Az ó-és középkori titkosírások és feltörésük matematikai vonatkozásai

GULYÁS GERGELY

Tartalom

1. Mi a titkosírás?
2. Történelme
3. Ókor
4. Középkor
5. Érdekességek az Újkorból

Mi a titkosírás?

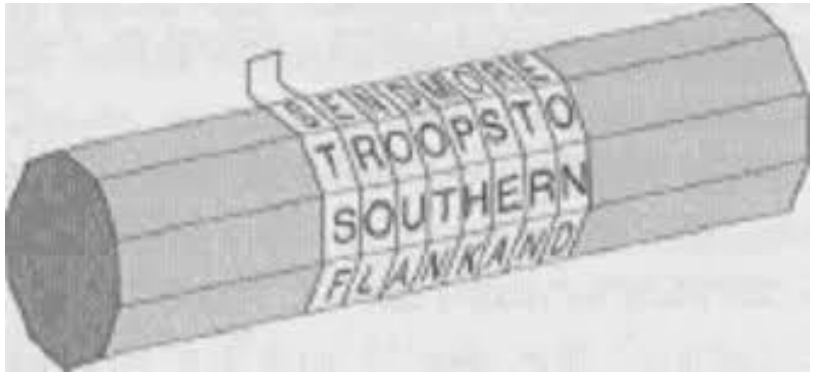
- A titkosírás (vagy kriptográfia) egy adott szöveg vagy üzenet “lefordítása” egy olyan kódra amit csak az érthet akinek birtokában van a “visszafordításhoz” szükséges információ.
- A kódolás során használhatnak többféle módszert, egyik ilyen például a képen látható Szkütalé. Más módszerek mint például az átrendezés vagy behelyettesítés szintén léteznek.
- Matematikailag bonyolultabb például a Caesar kódolás ahol egy meghatározott képlet alapján számolják ki az adott karakter kódolt megfelelőjét.



Történelme

Ókor - Szkütale

- A szkütale egy ókori teljesen mechanikus eszköz volt amelyet titkosításra használtak.
- A működése egyszerű: egy adott átmérőjű hengerre vagy adott élű hasábra feltekertek egy szallagot amelyre felírták a szöveget egymás alatti sorokban.
- A dekódolás egyszerű volt: egy ugyan olyan átmérőjű hengerre volt szükség amire ugyan úgy feltekerték a szallagot, így olvashatóvá vállt a szöveg.



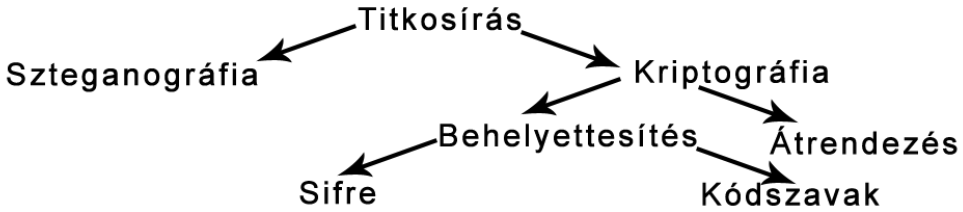
Ókor - A Cézár kerék

- A cézár kerék szintén egy titkosításra használt eszköz volt ami abban különbözött a Szkütale-től, hogy míg ott egy adott átmérőjű rúdra kellett feltekerni a szallagot, itt az üzenet megfejtéséhez egy kör alakú eszközre volt szükség.
- A kerék két egymástól függetlenül forgó tárcsáján helyezkednek el a betűk és ezzel lehet beállítani a megfelelő eltolást majd leolvasni a titkosított betűkhöz tartozó valós párjukat.



Ókor

- A titkosírás legősibb módja a szteganográfia vagy rejtett írás. Ennek lényege az volt, hogy a leírt szöveget minél inkább elrejtsék és így csak az tudja elolvasni, aki tudja hol kell keresni.
- Több módszer is létezett az üzenet elrejtésére, például ekkor találták ki az átrendezéses és a behelyettesítéses módszert is.
- Feltörésük időigényes, minél nagyobb a karakterszám annál tovább tart a lehetőségek száma miatt. Egy kb 30-35 betűs mondat például már szinte feltörhetetlen.



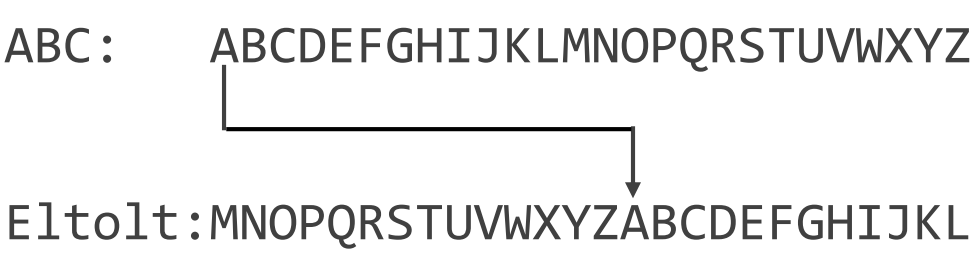
Ókor – Caesar-rejtjel

- Ez egy olyan eljárás amit Julius Caesar használt az üzenetek titkosítására. Az ABC betűit adott számmal eltolta.
- Legyen két ABC. Mindkettő a standard angol ABC, viszont az alsó eltolható jobbra és balra is (lehet hozzáadni és kivonni belőle).
- A jobb oldai példán az eltolás 14.
- Így például ha az n. betűből m. betű let akkor az n+1. betűből m+1 k-s maradéka ahol a k az ABC hossza (Ez angol ABC esetében 26, a Magyar esetében 40).

```
ABC:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Eltolt:MNOPQRSTUVWXYZABCDEFGHIJKL
```

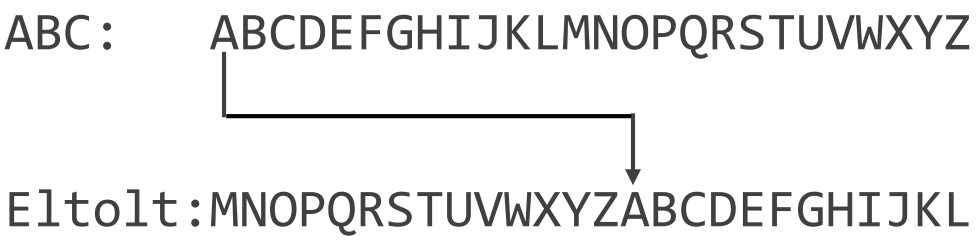
Ókor – Caesar-rejtjel

- A Caesar kódolás matematikailag is kifejezhető:
- $E_n(x) = (x + n)\ mod\ a$
- Ebben az esetben ‘*x*’ mindig a kódolandó betű, ‘*n*’ az eltolás mértéke, ‘*a*’ pedig a használt ABC mérete, angol esetén ez 26.
- Kulcstér: a lehetséges eltolások száma, angol ABC esetén ez 25 lehetőség.
- A dekódolás a következő formulával számolható:
- $D_n(x) = (x - n)\ mod\ a$

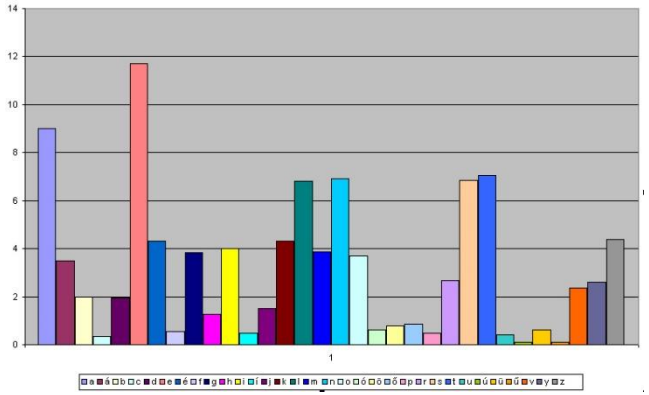


Ókor – Caesar-rejtjel

- A kódolás feltörése egyszerű, két eset lehetséges:
  - A támadó nem tudja, hogy Caesar-rejtjelről van szó
  - A támadó tudja ezt, viszont nem tudja az eltolás mértékét.
- Az első esetben un. frekvencia analízist kell használnia, viszont feltűnhet neki, hogy Caesar kódolást alkalmaztak.
- A második esetben csak végig kell próbálnia az ABC számú eltolást. Ez angol esetében 26.
- A kódolás így nagyon egyszerűen feltörhető.



Középkor



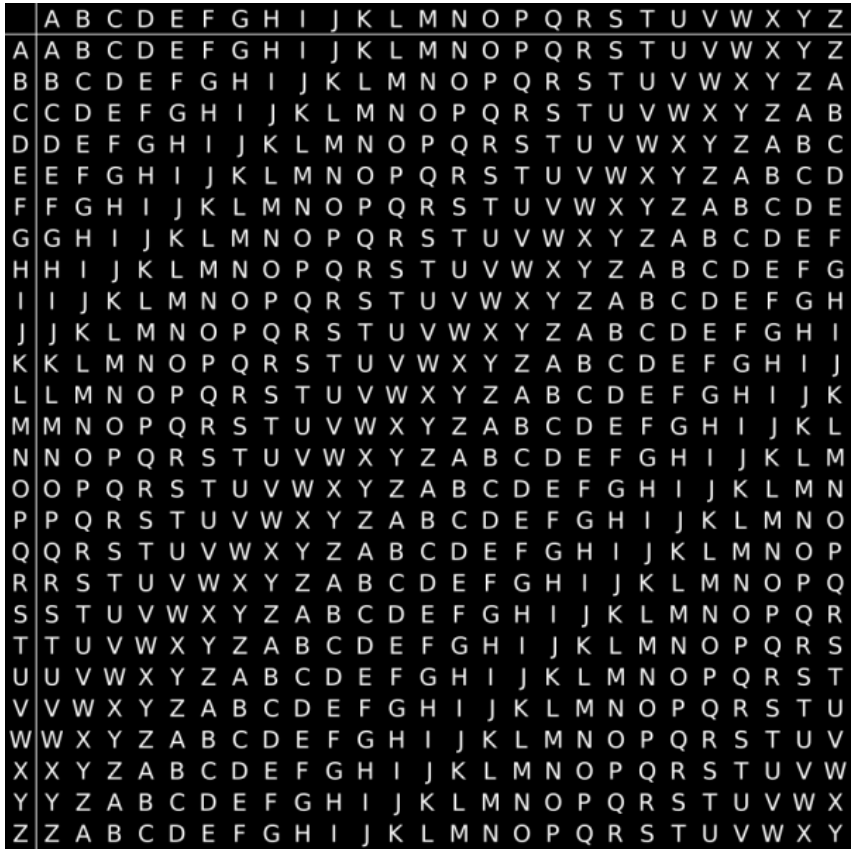
- A középkorban tovább fejlődött a titkosírás, a monoalfabetikus kódolás volt az elterjedt.
- A kód feltörésére a kriptoanalízis feltalálása után került sor. A kriptoanalízis a kódolt szöveg kulcs nélküli feltörését jelenti és ehhez statisztikai és matematikai tudás szükséges.
- A feltörés során a betűk számát veszik figyelembe amivel kideríthetik melyik karakter melyik valós karakternek felel meg.
- A képen a Magyar ABC-ben található karakterek előfordulásának gyakorisága látható.

Középkor

- Többen próbálták a monoalfabetikus kódolást megerősíteni, ilyen volt például a nullitások bevezetése. Ebben az esetben semmit nem jelentő karaktereket illesztettek be a kódba ezzel is nehezítve a feltörést.
- Kódolt üzenetek a Bibliában is előfordultak: észre vették, hogy a betűk között ugrálva bizonyos egységeket nagy számú EETLB karaktersorozatok vannak.
- A monoalfabetikus kód javítására bevezették a szólajstromokat. Ez azt jelentette, hogy a szöveg egyes szavait külön szimbólum jelölte.

Középkor – Vigenère kódolás

- A Vigenère kódolás egy olyan formája a titkosításnak ahol különböző Caesar kódokat alkalmaznak egy adott kulcsszó betűitől függően.
- Eleinte egy táblázatból kellett kiolvasni a betűket (jobb oldali kép) viszont később sikerült matematikai alapokra helyezni.
- A kódoláshoz szükség van egy kódolandó szövegre és egy a kódoláshoz használt kulcsra.



	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

Középkor – Vigenère kódolás

- A kódolás során a mintához hasonlóan a kódolandó szöveg minden betűjét a kulcs megfelelő betűjével tolják el.
- A kódolandó szöveg (E) legyen most “A Matematika története, a kulcs (K) pedig “titkos”. Az egyszerűség kevéért csak angol ABC betűit használtam.
- Ekkor a kódolandó szöveg minden betűjét eltova a kapott végeredmény (V) a 3. sorban olvasható.
- A képlete: $V: A \times A \to A, (a, b) \longmapsto c$

```
E: A Matematika tortenete
K: t itkostitko stitkosti
V: t utdsetbbuo lhzmobwmm
```

Középkor – Vigenère kódolás

- Eleinte törhetetlennek gondolták a kódot a lehetőségek nagy száma miatt.
- Euler volt az első aki észrevette, hogy hosszabb szöveg esetén periodikus ismétlődések vannak a szövegben. Ekkor az összes periodus legnagyobb közös osztója lesz a kulcs.
- Gyakorlottaknak a feltörés egy gyakoriság tábla birtokában és nem túl hosszú kulcs esetén kb. 6-8 órába telik.
- A kódolásra és a dekódolásra több nyelvben is készült programkód.

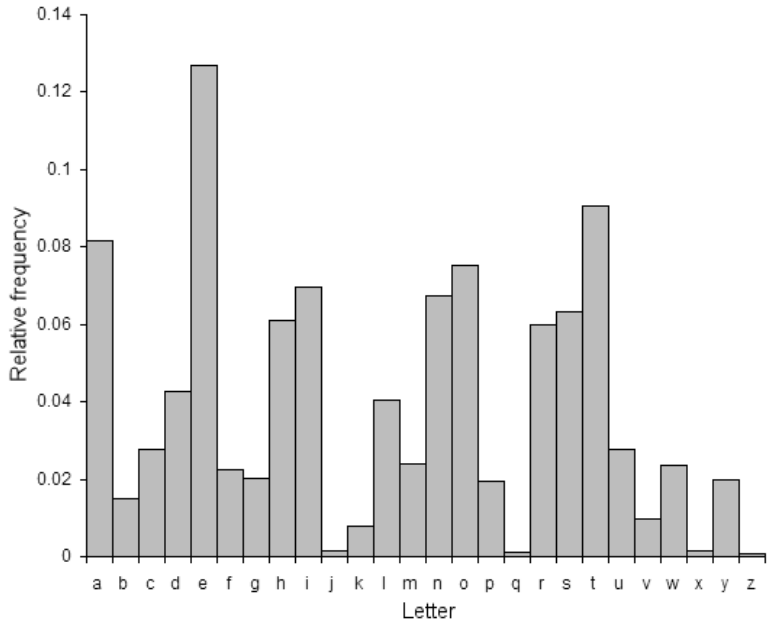
```
E: A Matematika tortenete

K: t itkostitko stitkosti

V: t utdsetbbuo lhzmobwmm
```

Kódfejtés – Gyakoriságelemzés

- Azon alapszik, hogy bármilyen szövegrészben bizonyos betűk vagy azok kombinációi adott gyakoriságokkal fordulnak elő. Egy adott nyelvben minden betű egy rá jellemző gyakorisággal rendelkezik.
- Ez használható kódfejtésre is, hiszen két lépésben megfejthető egy egyszerűen titkosított szöveg:
  - Első lépésként minden egyes betű előfordulását a szövegben (ennek legjobb szemléltetése egy hisztogram készítése)
  - Második lépésként ezt össze kell vetni az adott nyelv gyakorisági adataival.
- Ezzel a módszerrel megfejthető például egy helyettesítő módszerrel kódolt szöveg.



Érdekességek az Újkorból

- Cardano újkori matematikus találta fel a rejtjelező rácsot. Ő egy rácsot készített, amit egy adott szövegre ráillesztve lehetett kiolvasni a szöveget.
- A komplexitását növelte, hogy a rácsot négy módon lehet a szövegre illeszteni.

