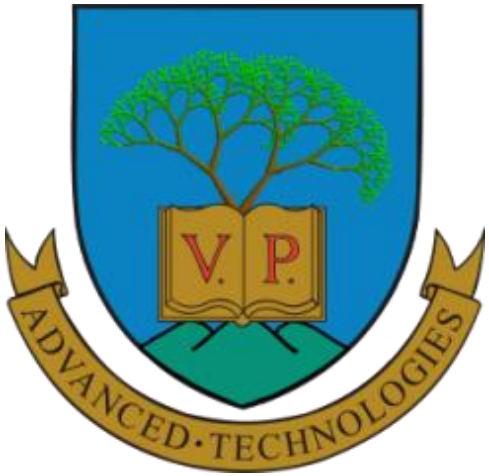
Kriptográfia

Smidla József

Pannon Egyetem, Műszaki Informatikai Kar



Veszprém, 2012. augusztus 21.

Szteganográfia

- Ógörög eredetű: leplezni
- Az információt nem titkosítják, hanem elrejtik
- Hérodotosz: Demeratus figyelmeztette Spártát Xerxész terveiről, viasztábla
- Hisztiaiosz felkelése a perzsák ellen: rabszolga fejére írt szöveg
- Láthatatlan tinta, citromlé, mikropont…

Szteganográfia

- Gárdonyi Géza: Egy magyar rab levele

„Kedves ezüstös, drága dádém!
Ezer nemes arany tizedét örömmel ropog-
tasd örök keserűség ivó magzatodért.
Egészségem gyöngy. A vaj árt. Ritkán óhaj-
tom sóval, borssal. Ócska lepedőben szá-
rítkozom álmomban, zivataros estén. Matyi
bátyám, egypár rózsát, rezet, ezüstöt, libát
egy lapos leveleddel eressze hajlékomba.
Erzsi, tűt, faggyút, ollót, gombot, levendulát adj!
Laci, nefelejts!

Imre”

Szteganográfia

- Gárdonyi Géza: Egy magyar rab levele

„Kedves ezüstös, drága dádém!
Ezer nemes arany tizedét örömmel ropog-
tasd örök keserűség ivó magzatodért.
Egészségem gyöngy. A vaj árt. Ritkán óhaj-
tom sóval, borssal. Ócska lepedőben szá-
rítkozom álmomban, zivataros estén. Matyi
bátyám, egypár rózsát, rezet, ezüstöt, libát
egy lapos leveleddel eressze hajlékomba.
Erzsi, tűt, faggyút, ollót, gombot, levendulát adj!
Laci, nefelejts!

Imre”

Kedden a török kimegy a városból. Száz emberrel el lehet foglalni.

Szteganográfia

Ezt látja a laikus

Ezt rejtették el

Kriptográfia

- Ógörög eredetű: κρυπτός (kryptós) = „rejtett”, γράφειν (gráphein) = „írni”, tehát „titkosírás”

- Kriptográfia: információrejtés
- Kriptoanalízis: visszafejtés

- Kriptológia : kriptográfia + kriptoanalízis
- Állandó „harc”: rejtjelezők vs. kódfeltörők

Kriptográfia

- Első említés: Káma szútra
- 64 művészet ismeretét írja elő a nők számára, példák:
- Ének, tánc, tetoválás, varázslat és ráolvasás, rejtvények megoldása, olvasás, kardvívás, íjjal való gyakorlat, asztalos-mesterség, titkosírás, szavak kiforgatása, háború és hadviselés művészete, stb…

Kriptográfia

- **Görögök**
  - Fésűs módszer

THY SECRET IS THY PRISONER; IF THOU LET IT GO, THOU ART A PRISONER TO IT

↓

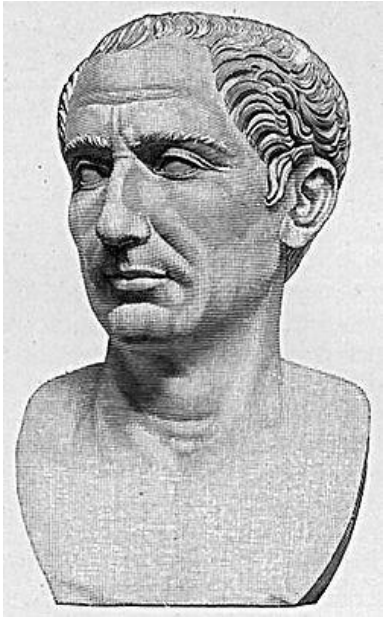
T H Y S E C R E T I S T H Y P R I S O N E R I F T H O U L E T I T G O T H O U A R T A P R I S O N E R T O I T

↓

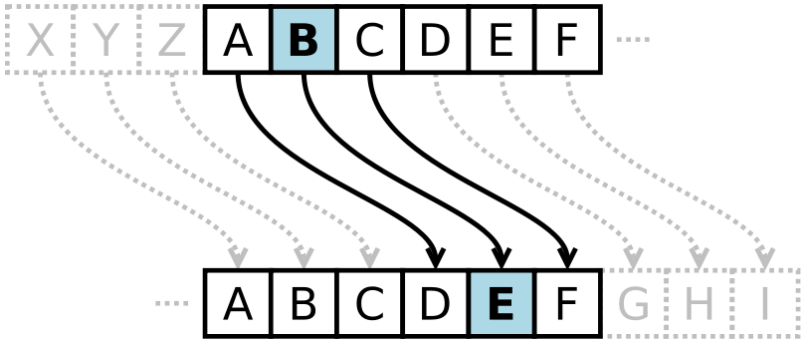
TYERTSHPIOEITOLTTOHURARSNROTHSCEITYRSNRFHUEIGTOATPIOETI

  - Átrendezés „szkütalé”-val
    - Lüszandrosz spártai hadvezér így szerez információt a perzsa Pharnabazosz támadásáról

Kriptográfia



- Caesar kód
- Minden betűt kicserél egy, az ABC-ben tőle *k* távolságra lévő betűvel
- A gall háborúk című műben említik, hogy Caesar így üzent az ellenség által körbevett Cicerónak



Kriptográfia

- A Caesar kódot általánosítása:
- Minden betű helyett egy másikat használunk
- Lehetséges párosítások száma 26 betűnél:
- 403 291 461 126 605 635 584 000 000
- Ezt biztos nem lehet megfejteni, hiszen rengeteg párosítást kell végignézni… gondolták hosszú évszázadokig

Kriptográfia

- Iszlám világ, Abbászida-kalifátus:
- Jól működő társadalom kialakítása,
- Alacsony adók, üzleti élet segítése
- Kereskedelem, ipar
- Korrupció visszaszorítása
- Tudományok magas szintű művelése
- Teológiai kutatások

Kriptográfia

- Korán tanulmányozása
- Az iszlám szerint a Koránt Mohamed részletekben, 23 éven át kapta meg Gábriel arkangyaltól
- Mohamed írástudatlan volt, ezért szóban terjesztette a szöveget (mások szerint tudott írni, csak nem volt rá ideje)
- Halála után azonban leírták a szöveget
- Eleinte több változat is létezett

Kriptográfia

- Arab tudósok azt vizsgálták, hogy a Korán változataiban mely részletek származnak Mohamedtől, és melyek nem oda valóak
- Szavak előfordulásának vizsgálata
- Később a betűket is vizsgálták
- Majd megszületett a gyakoriságanalízis
- Jákúb ibn Iszhák al-Kindi: Titkos üzenetek megfejtése

Kriptográfia

- Európa: Giovanni Soro, reneszánsz
- Vatikánban dolgozott, hozzá küldték a titkosított szövegeket megfejtésre
- Nem ismert, hogy az araboktól vette-e át a kriptoanalízis módszereit
- Philibert Babou: I. Ferenc francia királynak dolgozott
- Szintén francia: Francois Viete, a spanyol kódolt üzeneteket törte előszeretettel
- Spanyolok boszorkánysággal vádolták

Kriptográfia

- Megindult a küzdelem a kódfejtők és a kódolók között
- Nullitások, homofonikus kódbehelyettesítés, stb…
- Uralkodók, nemesek élete múlt azon, hogy az üzeneteiket megfejtik-e vagy sem

Kriptográfia

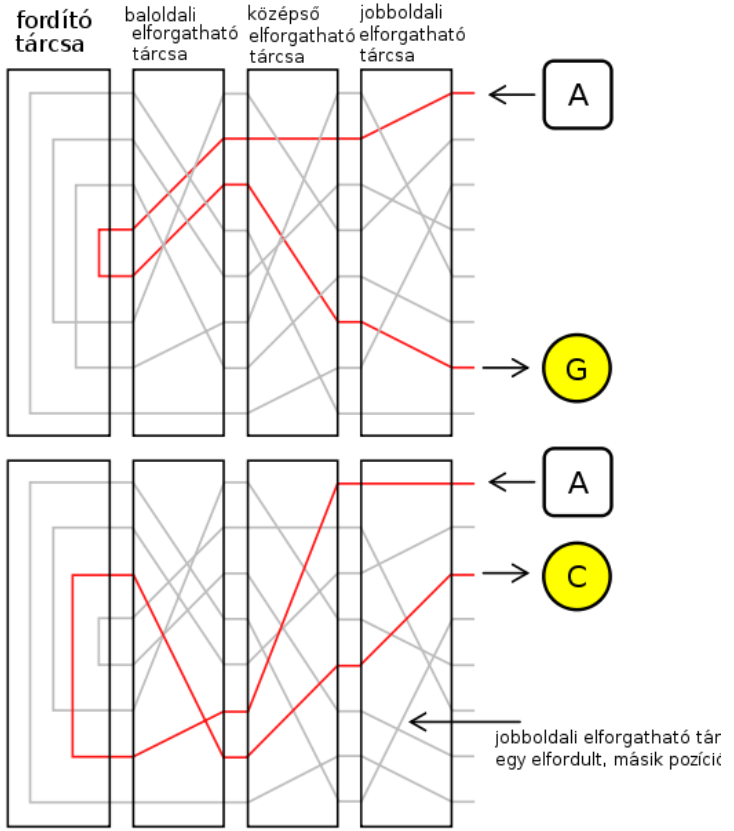
- Stuart Mária skót királynő
- VIII. Henrik testvérének, Margitnak unokája
- Katolikus volt, I. Erzsébet pedig protestáns
- I. Erzsébet VIII. Henrik és Boleyn Anna lánya: A katolikusok szemében trónbitorló
- Erzsébet fogságba ejtette Máriát
- Babington-féle összeesküvés
- Thomas Phelippes megfejtette a levelezést

Kriptográfia

- Enigma
- Arthur Scherbius német mérnök
- Feltörése kihatott

az Atlanti csatára

- Marian Rejewski
- Alan Turing
- Colossus



Kriptográfia

- Vigenere-kód

ATTACKATDAWN
LEMONLEMONLE
LXFOPVEFRNHR

	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

Kriptográfia

- Navahó kódbeszélők
- USA hadseregében szolgáltak
- Elsősorban a japánok elleni harcban alkalmazták őket
- Nem tudták megfejteni

Kriptográfia

- A megfejthetetlen kód: One Time Pad
- Az üzenetet bitsorozatként ábrázoljuk: **x**
- Szükséges egy ugyanilyen hosszú, véletlenszerű bitsorozatra: **k**
- Titkosítás: $y_i = x_i$ XOR k_i
- Megfejtés: $x_i = y_i$ XOR k_i
- A kulcsot tilos ismételni!
- Nagyon ritkán tudják alkalmazni

Kriptográfia

- A Voynich-kézirat (kb. XV. sz. eleje)