Titkosírások az ókorban és a középkorban

KÉSZÍTETTE: GYÖRFFY BÁLINT

Bevezetés

- Mióta emberek kommunikálnak egymással, azóta természetes igény van az üzenetek célba juttatására olyan módon, hogy csak a címzett kerülhessen az információ birtokába és illetéktelen személy elől a tartalom rejtve maradjon. Ha a csatorna nyílt, tehát számítani lehet arra, hogy az úton lévő adatokhoz más is hozzáfér, szükség lehet az adatok titkosítására.

Az ókori titkosírások

Szteganográfia

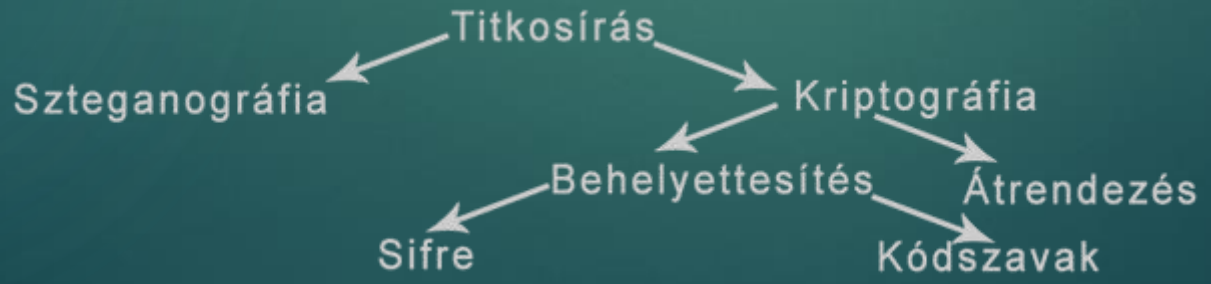
A szteganográfia az üzenetek titkos továbbításának legősibb módja az üzenet elrejtése. A szó jelentése rejtett írás.

- Leborotválták a küldöncének haját, ráírták az üzenetet, majd megvárták, amíg a küldöncnek haja újból kinő, így átkelhet a határon. Amikor a küldönc célba ért, leborotváltatta fejét és megmutatta az üzenetet.
- Már az első évszázadban is tudták azt, hogy a pitypang tejével is lehet írni, hiszen az a száradás után láthatatlan, de melegítésre barna lesz. Ez a tulajdonság sok szerves vegyületben megvan, így előfordult, hogy a kémek saját vizeletükkel írtak. (Használható hagymalé vagy tej is)

A titkosírások fajtái

A kriptográfia a szteganográfiával egy időben alakult ki, és célja nem magának az üzenetnek, csupán csak a tartalmának, jelentésének elrejtése, kódolása, hiszen a határőrök előbb-utóbb az üres lapot felmelegítik, leborotváltatják a hajat, azaz rájönnek a módszerre.

A kriptográfia két ágra oszlik: átrendezésre és behelyettesítésre.



Átrendezés

Átrendezésnek nevezzük azt a titkosítási módszert, amikor az üzenet szövegének betűit véletlenszerűen, vagy valamilyen szabályrendszer alapján átrendezik – a betűk megtartják eredeti hangértéküket, de megváltoztatják a pozíciójukat.

A spártai **szkütale** az ábrán láthatóhoz hasonlóan feltekertek egy papírt, erre vízszintesen írták rá a szöveget és így értelmetlen lett.



Titkosítandó szöveg:
Belépés díjtalan, kilépés bizonytalan!

Nyílt szöveg:
Babelilazénopknéiysltdéaipljéatsn

(minden harmadik betűt kell összeolvasni)

Behelyettesítéses módszer

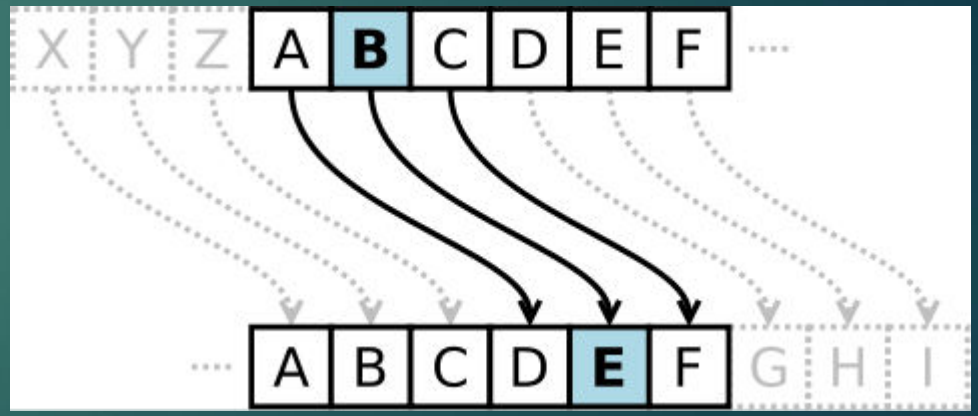
A behelyettesítés módszere esetén a nyílt szöveg minden betűjét egy másikkal helyettesítik – a betűk megtartják pozíciójukat, de megváltozik a hangértékük.

Monoalfabetikus kódok

Azokat a behelyettesítéses kódábécéket nevezzük monoalfabetikusnak, amelyek egy betűt egy másik betűvel vagy szimbólummal helyettesítenek.

A Caesar-rejtjel

Az úgynevezett Caesar-rejtjel, egy eljárás, amit Julius Caesar is használt. Itt **Caesar az ábécét egy bizonyos számmal eltolta**, azaz ha az n. betűből az m. lett, akkor az n+1-edikből m+1 k-s maradéka, ahol k az ábécé hossza.
(Augustus ezen annyit változtatott, hogy a az eltolás egy karakternyi volt, azaz az A helyett B, a B helyett C, …, a Z helyett A szerepelt. Emellett az X helyett mindig AA-t írt.)



Néhány ókori titkosírás

Polübiosz-négyzet

A Polübiosz-rejtjel egy egyszerű titkosítási eljárás, melynél az ABC 25 betűjét egy táblázatba foglalják. Itt a rejtjelezett betűk a mátrix elemeinek felelnek meg, a sorok és az oszlopok azonosítójából olvashatjuk le a kétjegyű kódot. Például:

Az üzenet: **ALMA** A kódolt szöveg: **11-31-32-11**

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

A Káma-szútrában található módszer

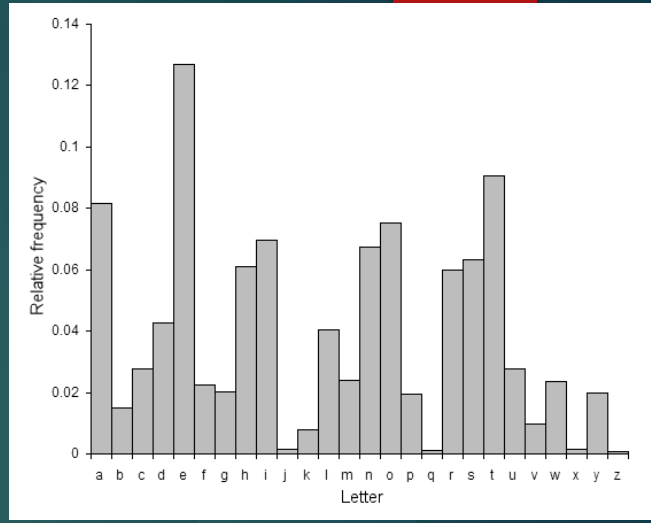
A Káma-szútrában található leírás az ábécé betűinek véletlenszerű párosítását és egymásnak kölcsönös megfeleltetését ajánlja. Például a 26 betűből álló angol ábécé esetén:

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

Kódolás	
Az üzenet:	TITKOSIRASOK
A kódolt szöveg:	RBRQCLBTXLCQ

A Caesar-rejtjel feltörése

- Ha tudjuk, milyen nyelven íródott a kódolt üzenet, akkor megfejtésének egyik módja az, hogy veszünk egy ugyanolyan nyelven írt nyílt szöveget, amely elég hosszú ahhoz, hogy legalább egy lapot megtöltsön, és megszámláljuk, melyik betű hányszor fordul elő benne.
- Ezután vesszük a kódszöveget, s annak szimbólumait is megszámláljuk. Megkeressük a legsűrűbben előfordulót, s azt behelyettesítjük a nyílt szöveg leggyakoribb betűjével, a sorban következőt a 'második'-kal, az az utánit a 'harmadik'-kal, és így tovább, míg be nem helyettesítjük a megfejteni kívánt szöveg minden szimbólumát.



Ha eleve tudjuk, hogy ebben a kódolásban van rejtjelezve az üzenet, akkor a legegyszerűbb esetben az eltolásokat fokozatosan változtatva a szöveg a megfelelőhöz érve spontán dekódolódik.

Ha nincsen sejtésünk a kódolási rendszerről, a statisztikák erős eszközök, ugyanis az egyes helyettesítések rendszeres azonosságát kihasználva a Caesar-gyanú megerősíthető. Ebben az esetben igazából nem annyira az egyes betűk, hanem a betűpárok nyújtanak felvilágosítást. Bármilyen eltolást is használjunk, esetleg keverést.

Középkori tiktkosírások

A középkorban főleg a behelyettesítéses titkosírásokat próbálták biztonságosabbá tenni különféle módszerekkel.

Behelyettesítéses algoritmus nullitásokkal

A gyakoriságelemzés megnehezítése céljából próbálkoztak nullitások bevezetésével, ami a semmit nem jelentő karaktereket jelenti.

homofonikus behelyettesítés

A betűk gyakorisága alapján ugyanannyi lehetőség feleltet meg egy betűnek, mint ahány százalék volt az elterjedtsége.

Ez sem nyújt azonban tökéletes biztonságot, hiszen különböző módokon megfejthető. Például az angolban a legfeltűnőbb jelekkel a Q rendelkezik, ami után csak U állhat. A többi betűnek is vannak hasonló tulajdonságai, minden nyelvben.

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
64	65	20	42	56	74	21	43	57	90	91	22	44	58	23	45	59	24	46	60	02	11	16	38	52	70
14	15	25	47	61	87	99	17	39			53	71	36	37	26		62	88	89	48		49		31	
54		50	51	27			63	06			72		32	55			79	00	12	34					
73			33	10			66	07			68		03	01			13	35	18						
67				19			76	81					93	28			29	30	40						
75				08			41	09					82	94			80	77	96						
97				84										86					85						
05				92															78						
				83															95						
				04																					
				69																					
				98																					

Polialfabetikus kódok

Polialfabetikusnak nevezünk minden olyan helyettesítő rejtjelezést, amely **többféle kódábécét használ** az üzenet kódolásakor.

A legismertebb polialfabetikus kódolás a Vigenère-kód

Vigenère-kód

A Vigenère-rejtjelezés eredetileg a betűknek egy adott kulcs szerint táblázatból való kikeresését jelentette, azonban a csoportelmélet segítségével egyrészt sikerült matematikai alapokra helyezni, másrészt pedig a feltörését és annak nehézségét meghatározni.

Vigenère-kód egy **adott kulcsszó betűitől függően, különböző Caesar-kódokat használ**. A kód a következőképp működik: a táblázatban az összes Caesar-kód fel van tüntetve, minden betűvel, és a megfelelő kóddal kezdődő ábécé a kódolás alapja. A Vigenère-kód gyakorisági elemzéssel megfejthetetlen.

	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

Kódolás

A rejtjelezéshez a nyílt szövegen túl egy kulcsra is szükség van, aminek segítségével a kódolt szöveget létrehozzuk. A nyílt szöveget kulcs hosszúságú darabokra osztjuk, majd a darabok alá a kulcsot írva az egyes betűket egy táblázat megfelelő rovatából keressük ki. A táblázatban a Caesar-kódok vannak felsorolva.

Vigenère-kód példa

Vigenère-kód példa	
Nyílt szöveg:	BUDAPEST FELETT AZ ÉG FELHŐTLEN
Kulcs:	LOJZILOJ ZILOJZ IL OJ ZILOJZILO
Kódolt szöveg.	NGNZWÖÉB ÉMÜQBS IK RŐ ÉMÜUXSSÖY

A Vigenère-kód feltörése

A kódot a számtalan variációs lehetőség miatt sokáig feltörhetetlennek gondolták, azonban Leonhard Euler felfedezte, hogy **a kulcsnál lényegesen hosszabb szöveg esetén periodikus ismétlődések lesznek a kódolt szövegben**. Az összes periódus legnagyobb közös osztója lesz a kulcs hossza. Ekkora darabokra bontva a szöveget a visszafejtés lényegesen egyszerűbbé válik.

A kódolt szöveget ugyanis a **betűk helye szerint k csoportba oszthatjuk**. Az első halmazba az 1., (k+1)-edik (2k+1)-edik, stb., a másodikba a 2., (k+2)-dik, stb... karakterek kerülnek. Ezek után a halmazokra gyakoriságanalízist végzünk, így a szöveg és a kulcs párhuzamosan fogja adni magát. Gyakorlott rejtjelfejtőnek gyakoriságtáblázat birtokában, nem túl hosszú kulcs esetén mintegy **6-9 órába telik megfejteni a kódolt szöveget**.

Titkosírások és a matematika kapcsolata

- A titkosírások feltörése sok matematikai területet érint.
- Statisztika: a Caesar-rejtjel feltörése kapcsán, a betűk gyakoriságán alapuló feltörési módszer.
- Csoportelmélet és számelmélet: Az adott hosszúságú Vigenère-kód egyszerűsítése.
- Kombinatorika: a kódolások feltörése brute force módszerekkel.
- Frekvencia analízis: Vigenère-kód kulcsának hossza meghatározásához.

Köszönöm a figyelmet!

Források

- https://hu.wikipedia.org/w/index.php?title=A_kriptogr%C3%A1fia_t%C3%B6rt%C3%A9nete&action=edit&section=17#Egy%C3%A9b_m%C3%B3dszerek
- https://hu.wikipedia.org/wiki/Vigen%C3%A8re-rejtjel
- https://hu.wikipedia.org/wiki/Caesar-rejtjel