30. óra Adatvédelem

BLZS©

1010110110101011011011
1110101HACKED11110110
0001010100100001011111
1001010101010101010100
1111100111111011001000

20. század második feléig

BLZS©

A 20. század második feléig a kriptográfiát kizárólag katonai és diplomáciai alkalmazásokban használták

kriptgráfia = titkosírás, rejtjelezés

A 20. század második felétől

BLZS©

A 20. század második felétől a kriptográfia
megjelent az üzleti életben
(elsősorban banki alkalmazásokban)

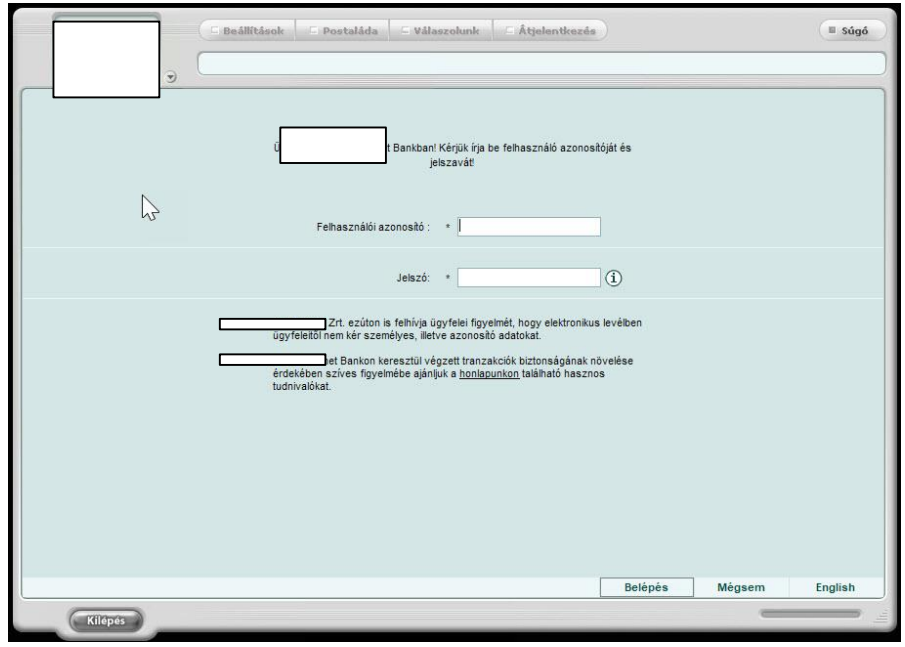
A titkosság mellett fontossá vált az integritásvédelem,
a hitelesítés, a letagadhatatlanság, stb.

A 20. század végétől

BLZS©

A 20. század végétől a kriptográfia a mindennapi élet részévé vált

- SSL (Secure Socket Layer)
- Web tranzakciók biztonsága
- GSM biztonsági architektúra – mobiltelefon-hálózat biztonság



Történelmi példák

BLZS©

„már az ókori görögök is …"
– a spártaiak szkütaléja

- i.e. 400 körül használták a spártaiak
- az üzenet betűinek átrendezésén alapszik
- kulcs = a rúd átmérője, kulcstér mérete kicsi

Történelmi példák

BLZS©

„veni, vidi, vici” – Julius Caesar rejtjelezője

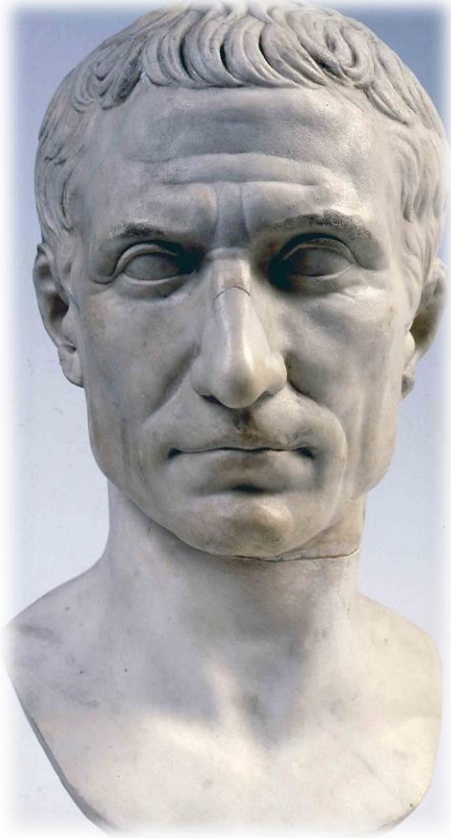
- Az üzenet betűinek helyettesítésén alapszik
- Minden betűt az ABC-ben hárommal későbbi betűvel helyettesítünk.

- nyílt: 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
- kódolt: 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

RETURN TO ROME → UHWXUA WR URPH

kulcs = az eltolás mértéke (Caesar esetén 3)

kulcstér mérete = 26-1 = 25

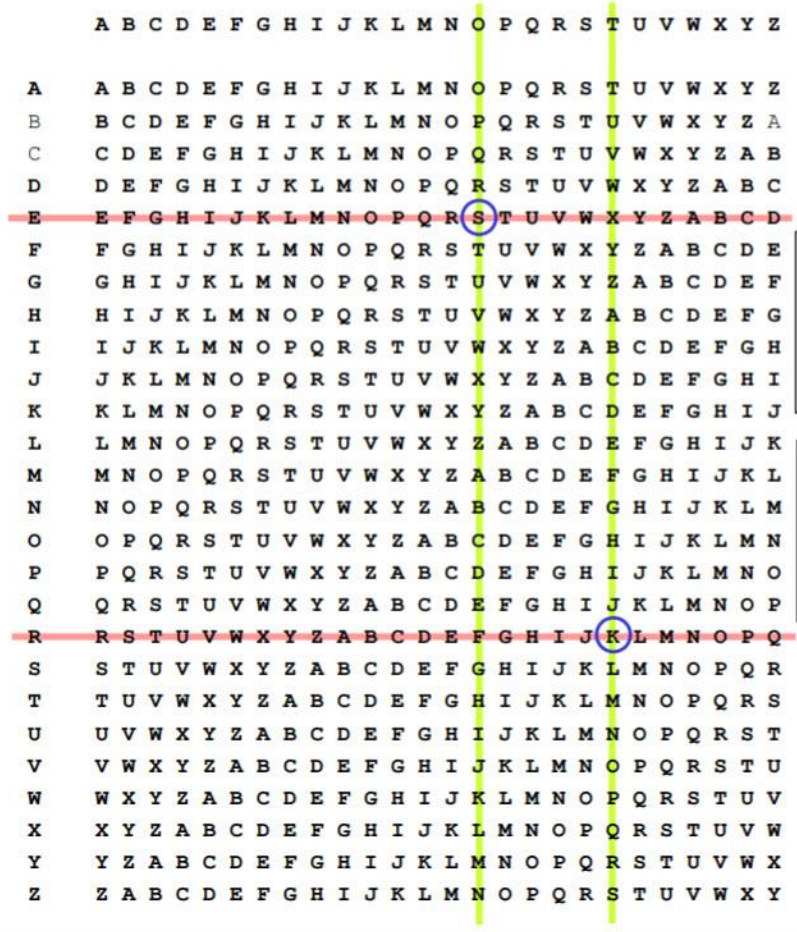


Történelmi példák

BLZS©

a „feltörhetetlen” sifre – Vigenère kód

Polialfabetikus helyettesítés – a Vigenère kód



	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:

```
        kulcs: RELAT IONSR ELATI ONSRE LATIO NSREL
  nyílt szöveg: TOBEO RNOTT OBETH ATIST HEQUE STION
rejtett szöveg: KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY
```

dekódolás:

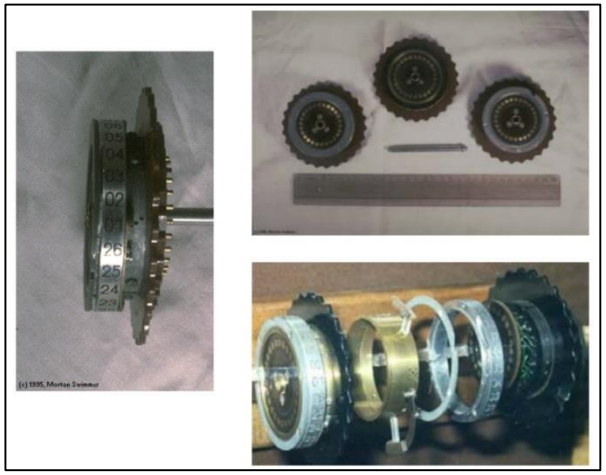
```
        kulcs: RELAT IONSR ELATI ONSRE LATIO NSREL
rejtett szöveg: KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY
  nyílt szöveg: TOBEO RNOTT OBETH ATIST HEQUE STION
```

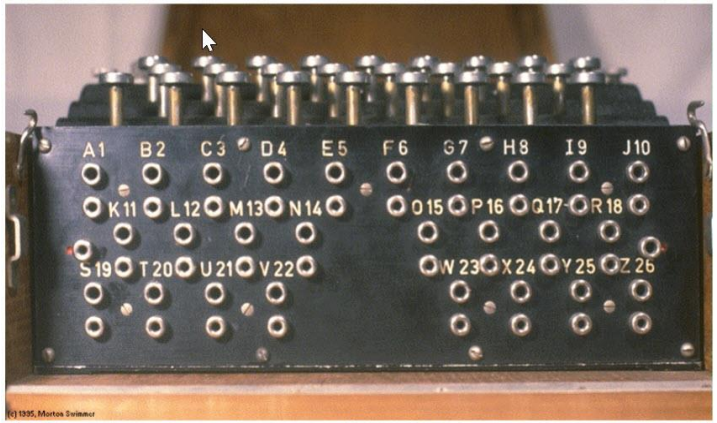
Történelmi példák

BLZS©

A rejtjelezés gépesítése – az Enigma

- az első elektromechanikus rejtjelező gép
- Arthur Scherbius szabadalma [1918]
- 1926-ban rendszeresítik a német hadseregben





Adatok védelme

BLZS©

Az adatok megóvása a külső behatásoktól valamint az eszközök közelébe jutás megnehezítése.

- Villamos hálózat helyes kialakítása
- Szünetmentes tápegységek használata (UPS)

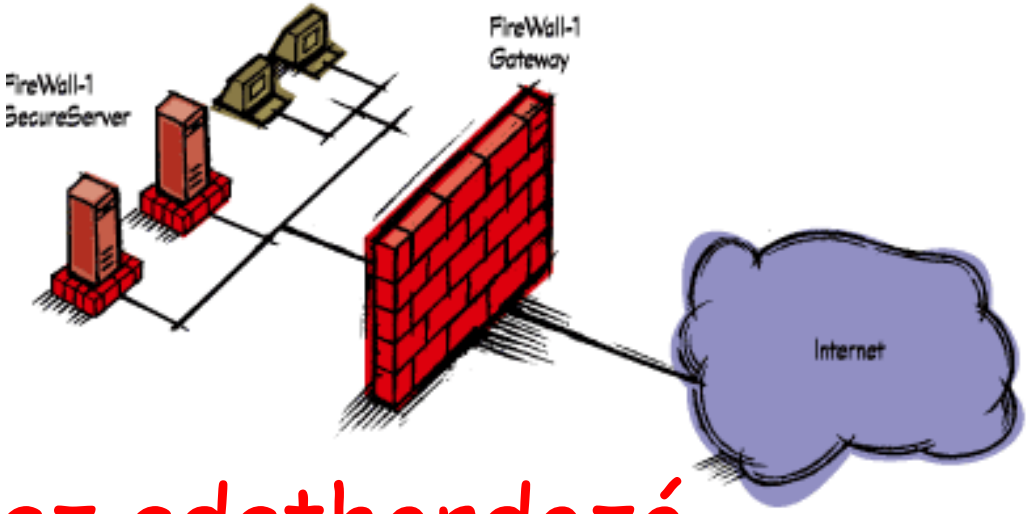
Az adatvesztések közel 50%-át a tápellátás zavaraira lehet visszavezetni.

- Megfelelő adattároló típusok kiválasztása
- Betörésvédelem

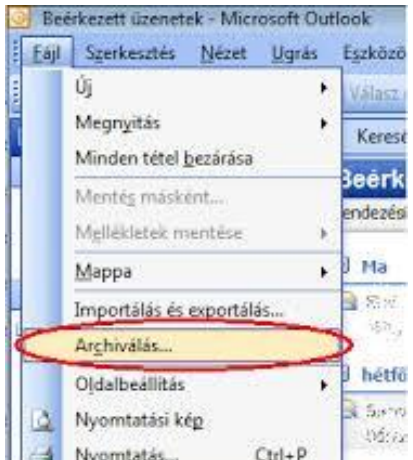
Leselkedő veszélyek

BLZS©

- Illetéktelen hozzáférés (megfelelő jelszó, tűzfal, azonosítás)



- A számítógép, vagy az adathordozó meghibásodása, sérülése (rendszeres archiválás)



Leselkedő veszélyek

BLZS©

- Vírusok
  (naprakész vírusírtó)

- Túlfeszültség,
  áramszünet (UPS)

- Jogi kérdések
  (szerzői jogok)