alatt tudja megfejteni.
- Az alábbi prezentációban csupán néhány speciális témakörrel fogunk foglalkozni.

A kriptográfia története

- A titkosírás alakulása:
-



A titkosírás ősi módszerei (Szteganográfia)

- A „szteganográfia” mint szó görög eredetű. Jelentése „leplezni, rejtett üzenetet írni”
- A szteganográfiával módszerével létrehozott rejtett üzenetek lényege, hogy az üzenet létezéséről csak a címzett tudjon.
- Ezzel szemben a kriptográfiában a titkosított tartalom létét nem álcázzák, de a tartalom csak a megfelelő rejtjel segítségével olvashatja a fogadó.

Példák a szteganográf technikákra az ókori történelemben.

- Az egyik legismertebb módszer az „elrejtett üzenet”, ilyenkor például a rabszolga fejbőrére írtak. Miután a rabszolgának visszanőtt a haja, akkor indították útnak.
- A másik szintén elterjedt módszer az úgynevezett „láthatatlan tinta”. A titkosított üzenetet egy másik szöveg sorai közé írták. Egy megfelelő eljárás alkalmazásával (pl. vegyszeres kezelés, melegítés) az üzenet újra olvasható vállt.

Szteganográfia az informatikában

- Alapvető szempont, hogy megfelelő méretű „zajos” hordozó álljon rendelkezésre.
- Zajos hordozó lehet például egy beszkennelt kép. Az információkat általában a legkisebb helyi értékű bitek (LSB) manipulálásával ágyazzák be. A programokban olyan algoritmusokat alkalmaznak, amelyek képpontonként megvizsgálják, a környező pixelek milyen szín- és világosságértéket hordoznak.
- Mindig kevés LSB-t módosítanak, hogy ne lehessen kiszűrni a módosított képpontokat.

Szteganográfia az informatikában

- A statisztikai eloszlására is ügyelni kell, több üzenetet például ugyanazok a pontok nem hordozhatnak , ugyanaz a kép pedig természetesen nem fordulhat többször a címzett és feladó között.

A kriptográfia története – átrendezéses módszer

- Átrendezéses titkosírási módszer lényege, hogy az üzenet szövegének betűit véletlen vagy valamilyen szabályrendszer segítségével átrendezik. Ilyenkor a betűk megtartják eredeti értéküket de a pozíciójuk megváltozik.

A titkosírás ókori módszerei- átrendezéses módszer

- Az egyik leghíresebb görög titkosító eszköz a skytala. Ez az eszköz két teljesen egyforma farúdból áll, amelyből az egyik a feladónál, a másik a fogadó félnél található. A rúdra szorosan egy vékony pergamenszalagot helyeznek. Az üzenetet a farúd hossztengelyére írják. Az üzenetcsík csak akkor olvasható ha a megfelelő méretű eszközre csavarják rá.
- Az alábbi videón megtekinthető a skytala működése:
- Link
-



A kriptográfia története- behelyettesítéses módszer

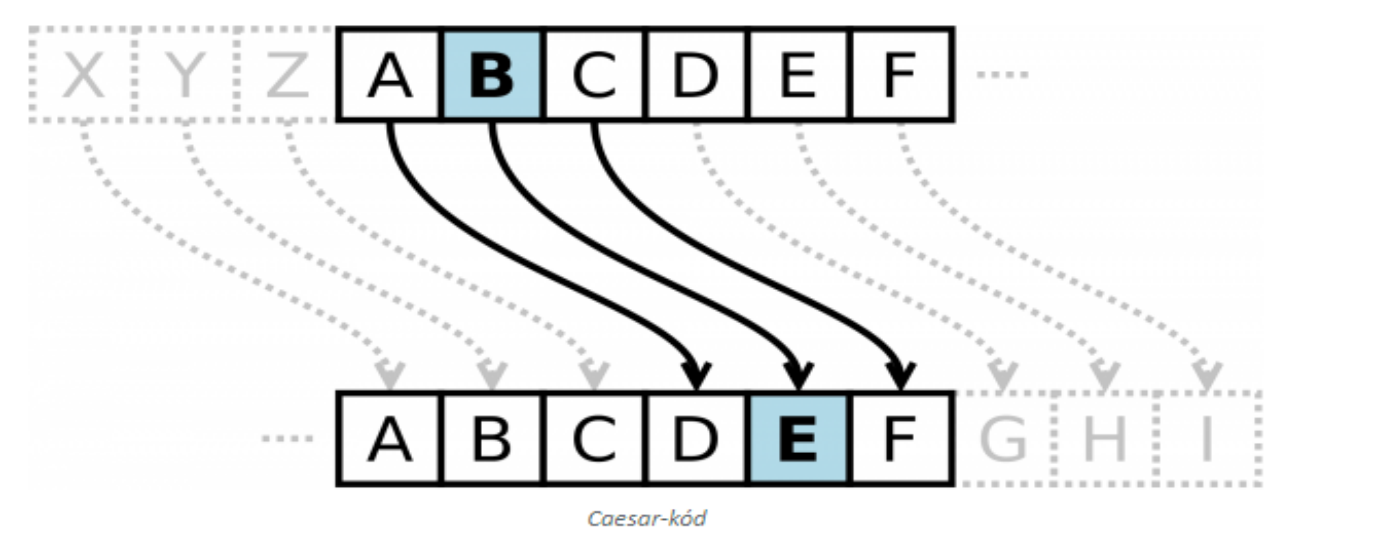
- A behelyettesítéses módszer esetén a szöveg minden betűjét egy másikkal helyettesítünk.
- Az egyik ilyen módszer az „atbas”, amelynek a lényege a betűk felcserélése. Az alapja, hogy az elsőt és utolsót, a másodikat és az utolsó előttit, stb.. cseréli fel.

A kriptográfia története- behelyettesítéses módszer – Caesar kód

- Az egyik leghíresebb ókori behelyettesítéses módszer a Caesar rejtjel. Lényege, hogy az üzenetet úgy fogalmazzuk meg, hogy a szöveg minden betűje helyett az ABC-ben hárommal utána lévőt írjuk. Például az A helyett D-t, a B helyett E-t. Dekódolásnál ezen módszert alkalmazzák csak visszafelé.
- Az alábbi linken megtekinthető a Caesar algoritmus működése: LINK

A kriptográfia története- behelyettesítéses módszer – Caesar-kód

- Példa a három betűs eltolásra:

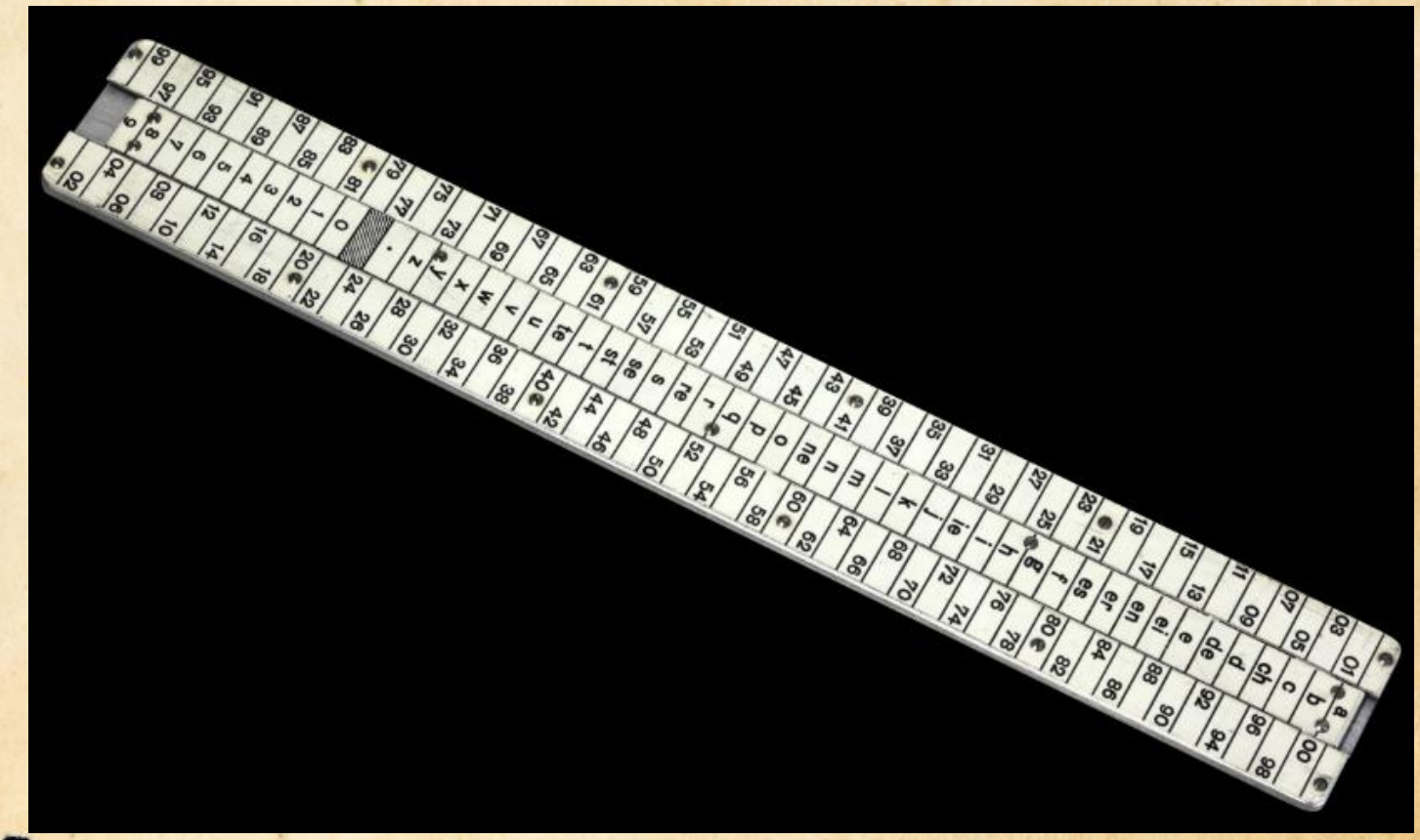


Caesar-kód

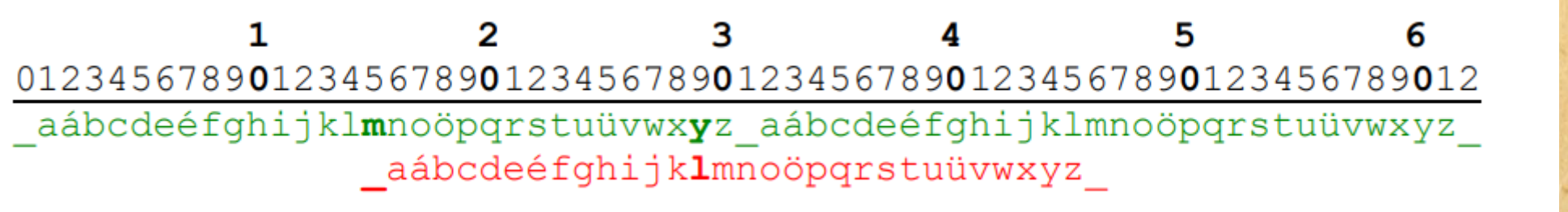
- A Caeasar rejtjel könnyen dekódolható, elég csak az eltolás mértékét megállapítani

Eszközök a Caesar-kód megfejtésére

- Csúszókód-logarléc:



Eszközök a Caesar-kód megfejtésére



- Eltolás (összeadás) művelet például m -el: zöld m alá húz egy „_” , majd minden piros betű fölött eltolja.
-

A titkosírás története - középkor

- A középkori Európa-i titkosírás kultúrájában terjedt el a helyettesítő rejtjel (vagy helyettesítő kód).Ennek a lényege, hogy a szöveg minden elemét egy szabályos rendszer segítségével alakítják át egy titkosított szöveggé. A címzett egy előre elkészített helyettesítő eljárással tudja csak megfejteni a szöveget.
- A helyettesítő eljárás fajtái a „monoalfabetikus rejtjel” és a „polialfabetikus rejtjel”
- A helyettesítő eljárás rengeteg kulccsal használható (angol ABC esetén 26! azaz 88 bit) mégis könnyen feltörhető.

A titkosírás története - középkor

- A „monoalfabetikus rejtjel” esetén a titkosítandó szöveg teljes egészében ugyan azt a helyettesítési eljárást használja. Egy karakter kódolása csakis ugyanazzal az új karakterrel történhet. Ennek következtében ezt a módszerű rejtjelezést könnyen fel lehet törni gyakoriságelemzés módszerével, amely a karakterek gyakoriságát tanulmányozza.
- Az alábbi linken megtekinthető „monoalfabetikus rejtjel” működése és feltörése: LINK

A titkosírás története - középkor

- A behelyettesítéses módszer másik ismert fajtája a „polialfabetikus rejtjel”. Ez egy olyan eljárás amely többféle eljárást használ a szöveg titkosításához.
- Az eljárást Leon Battista Alberti kezdte el kifejleszteni az 1460-as években. A végső kidolgozást Blaise de Vigenére francia diplomata fejezte be. Ezért ezt a módszer ma úgy ismerjük, hogy Vigenére-kód.
-

Vigenére-kódolás



-
- A Vigenére-kód működése során az adott kulcsszó betűiből függően különböző Caesar-kódokat használ. A kódolás során szükség van egy táblázatra amelyben Caesar-kódok vannak feltüntetve, és egy kulcsra. Kódolás során a szöveget kulcs hosszúságú darabokra bontjuk, majd a darabok alá a kulcsot írva az egyes betűket egy táblázat megfelelő rovatából keressük ki. A megfelelő kódolt karaktert a nyílt karakter oszlopában és a kulcs karakter sorában találjuk

Vigenére-kódolás

- A kódolás egyik fontos eleme a „tabula recta” amely egy ABC-ket felsorakoztató táblázat.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenére-kódolás

- Példa a kódolásra:
- Legyen a nyílt szöveg a „süt a nap”, a kulcs pedig a „Lojzi”
- Elég csak a megfelelő kód-ABC-ket felsorolni.
- AÁBCDEÉFGHIÍJKLMNOÓÖŐPQRSTUÚÜŰVWXYZ
  IÍJKLMNOÓÖŐPQRSTUÚÜŰVWXYZAÁBCDEÉFGH
  JKLMNOÓÖŐPQRSTUÚÜŰVWXYZAÁBCDEÉFGHIÍ
  LMNOÓÖŐPQRSTUÚÜŰVWXYZAÁBCDEÉFGHIÍJK
  OÓÖŐPQRSTUÚÜŰVWXYZAÁBCDEÉFGHIÍJKLMN
  ZAÁBCDEÉFGHIÍJKLMNOÓÖŐPQRSTUÚÜŰVWXY

Vigenére-kódolás

- A kódolt karaktert a nyílt karakter oszlopában és a kulcs karakterének sorában találjuk.
- Nyílt szöveg: Süt a nap
- Kulcs: Loj z iLo
- Kódolt szöveg: Cib z uLd

A titkosírás története – középkor – Vigenére-kód folytatás

- A Vigenére rejtjelezés olyan biztonságos volt, hogy „*le chiffre indéchiffrable”* azaz feltörhetetlen kódnak hívták. Ezt a fajta rejtjelezést a gyakoriság elemzéssel nem lehetett megfejteni. Csak az 1800-as években tudták először feltörni.
- A rejtjelezés egyértelműen hozzárendel minden betű párhoz egy meghatározott betűt a következő módon: $V: A \times A \rightarrow A, (a,b) \mid\rightarrow c$

A titkosírás története – középkor – Vigenére-kód folytatás

- Mivel egy véges csoportról van szó a Vigenére-kód analóg a szorzással és az osztással. Ha a kódolás során kifutunk az ABC elemiből, akkor vissza kell térni a sor elejére. Mivel minden sorban az ABC minden elem megtalálható így az eltolás összeadásként is értelmezhető. Ennek következtében a dekódolás kivonásnak felel meg.
- Az alábbi hivatkozáson megtekinthető az algoritmus működése: LINK

Vigenére-kód megfejtése



A Vigenére-kód megfejtésénél mindenképpen meg kell említeni Leonhard Euler nevét.
Euler 1670-ben született a Svájc-i Bázel-ben.
Apja Paul Euler kálvinista lelkész, anyja Margaretha Brucker nemesi családból származott. Már jó úton haladt, hogy apja kívánságának megfelelően lelkész legyen, amikor Johann Bernoulli észrevette Leonhard Euler matematikai tehetségét.
Euler kiemelkedő sikereket ért el a matematika terén pl: Euler-tétel, Euler-egyenes, Euler-turbinaegyenlet.
Részletesebben itt olvashatnak az életéről és munkásságáról.

Vigenére-kód megfejtése

A Vigenére rejtjelezés megfejtésénél Euler megfigyelte, hogy a lényegesen hosszabb szöveg esetén periodikus ismétlődések lesznek a kódolt szövegben.
Ezeknek a periódusoknak a hosszából a kulcs hosszára lehet következtetni.
Ekkora darabokra bontva a szöveget a visszafejtés lényegesen egyszerűbbé válik.
A fenti eljárás akkor igazán hatékony, ha hosszú a szöveg és rövid a kulcs

Cardano rejtjelező rácsa.

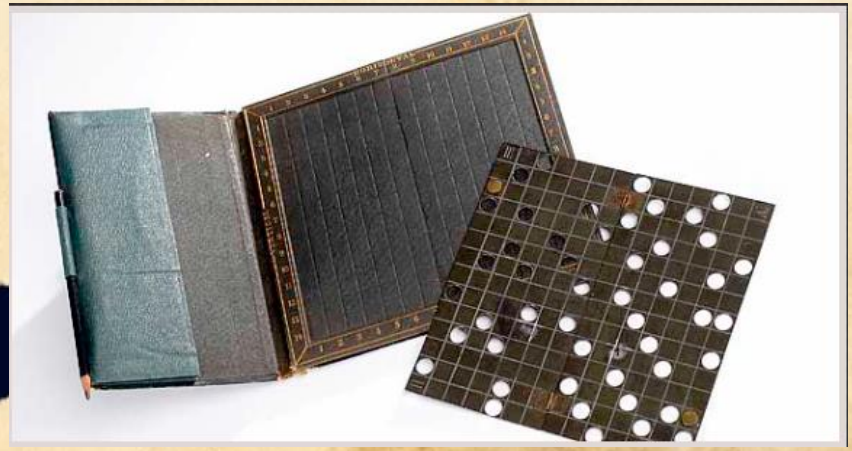


- Gerolamo Cardano (1501-1576) olasz származású matematikus, fizikus, orvos, asztrológus, mérnök.
- Főbb munkássága közé tartozik a harmad és negyed fokú egyenletek megoldásai.
- Az 1545-ben kiadott „Ars Magna” című könyvében jelent meg először az a módszer, amellyel a negyed fokú egyenletet harmad fokúvá lehet átalakítani.
- Az ő nevéhez fűződik a róla elnevezett kardántengely is.

Cardano rejtjelező rácsa.

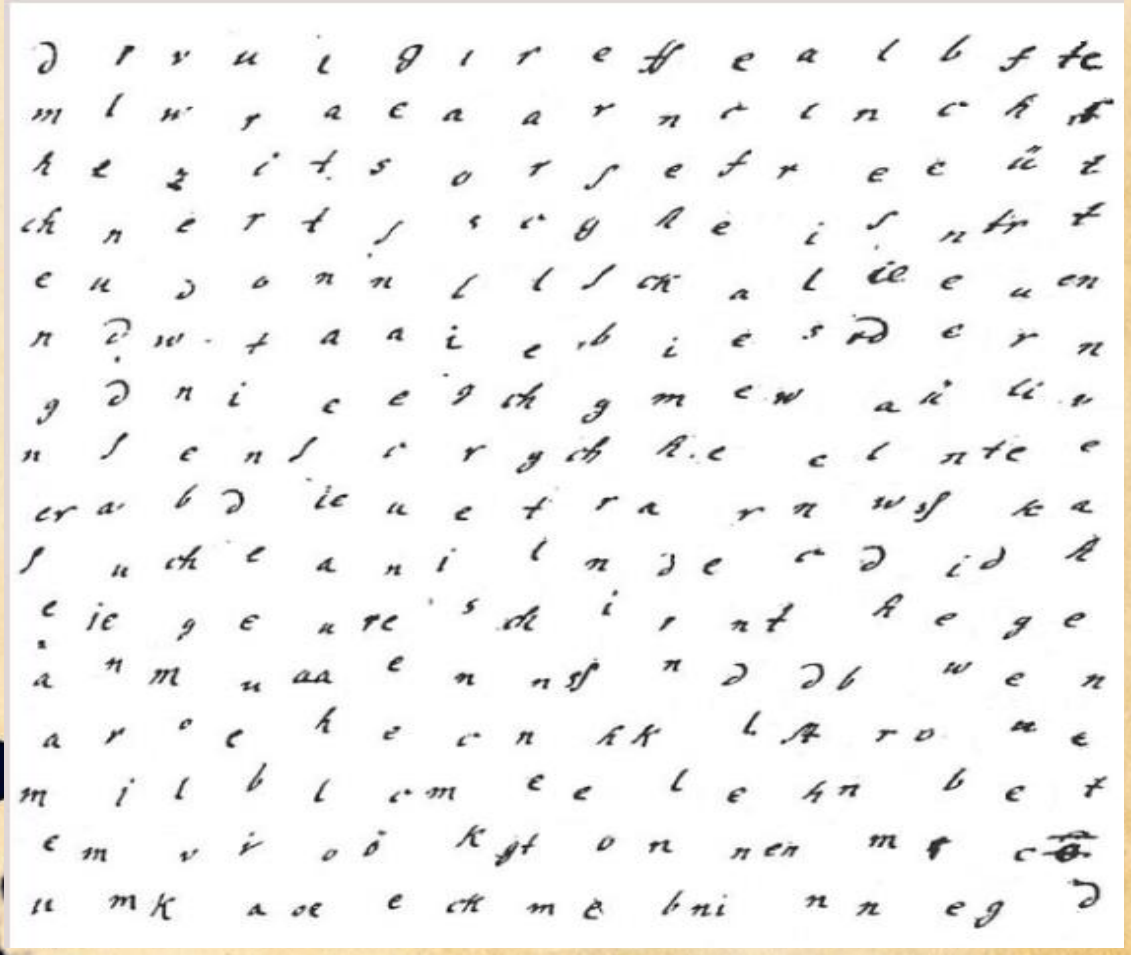
- Idézet Charles J. Mendelsohn: Cardan on cryptography cikkéből:
- *„Végy két azonos méretű pergamen lapot, és azonos vonalak mentén készíts kivágásokat 5 különböző helyeken. Ezek a kivágások legyenek kicsik, de mégis legalább akkorák, mint az ABC nagybetűi. Az összes kivágásokba összesen 120 betűt lehessen elhelyezni. Az egyik pergamen lapot majd a levelező társadnak adod. Amikor alkalom adódik, először írd az üzenetedet olyan tömören, ahogy csak lehetséges, így az üzenet kevesebb betűt is tartalmazhat, mint amennyi a kivágott ablakokban elhelyezhető. Amikor beírtad az üzeneted az egyik pergamen lapra, tedd ugyanezt a másikkal is. Ezután töltsd ki az első lapon az üresen maradt helyet úgy, hogy teljes mondatokra egészítsék ki a már ráírt szöveget. Ez a kitöltés úgy történjen, hogy a teljes szöveg stílusa és tartalma összefüggő és egységes legyen. Amikor a levelező társad megkapja a te üzenetedet, ráhelyezi a megfelelő kivágásokkal ellátott pergament, és így elolvashatja az üzenetet."*

Cardano rejtjelező rácsa.

- Kétféle eljárást ajánlott a rácshoz: az első, miszerint egy ártalmatlannak tűnő szövegbe kell a rácsot elhelyezni, ezáltal megkapva a szöveget.
- A másiknál a rács forgathatósága miatt a rácsot négyszer el kellett forgatni a megfelelő sorszámozáshoz, ahova szövegként be lehetett írni a kódolandó üzenet betűit sorban.
- 

Cardano rejtjelező rácsa példa

- Adott az alábbi levél (V. Vilmos németalföldi helytartó levele)



Cardano rejtjelező rácsa példa

- A 90-es évek közepén a dekódoló személyek észrevették, hogy néhány karakter lejjebb áll mint a többi. Feltételezték, hogy ezek a karakterek utólag, egy forgatható rácson keresztül lettek beírva. A rácsot rekonstruálva, majd ügyesen elforgatva összeolvasták a betűket, és meg is fejtették az átlyuggatott lemezen át készült német nyelvű titkosírást.

Cardano rejtjelező rácsa példa 2.

- Adott egy német nyelvű kódtábla:
- A sor és oszlopokra az alábbi összefüggés írható fel:
- 1<=x<=8 és 1<=y<=8

E	H	N	E	D	I	R	U
N	N	N	E	T	Ä	E	C
H	N	U	S	N	R	N	D
A	Z	S	E	C	W	T	H
A	E	S	N	E	W	C	Z
H	O	O	I	B	T	G	O
O	C	T	H	N	E	T	E
A	E	L	F	B	A	U	A

Cardano rejtjelező rácsa példa 2.

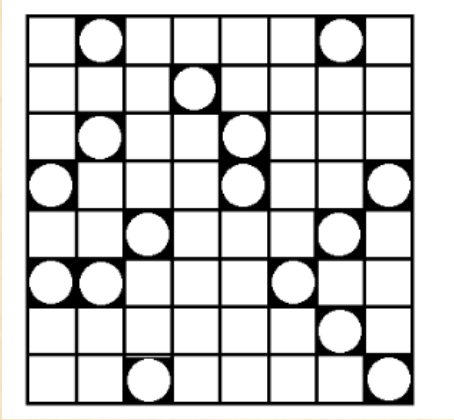
- Az egyenletrendszereket próbálgatásokkal megoldjuk.

1)	$x^3 = y$ & $x^3 \neq x$	9)	$3x+4y = 25$ & $4x+3y = 24$
2)	$x+y = 15$ & $x+1 = y$	10)	$x^2-3y^2 = 1, y>1$
3)	$x+y = 11$ & $x-y = -3$	11)	$3x = y$ & $x+2 = y$
4)	$3x = y$ & $x = y-4$	12)	$3x = 2y$ & $x = y-1$
5)	$x*y = (x+1)*(y-1) = 3*(x+y-1)$	13)	$x = 2y$ & $x+y = 9$
6)	$2x+y = 7$ & $3x+2 = y$	14)	$x = y^3 -1$
7)	$x^2+y^2 = 89, x>y$	15)	$x-2y = 1$ & $2x+y = 7$
8)	$2*x*y = 50$	16)	$x = 2*(y+1)^2$

- Megoldás:
- (2,8), (7,8), (4,7), (2,6), (5,6), (1,5), (5,5), (8,5), (3,4), (7,4), (1,3), (2,3), (6,3), (7,2), (3,1), (8,1),

Cardano rejtjelező rácsa példa 2.

A kapott koordinátákkal megkapjuk a pontos kinézetét a dekódoló rácsnak:



Miután a dekódoló rácsot ráhelyeztük a szövegre,a megfelelő betűk kiolvasása után a rácsot a közzéppontja körül többször elforgatjuk 90 fokkal.

Cardano rejtjelező rácsa példa 2.

A kívánt kódrészleteket itt is próbálgatásos módszerrel kapjuk.
A rács forgatásánál minimum 8 lehetőséget kell végigpróbálni.
Ez azért szükséges mert nincs előre megadva a dekódoló rács forgási iránya.
Mindkét forgásirány próbálgatásnál négy-négy szövegrészt kell sorba rendezni.
Az így kapott karakterek mindig soronként olvassuk ki.
Az eredményként kapott szöveg:
„Einundzwanzig neue Unterseeboote fahren nach Schottland nächste Woche ab.”

Felhasznált irodalom

- Kriptográfia története.
- Szteganográfia
- Csúszókód – logarléc
- Rejtjel-rács a valódi történelemben
- Gerolamo Cardano
- Szteganográfia: nagyon rejtett jelek
- Caesar-rejtjel
- 2018 - PannonEnigma verseny