

INFORMATIKAI BIZTONSÁG ALAPJAI

4. előadás

Göcs László

főiskolai tanársegéd

Neumann János Egyetem GAMF Műszaki és Informatikai Kar

Informatika Tanszék

Titkosítás, hitelesítés



Titkosítás

A **titkosítás** vagy **rejtjelezés** a kriptográfiának az az eljárása, amellyel az **információt** (*nyílt szöveg*) egy **algoritmus** (*titkosító eljárás*) segítségével olyan szöveggé alakítjuk, ami olvashatatlan olyan ember számára, aki nem rendelkezik az olvasáshoz szükséges speciális tudással, amit általában **kulcsnak** nevezünk.

Az eredmény a titkosított információ (*titkosított szöveg*). Sok titkosító eljárás egy az egyben (vagy egyszerű átalakítással) használható megfejtésre is, azaz, hogy a titkosított szöveget újra olvashatóvá alakítsa.

Mire való a titkosítás?

Értékes információ elrejtésére

Lehetővé teszi:

- Személyiségi jogaink megőrzését
- Információkhoz való hozzáférés szabályozása
- Elektronikus fizetőeszközök használatát
- Privát és üzleti ügyeink biztonságos intézését

Titkosítás

Egy üzenet olyan leképezéseA védett titkos információ tudománya

Kriptográfia

Olyan módszerrel foglalkozik, amelyek biztosítják az üzenetek vagy tárolt információk titkosságát, védettségét, hitelességét.

Mire való a titkosítás?

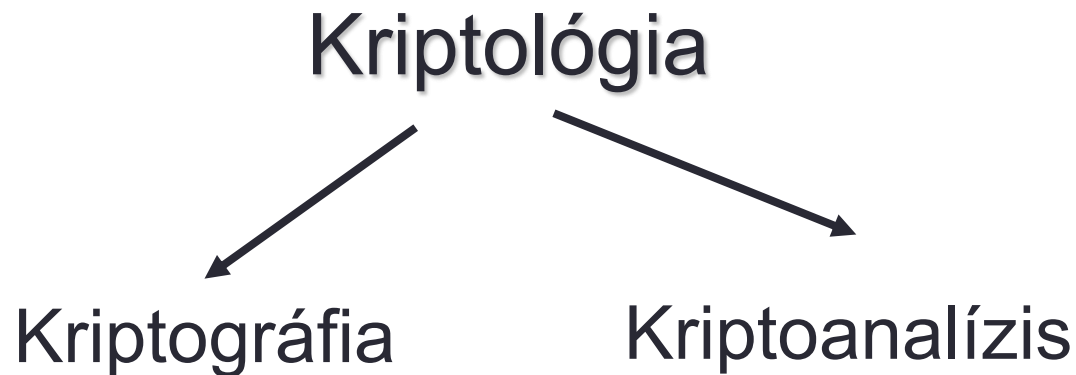
Kriptoanalízis

A titok – többnyire illetéktelen – megejtésére, feltöésére irányuló eljárásokkal foglalkozik.

A kriptográfia alapvető feladata

- Biztosítsa azt, hogy bizonyos adatok, csak az azok felhasználására kijelölt körben legyenek elérhetőek, ne juthassanak **illetéktelenek** birtokába.

A kriptológia „a szó rejtésének tudománya”, a görög „**krüptosz**” (rejtett) és a „**logosz**” (szó) szavakból származik.



A **kriptográfia**

(„**grafo**” görögül azt jelenti: írni) tudománya olyan módszerek (algoritmusok) kidolgozásával foglalkozik, amelyek biztosítják az üzenetek:

- titkosságát;
- védettségét;
- hitelességét.

A **kriptoanalízis** a kriptográfiai algoritmusok vizsgálatával foglalkozik.

Célja általában

- az algoritmus „feltörése”, vagyis a rejtett üzenet illetéktelen megfejtése vagy
- az algoritmus kijátszása/manipulálása illetve
- annak bizonyítása, hogy egy algoritmus egy bizonyos támadásellen védett.

- **kriptográfia**, mely olyan módszerekkel foglalkozik, amelyek biztosítják az üzenetek vagy tárolt információk **titkosságát**, **védettségét**, illetve **hitelességét**.

Matematikai módszereket alkalmazó algoritmusok az eszközei, amelyek használatának pontos leírását a **kriptográfiai protokollok** tartalmazzák.

- **kriptoanalízis**: a titok – többnyire illetéktelen – megfejtésére, feltörésére irányuló eljárásokkal foglalkozik.

A kriptográfia legalapvetőbb szolgáltatásai:

- Titkosítás
- Hitelesítés
- Partnerazonosítás
- Digitális aláírás és időpecsét
- Hozzáférés-védelem, jogosultság
- Eseménynapló

- **Titkosítás:**

egy üzenet olyan leképezése, átalakítása, hogy annak információtartalma **csak meghatározott eszközök birtokában** állítható vissza. Az üzenet bármilyen típusú állomány lehet, titkosítására **kulcsot** használnak. Ezzel lehet az állományt visszafejteni.

Az adattitkosítás leírható *matematikai függvény*nyel, amely az eredeti szöveghez **P** a kódolt szöveget **$e(P)$** rendeli.

- **Hitelesítés:**

a tárolt adatok vagy kommunikációs üzenetek tartalmára vonatkozó védelmi eljárás. Az adatokat a **hamisítás, manipulálás, megváltoztatás, kiegészítés** ellen védi. Azt bizonyítja, hogy az adatok a keletkezésük óta nem változtak.

- **Partnerazonosítás:**

a partnerek kétséget kizáró, **kölcsönös azonosítására** használt eljárás. A küldő biztosítja, hogy az üzenetet csak az általa kiválasztott vevő partner értheti csak meg, a fogadó fél pedig egyértelműen tudja bizonyítani, hogy az üzenetet a küldőtől kapta.

- **Digitális aláírás és időpecsét:**

Az üzenethez kapcsolva képes **bizonyítani** azt, hogy ki volt az üzenet kibocsátója, és hogy az üzenet **sértetlen**. Az időpecsét pedig a **keletkezés idejét** bizonyítja, így véd az újra kibocsátás ellen.

- **Hozzáférés-védelem, jogosultság:**

a „valamit tud és valamivel rendelkezik” elvet alkalmazva valósítja meg a különféle informatikai rendszerekhez való **szelektív** hozzáférést. Jelszavakat menedzselő, ellenőrző, illetve hozzáférési jogosultságot és hardverkulcsot kezelő részekből áll.

- **Eseménynapló:**

automatikusan rögzíti az informatikai rendszerben történő **összes lényeges aktivitás időpontját** és körülményeit. Beállításai és működési mechanizmusai csak a legmagasabb jogosultsággal rendelkező felhasználók számára elérhetőek.

Biztonsági célok / szolgáltatások

1. Bizalmasság (Confidentiality, privacy, secrecy)

Csak azok érhessék el az információt, akik arra jogosultak.

2. Sértetlenség (data Integrity)

Védelem az adatok jogosulatlan módosítása ellen
pl. beszúrás, törlés, helyettesítés.

3. Hitelesség (Authenticity)

- a kommunikáció szereplőinek hitelesítése (partner authentication)
- az üzenetek hitelesítése
(eredet, tartalom, küldési idő, stb., message authentication)

4. letagadhatatlanság (non-repudiation)

A digitális biztonság fogalomkörében a letagadhatatlanság azt jelenti, hogy biztosítjuk

- az üzenet elküldését
- Az üzenet a jogosult ügyfélhez küldődjek el
- A jogosult ügyfél kapja meg

A letagadhatatlanság olyan eljárás, amellyel garantálni lehet, hogy

- a feladó később ne tagadhassa le az üzenet elküldését;
- a fogadó ne tagadhassa le, hogy megkapta az üzenetet.

Pl. **"elektronikus aláírás"** = az üzenet hitelesítése + letagadhatatlansága"

A kriptográfia alapvető feladatai

- rejtjelezés/megfejtés (*encryption/decryption*)
- elektronikus aláírások, időpecsétek (*digital signature, time stamp*)
- hitelesítés (*certification*)
- partnerazonosítás – identifikáció (*identification*)
- azonosító hitelesítése – autentikáció (*authentication*)
- jogosultságok kiosztása – autorizálás, tulajdonság birtoklás (*authorization, attribute ownership*)
- hozzáférés szabályozás (*access-control*)
- titokmegosztás, titokszétvágás (*secret sharing/spitting*)

Alkalmazási területek

- titkosított üzenetküldés (encryption)
ez a klasszikus kriptográfia
- hozzáférés szabályozás (access control)
pl. szoftverek, adatbázisok védelme, pay per view TV csatornák
- banki tranzakciók
- elektronikus kereskedelem
vevő+bank+bolt, mindenki csak a rá tartozó információkat lássa
- elektronikus pénztárca
- elektronikus szavazás (*anonimitás is kell !*)
- elektronikus publikáció

A kriptográfiai algoritmus biztonsága függ

- a választott algoritmus erősségétől
- a kulcs hosszától

Jó algoritmus esetén a **kulcshossz növelésével** a biztonság növelhető.

Például:

Ha egy algoritmus csak teljes kipróbálással (Brute Force) törhető, akkor plusz egy bit kétszeres biztonságnövelést jelent.

Alapkérdés: Mit-, ki ellen-, mennyi ideig kell védeni?

Rejtés és /vagy titkosítás

- 2000-2500 évvel ezelőttől: rejtés (**szteganográfia**)
 - Pl. betűk észrevétlen megjelölése ártatlannak látszó *(fedő) szövegben. (tűjelek, láthatatlan tinták...)*
- A mai alkalmazásai: kereskedelmi, **copy right** információk elrejtése (képben, mozgó képben, hangfájlokban. Elektronikus vízjel.
- Igen fejlett technikák vannak rá, amelyek „kibírják” a fedő kép, hang szöveg... szerkesztését, másolását is.
- A szteganográfia azonban más, mint a kriptográfia. *(jóllehet együtt is alkalmazhatók)*

Kriptográfia - szteganográfia

A **szteganográfia** (adatrejtés, datahiding)

A kommunikáció művészete és tudománya, lehetőség magának a kommunikációnak az elrejtésére. Ellentétben a kriptográfiával, ahol a támadó észreveheti, feltörheti és módosíthatja az üzenetet, a szteganográfia célja, hogy a **nyílt szöveget úgy rejtse el** a gyanúmentes üzenetbe, hogy a **támadó ne is láthassa** meg, hogy a továbbított üzenet egy második – esetleg titkosított – üzenetet tartalmaz (Markus Kuhn 1995)

Például

- láthatatlan tintával
- rabszolga fejbőrére írva (*hátránya meg kell várni, míg kinő a haja*)
- képben a színeket leíró bájtok alacsony helyiértékű bitjeiben (*szemre nem látható*)
- szórt spektrumú adásban (*fehér zajként észleli a külső megfigyelő*)

Kriptográfia – szteganográfia példák

- *A kínaiak finom selyemszövetre írtak, összegyúrták viaszba forgatták, majd a viaszgolyót az üzenet vivője lenyelte.*
- *Főtt tojás héjára timsóból, és ecetből készült tintával írva, beszívódik és a fehérjén lesz olvasható az üzenet.*
- *A II. világháborúban elterjedt a mikropont, melyben 1 gépelt oldalt 1mm-es pöttyé zsugorítanak.*
- *1. Réz-szulfát (CuSO_4) vizes oldata világos kék. Ha ammónium-hidroxid (NH_3) oldat fölé tesszük, akkor sötét kék lesz. Így láthatóvá válik a papíron.*
($\text{Cu}^{2+} + \text{NH}_3 \rightarrow [\text{Cu}(\text{NH}_3)_4]$)
- *2. Kobald-klorid (CoCl_2) vizes oldata halvány rózsaszín (így nem látszik a papíron). Melegítve öngyújtó felett a vízvesztés miatt kék lesz. Ha megszárad újra eltűnik.*
- *3. Kálium-nitráttal (KNO_3) írva nem látszik, de parázssal "megégetve" az izzás tovaterjed az íráson, mert a kálium-nitrát táplálja a parazsat.*

Titkosító kódolók

- **a helyettesítő kódolók** megtartják az eredeti szöveg karaktereinek sorrendjét, csak azokat más alakkal ruházzák fel;
- **a keverő kódolók** nem keresnek más betűalakot, de az eredeti sorrendet átalakítják.

Betűhelyettesítés

A legegyszerűbb titkosírások

A módszer hátránya:

- ***a betűgyakoriság problémája***

(A nyelvben is vannak gyakrabban előforduló betűk, pl. a magyarban az E,A,T,O,L. Ha megfelelő hosszúságú kódolt szöveg kerül illetéktelen kezébe, gyakoriságanalízissel az információ esetleg megfejthető.)

- ***a betörési pont problémája***

(Ismert nevek, fogalmak, dátumok szerepelhetnek a kódolt szövegben, amelyek könnyen kitalálhatók, így sok betűpár ismertté válik.)

Titkosítás

Az üzenet küldője egy titkos **eljárást** (kulcsot), használ az üzenet titkosítására

A címzett **ugyanazt a kulcsot ismeri**, így az üzenetet vissza tudja fordítani (**dekódolni**).

A kulcs átadásához **biztonságos csatorna** szükséges.



Titkosítók generációi

- **Első generáció:** XVI-XVII. századig, főleg egyábécés helyettesítések (pl. Caesar)
- **Második generáció:** XVI-XIX században, többábécés helyettesítések (pl. Vigenére)
- **Harmadik generáció:** XX sz. elejétől Mechanikus és elektromechanikus eszközök (pl. Enigma, Hagelin, Putple, Sigaba)
- **Negyedik generáció:** a XX. század második felétől produkciós titkosítók, számítógépekkel (pl. DES, Triple DES, Idea, AES)
- **Ötödik generáció:** kvantumelvű titkosítások, sikeres kísérletek vannak rá.

- Caesar titkosítása: betűhelyettesítés
- 1600-as évekig: kódszavak, betűhelyettesítés, titkos írásjelek, mind triviálisan feltörhető
- Balise de Vigenère (1523-1596): nagy lépés, a Vigenère féle titkosítás: a nyílt szöveg is része a kulcsnak. 200 évig nem tudták feltörni.
- Gyorsulás 1900-tól
- Második világháború: kriptográfia és kriptóanalízis alapvető fontosságú (pl. *Enigma* és megfejtése)
- 1976: DES és a nyílt kulcsú titkosítás (Diffie-Hellman), RSA

- 1991: Phil Zimmermann – PGP
- 1994: RC5
- 2000: AES (Rijndael)

Caesar-féle helyettesítéssel módszer (monoalfabetikus helyettesítés)

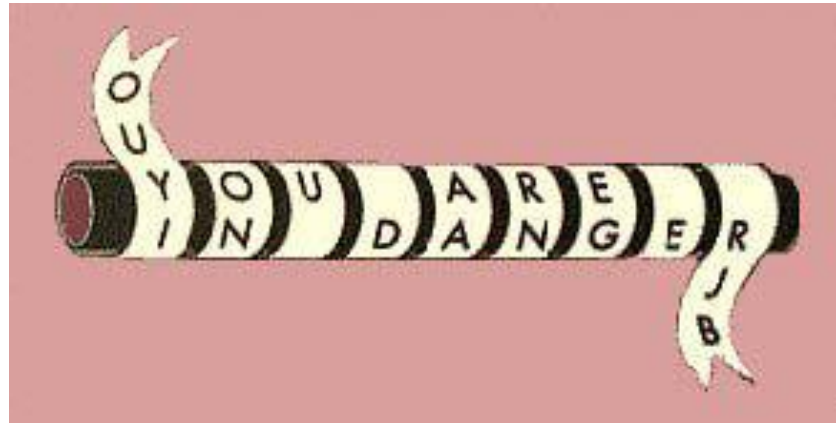
- Minden betűt az ábécében a hárommal utána következővel helyettesített (Kulcs=3)
(általánosítottabb változatában $0 < \text{Kulcs} < 26$)
- xxxxxxxxxxxx szónak **LQIRUPDWLND** felel meg
?

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
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

A szkütalé

A szkütalé

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



Polübiosz-féle titkosítás

- Minden betűhöz egy kétjegyű számot rendelt (sor-oszlop azonosítót)

pl: **252122113221**

?

	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

KFGAMF

2111131512343425

321113432511241133134324

	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

Tetszőleges monoalfabetikus helyettesítés

- abcdefghijklmnopqrstuvwxyz
QWERTZUIOPASDFGHJKLYXCVBNM
vagy
- abcdefghijklmnopqrstuvwxyz
✌️🌀🌀🌀🌀♂️🐉🌀🌀er&●○■□□□□◆◆◆❖◆☒☒⌘

A monoalfabetikus helyettesítéses titkosítás feltörése

- Az adott nyelvre vonatkozó, már az **ókorban** is ismert **betűgyakorisági táblázat** segítségével
- Nem fedik el a betűk előfordulási gyakoriságát

Jules Verne: Sándor Mátyás

A
titkosírások több irodalmi műben
fontos szerepet kapnak.
Jules Verne: Sándor Mátyás
című regényében is
találkozhatunk az
átrendezéses titkosításnak
egy érdekes példájával:

R	H	G	A	A	Z
Ü	Y	G	G	R	É
A	F	X	S	G	M
N	T	L	Á	R	É
E	Z	L	F	T	É
S	E	R	É	O	G

	X		X		X
				X	
		X			
	X			X	
					X
			X		

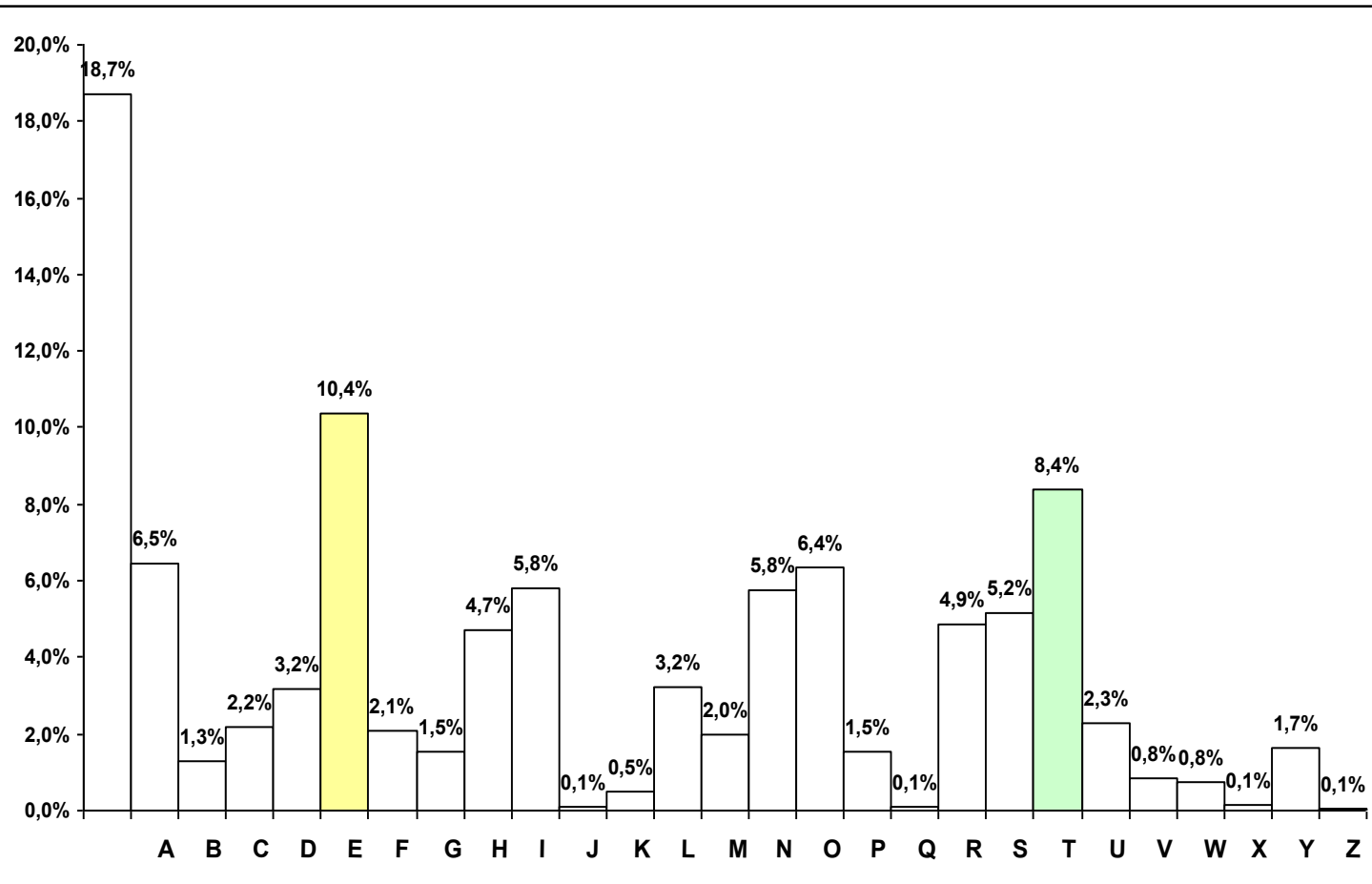
Ráhelyezve a szövegre a lyukak (X) helyén felbukkanó betűket leírva, majd a rostélyt negyed fordulattal elfordítva a következő szöveg jön ki:

H	A	Z	R	X	T	R	É	É
G	É	S	N	E	L	T	E	G
G	Ü	F	G	Á	Z	S	R	O
R	A	Y	G	A	M	L	E	F

*Torontál Simon bosszúságára érthetetlen szöveg jön ki,
de **vissza felé** olvasva:*

...FELMAGYARORSZÁGFÜGGETLENSÉGÉÉRTXRZAH

Az angol nyelv betűgyakorisága



de Vigenére-féle több ABC-s titkosítás

- **Betűmátrixot** használt
- **Elfedi** az élő nyelv betű előfordulási gyakoriságát:
 - ugyanazoknak a betűknek más jel felel meg a kriptoszövegben,
 - különböző betűknek ugyanaz a jel is megfelelhet a kriptoszövegben.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

de Vigenére-féle több ABC-s titkosítás

- Kulcs: **GHYMES**
- A titkosítandó szöveg
EGYINFORMATIKUSNAKSOKATKELLTANULNI
- A kulcsszó betűje által mutatott sor és a szöveg betűje által meghatározott oszlop kereszteződésében levő betűt helyettesítjük
- **GHYMESGHYMESGHYMESGHYMESGHYMESGHYME**
- **EGYINFORMATIKUSNAKSOKATKELLTANULNI**
- **KNWURXUYKMXAQBQZECYVIMXCKSJFEFASLU**

Keverő kódolók

- **Oszlop alapú keverő**

Kulcs nem tartalmazhat azonos karaktereket!

A kulcs szerepe: az oszlopok megszámozása

- A plaintextet a kulcs hosszúságának megfelelő blokkokra tördeljük,
- A blokkokat egymás alá helyezzük
- A kulcsnak megfelelő sorszámozással az oszlopokat összefűzzük a kriptoszöveggé.

Oszlop alapú keverő

- Kulcs: **GHYMES**

- Plaintext:

EGYINFORMATIKUSNAKSOKATKELLTANULNI

- Kriptoszöveg?

NTATAXEOKSEUGRUOLLIANATIFIKNXYMSKLN

- GHYMESGHYMESGHYMESGHYMESGHYMESGHYMES
- EGYINFORMATIKUSNAKSOKATKELLTANULNIXX

236415 (a kulcs betűinek sorrendje az abc-ben)

EGYINF

ORMATI

KUSNAK

SOKATK

ELLTAN

ULNIXX

- NTATAXEOKSEUGRUOLLIANATIFIKKNXYMSKLN

Oszlop alapú keverő kódolással készült az alábbi kriptoszöveg.

W A E C O X N O U N A N T K H I I X E R T T T X

A kulcs: HOME.

Mi a Plain text? (szereplejen a megoldáshoz vezető út)

W A E C O X N O U N A N T K H I I X E R T T T X

H O M E

2 4 3 1

N	E	T	W
O	R	K	A
U	T	H	E
N	T	I	C
A	T	I	O
N	X	X	X



NETWORKAUTHENTICATIONXXX

ENIGMA

- II. világháború kulcsszerepet játszó kódoló eszköze
- a németek fejlesztették ki, a lengyelek (*Marian Rejewski*), majd az angolok fejtették meg

1918 körül tervezte *Arthur Scherbius* Németország-ban, és mintegy tíz évvel később kezdték általánosan használni a hadseregben a légi- és tengeri erőknél, valamint néhány kormányzati szervnél, illetve az üzleti életben.



ENIGMA részei



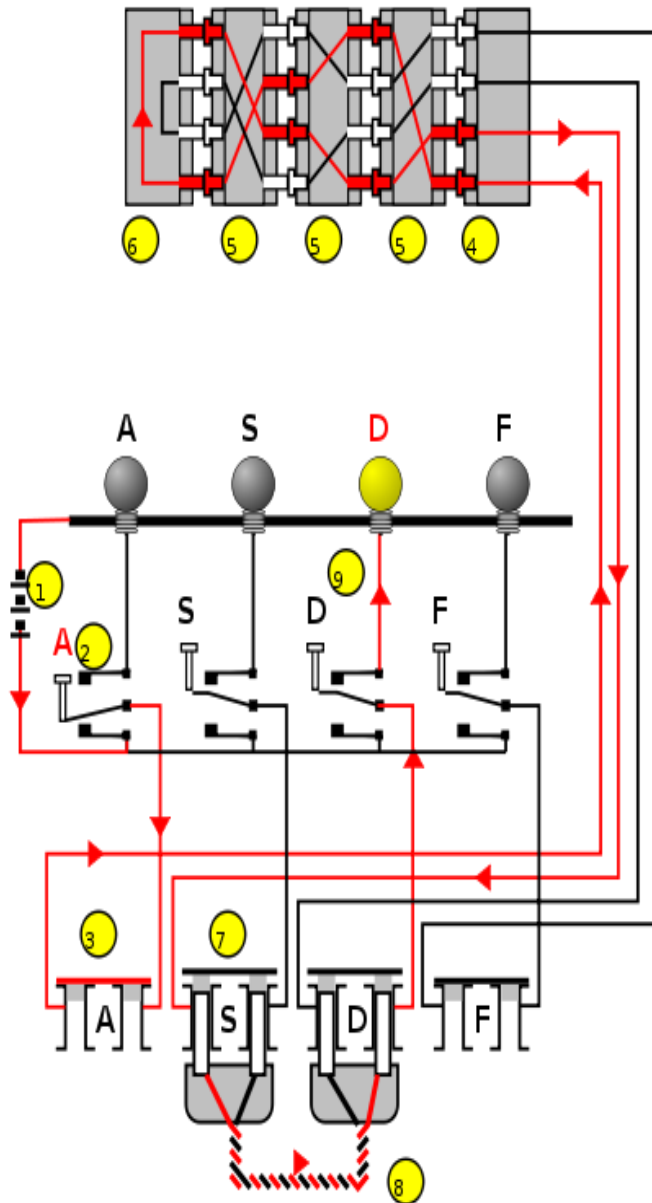
három forgó tárcsa
(rotor) + reflektor

egy 26 lámpás kijelző, ami a
titkosítás és a megfejtés
eredményét mutatta

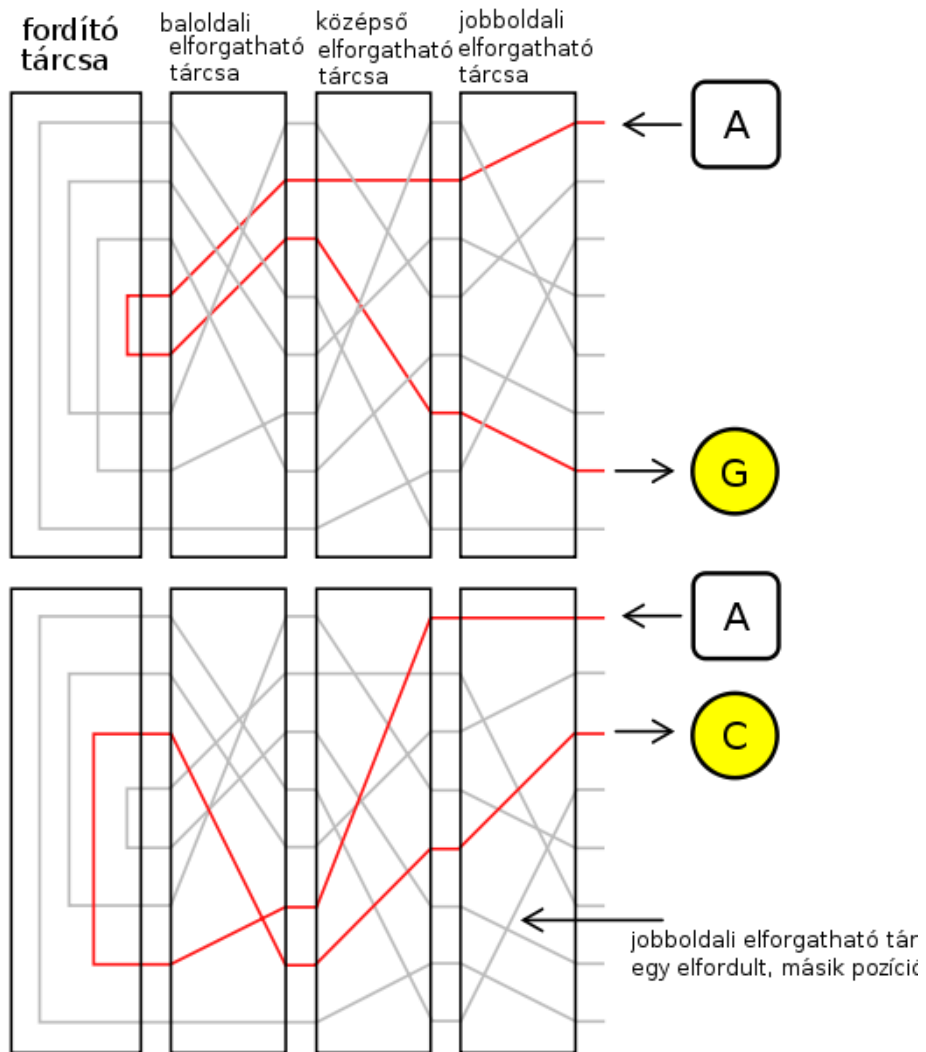
Billentyűzet 26 betű

Kapcsolótábla
stecker

ENIGMA



- Minden tárcsának 26 beállítási helyzete van.
- A 26 harmadik hatványa 17.576.
- Ha ezt összeszorozzuk a tárcsa-kiválasztás lehetséges eseteinek számával (60), 1.054.560-at kapunk eredményül.
- Ha ezt az eredményt megszorozzuk a lehetséges kapcsolótábla csatlakozások számával ami kb. 150 billió!
- Tehát az Enigma 150 trillió módon állítható be a rejtjelezést megelőzően.



Egy négyrotoros Enigma-variáns



A titoktartást 1970-ben oldották fel, és a világ ekkor szerzett csak tudomást a Bletchley Park létezéséről és az Enigma feltöréséről

A történészek becslése szerint az Enigma feltörése nélkül a háború akár 1948-ig is eltarthatott volna !

A Navajo-kód

A világháború alatt más titkosító gépeket is használtak (Japán – purple, Brit – Type-X, USA – SIGABA). A csendes-óceáni hadviselés során rádöbbentek a rejtjelező gépek legnagyobb hátrányára, a lassúságukra.

Navajo-kódbeszélők

- Sok, angolul jól beszélő férfi
- Olyan nemzetség, ahol nem jártak euópai kutatók

A gyakran használt katonai kifejezéseknek kerestek navajo megfelelőt.

(pl.: vadászgép → kolibri, bombázó → keselyű, csatahajó → bálna)

Amiknek nem volt megfelelőjük, lebetűzték.

420 Navajo-kódbeszélő teljesített szolgálatot a II. világháborúban.

A – Ant – vo-la-csi

B – Bear – sus

C – Cat – moaszi

D – Deer – Be

E – Elk – Dze

F – Fox – Mae

.

.

.

<http://www.history.navy.mil/faqs/faq61-4.htm>

Titkosítás, hitelesítés 2



Könyvajánló

Virasztó Tamás

Titkosítás és adatrejtés

Biztonságos kommunikáció és algoritmikus adatvédelem



NetAcademia Oktatóközpont

VÉDELEM

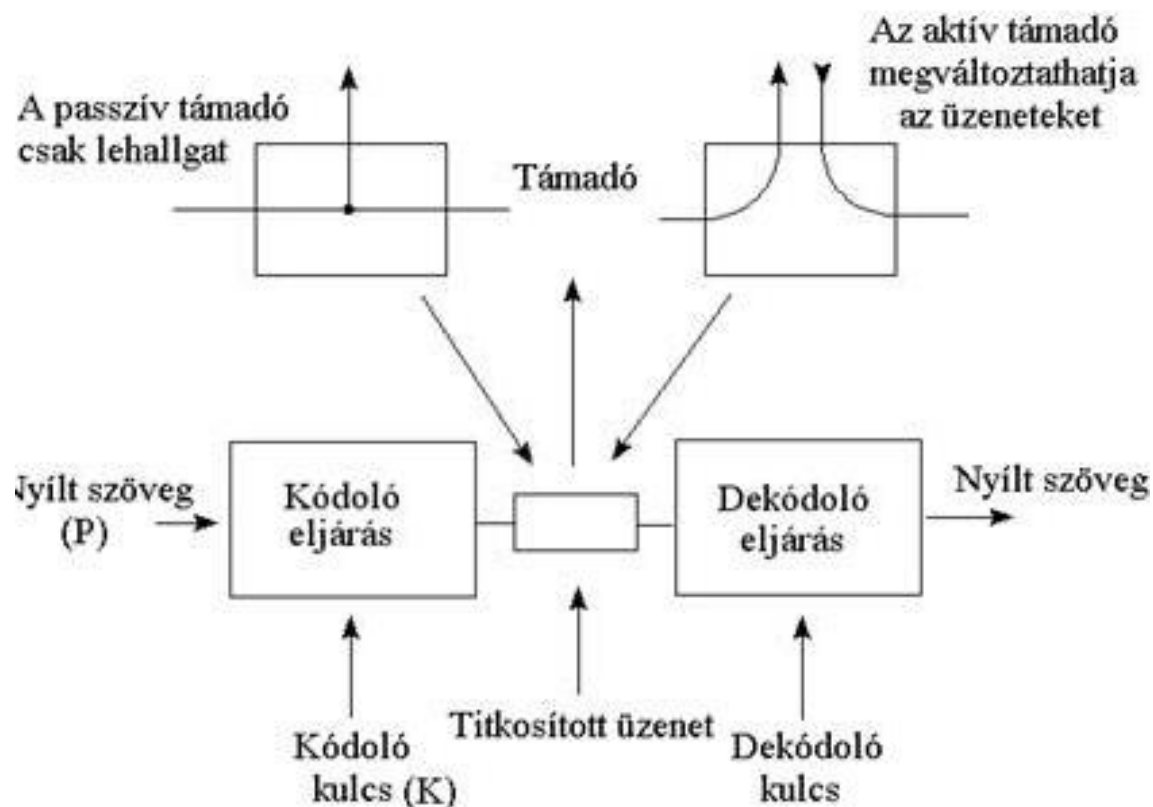
- Mit kell védeni?
Az információt.
- Melyik információt kell védeni?
Az értékeset.
- Mi az értékes információ?
Amit annak tartunk.
- Hol van az értékes információ?
Adathordozón vagy átviteli csatornán.
- Mitől kell védeni az értékes információt?
Megsemmisüléstől, eltulajdonítástól.

VÉDELEM

- Azt az üzenetet, adatot, amit el akarunk küldeni **nyílt szövegnek** (plaintext, cleartext) nevezzük. □
- Azt a műveletet, amely a nyílt szöveget, annak értelmét vagy más jellemző tulajdonságait elrejtí, **titkosításnak** nevezzük (enciphering, encryption). Eközben valamilyen kriptográf algoritmust (cipher).
- A létrejövő értelmezhetetlen adathalmazt **titkosított** vagy kriptoszövegnek (ciphertext) nevezzük. □
- a titkosított szöveg nyílt szöveggé való jogosult visszaalakítását **megfejtésnek** (deciphering, decryption) nevezzük. □
- a titkosított szöveg nyílt szöveggé való jogosulatlan (értsd: kulcs nélküli) megfejtését **visszafejtésnek** vagy **feltörésnek** nevezzük.
- és mindehhez kell a **kulcs** (key).

Kriptográfia

- A kriptográfia alapvető feladata, hogy **algoritmus eszközökkel** biztosítja azt, hogy a védett adatok csak az azok felhasználására kijelölt körében legyenek elérhetőek, **ne juthassanak illetéktelenek** birtokába.



KERCKHOFFS-elv

„ A kódolási rendszer megbízhatósága nem függhet a titkosítási algoritmustól, azt a csak a kulcs titkának megőrzésére szolgál”

Ha a kulcs **kompromittálódik**, akkor elegendő a kulcsot lecserélni, maga az eljárás tovább alkalmazható.

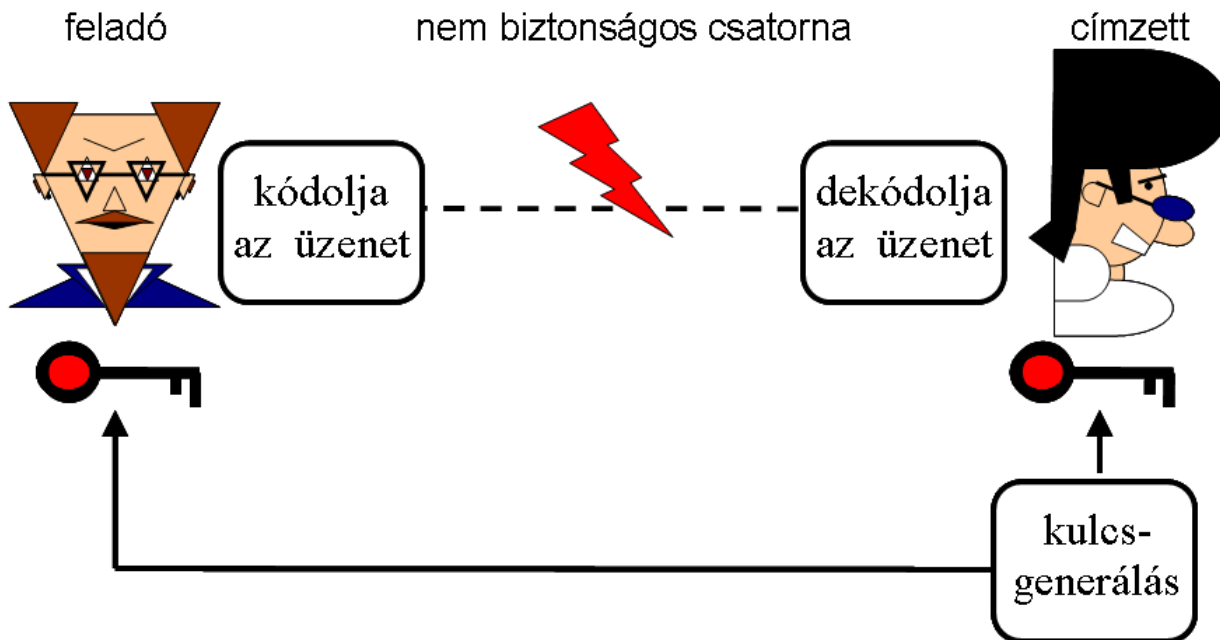
SZIMMETRIKUS KULCSÓ TITKOSÍTÁS

Olyan kriptográfiai módszerek tartoznak a szimmetrikus kulcsú kriptográfia körébe, amelyek esetén **kódoláshoz és dekódoláshoz ugyanazt a kulcsot** használjuk.

Az ilyen eljárások biztonsága a **kulcs titkosságán** alapszik.

Ilyen titkosítási algoritmusok például a következők:

- DES,
- 3DES,
- AES,
- Blowfish,
- RC4



Függetlenül attól, hogy a kulcsot hol generáljuk - a kulcs **biztonságos, titkos** csatornán kell, hogy **eljusson** mind a kódolóhoz, mind a dekódolóhoz.

A kulcsként használt információ tehát a rejtjelezéshez használt algoritmus egyik paramétere. Ha m a titkosítandó üzenet, és k a titkos kulcs,

$$\text{akkor az } \mathbf{M} = \mathbf{C}_k(\mathbf{m})$$

összefüggés adja meg a titkosított üzenetet. A \mathbf{C}_k titkosító függvény vagy algoritmus a következő tulajdonságokkal bír:

- titkosított \mathbf{M} üzenet a k kulcs ismeretében könnyen kiszámítható – ez a **titkosítás folyamata**.
- A titkosított \mathbf{M} üzenetből könnyen kiszámítható az eredeti üzenet, de csak akkor, ha ismerjük a k kulcsot – ez az **üzenet megoldása**.
- A titkosított \mathbf{M} üzenetből nem lehet meghatározni az eredeti üzenetet, ha nem ismerjük a k kulcsot. Ez akkor sem végezhető el, ha ismerjük a titkosító függvény felépítését, vagyis a \mathbf{C} titkosító algoritmus **csak a k kulcs ismeretében** invertálható. Ez a tulajdonság garantálja a Kerckhoffs-elv betartását.

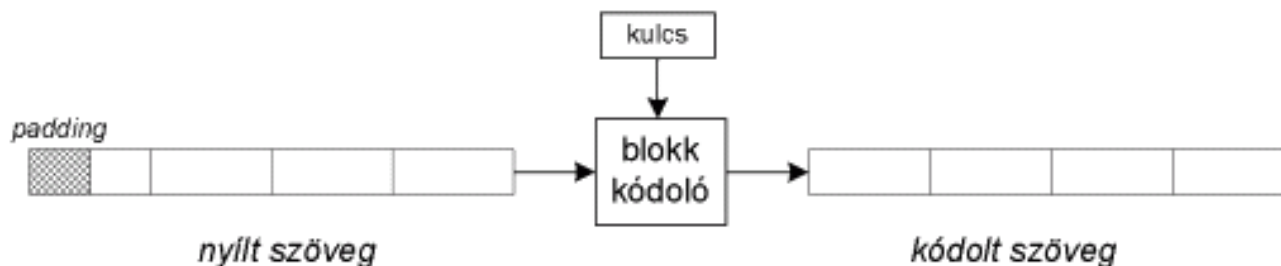
Az ilyen trükkös eljárásokat csapdafüggvényeknek (trapdoor functions) nevezzük. A vissza- felé vezető út, vagyis a titkosított üzenet visszaállítása, elolvasása az

$$\mathbf{m} = \mathbf{D}_k(\mathbf{M}) = \mathbf{C}^{-1}_k(\mathbf{M})$$

egyenlettel írható le, ahol \mathbf{D}_k a **megoldó algoritmus**. Tulajdonképpen a \mathbf{C} titkosító algoritmus **inverze**, ezért \mathbf{C}^{-1} módon is jelölhetjük.

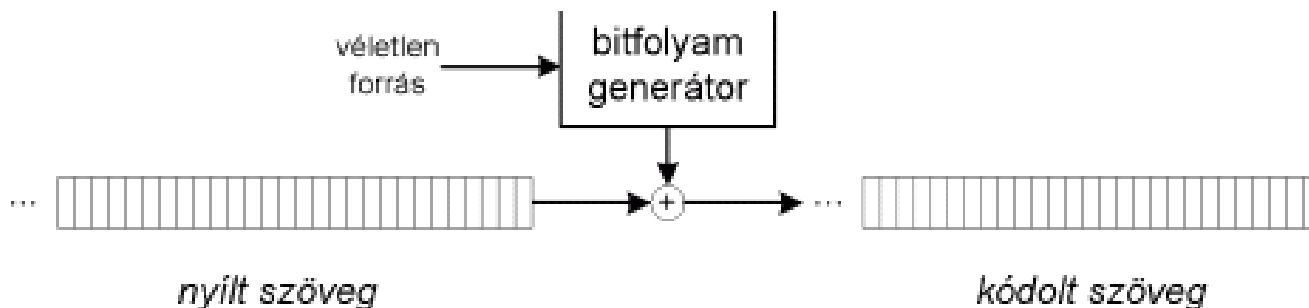
Blokk kódolók

- Az üzenetet adott méretű üzenet blokkra kell felosztani (egy blokk általában 64-128 bit)
- Ha az üzenet-darab nem tesz ki egy teljes blokkot, gondoskodni kell a teljes kiegészítésről (padding).



Folyamat kódolók

- A folyamatában érkező üzenetet kisebb egységeként (pl. bájt) képesek kódolni.
- RC4, SEAL, VRA, A5...



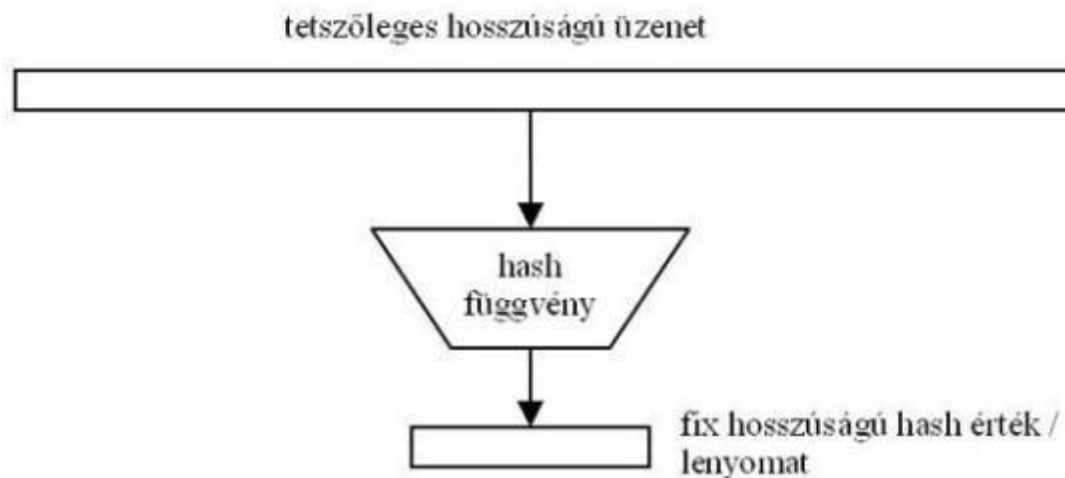
HASH függvények

Egy hash függvény tetszőleges hosszúságú üzenetet **fix hosszúságú** bitsorozatba képez le.

Az így kapott eredményt „**hash értéknek**” vagy „**lenyomatnak**” is nevezik.

Mivel a bemenet hossza nagyobb, mint a lenyomat vagyis a kimenet hossza, így elvileg nem kizárt, hogy két különböző üzenet hash értéke megegyezik.

HASH függvények



A gyakorlatban a legelterjedtebb hash az **SHA-1**, bár sokat használgják a már nem biztonságos MD5 függvényt is. Az MD5 128 bites, a SHA-1 160 bites hash értéket állít elő, viszont mindkettő 512 bites blokkokban dolgozza fel az üzeneteket.

PROTOKOLOK

- **Rejtjelező struktúrák**

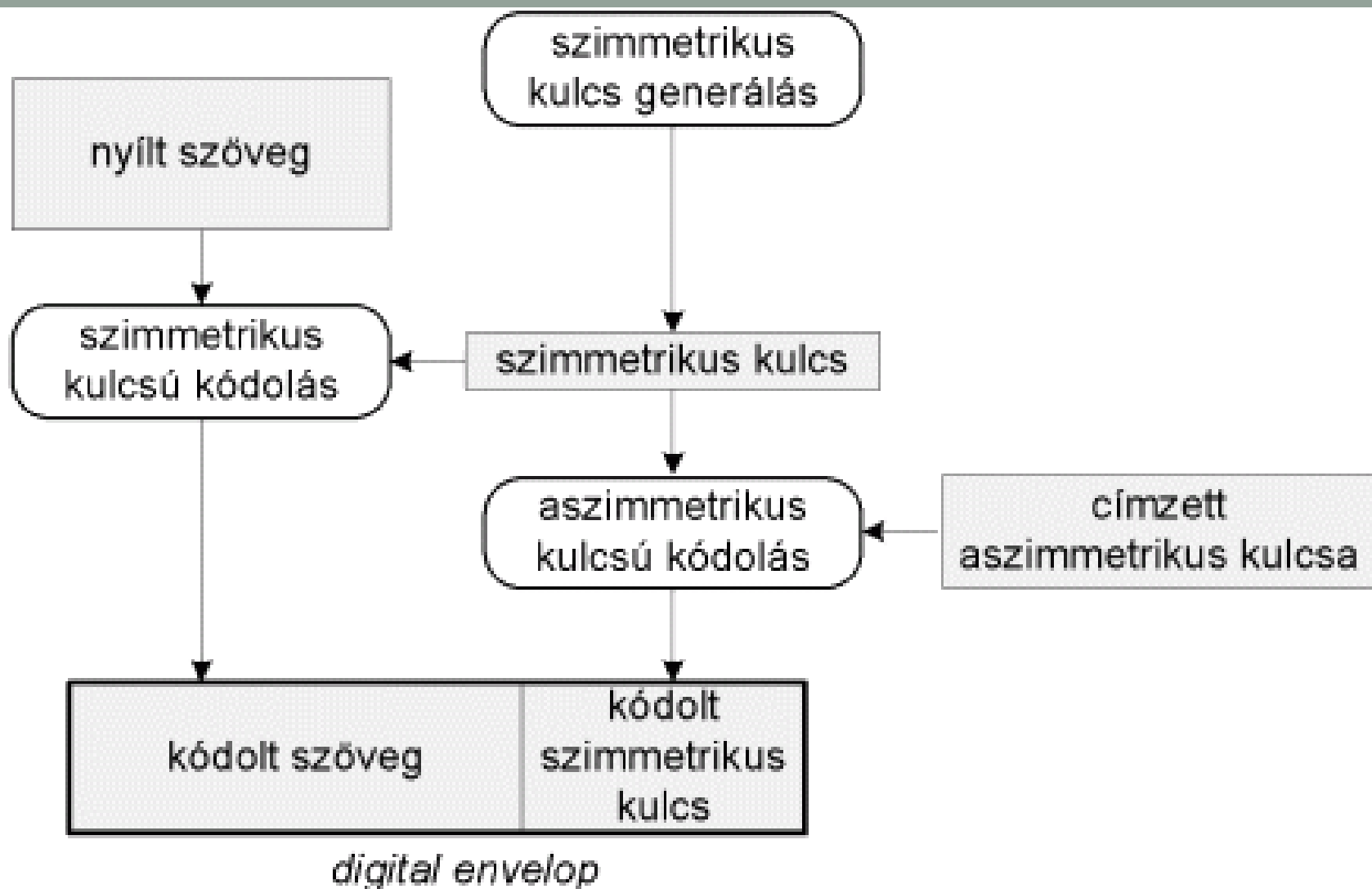
A szimmetrikus kulcsú kódolókat erősebbé tehetjük, ha egymást követő üzenetegységek kódolása során visszacsatolást is alkalmazunk, ezzel elérve azt, hogy ugyanannak az üzenet-részletnek más és más kódoltja lesz.

Felhasználási módok: ECB, CBC, CFB, OFB, CTR.

PROTOKOLOK

- **Enveloping**

- A szimmetrikus és aszimmetrikus kulcsú kriptográfia ötvözése.
- Az üzenetet frissen generált, véletlen szimmetrikus kulccsal kódolják.
- Mindkét részt (a kódolt üzenetet és a kódolt kulcsot) eljuttatják a címzettnek.



PROTOKOLOK

- **Üzenet hitelesítés**

Az üzenetek hitelessége igazolható az üzenet azonosító kóddal (Message Authentication Code, MAC)

- Lenyomatkészítő függvény
- Szimmetrikus kulcsú kódolás
- És a kettő ötvözete

KULCSMENEDZSMENT

- Szimmetrikus kulcsú kódolás alkalmazásakor elsőként is biztosítanunk kell, hogy a használni kívánt **közös kulcs minden félnél rendelkezésre álljon**.
- Kiosztásnál ügyelni kell a **kulcs titkosságára** és hitelességére.
- A kulcskiosztás (kulcs-csere) történhet személyes találkozás alkalmával, de erre a célra léteznek kriptográfiai **kulcsmenedzsment protokollok** is.

KULCS-CSERE (SZIMMETRIKUS KULCSÚ KÓDOLÁSSAL)

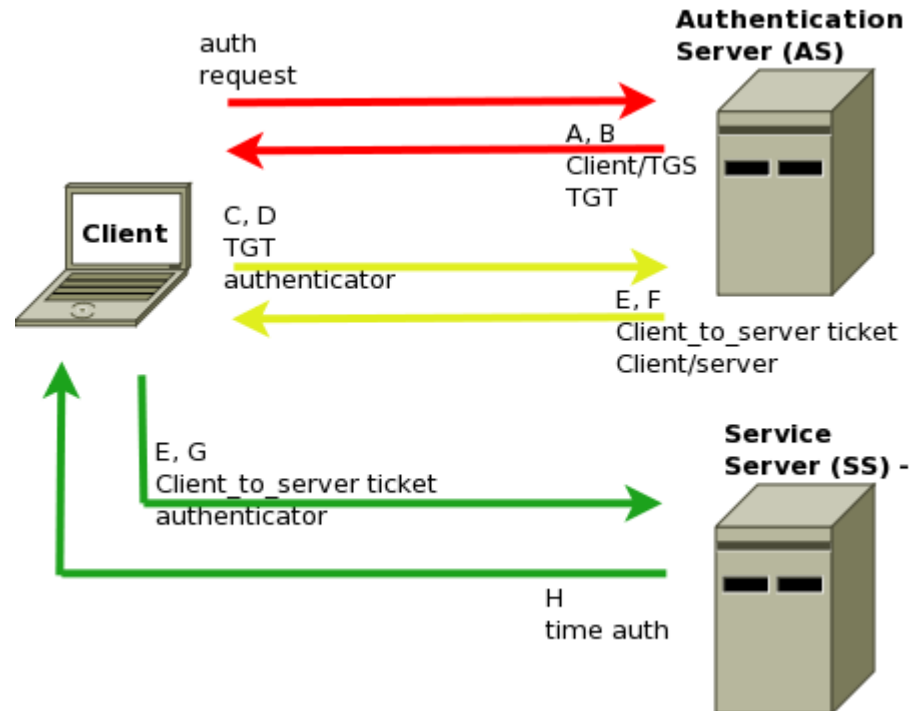
- A rendszerben kell lennie egy mindenki által megbízhatónak elfogadott szervernek (kulcselosztó központ), amellyel való kommunikációhoz **minden félnek létezik** már előre kiosztott, hosszú ideig használatos szimmetrikus kulcsa.
- A felek a **szerver közvetítésével** tudják kicserélni a kettőjük kommunikációjához szükséges aktuális kapcsolási kulcsot.

KERBEROS



1. A **kliens** azonosítja magát a **Hitelesítési Szervernek** és kap egy **jegyet**. Minden jegy időbélyeges.
2. Majd felveszi a kapcsolatot a **Jegy Kiadó Szerverrel**, és a kapott jegyet felhasználva azonosítja magát, majd egy szolgáltatást kér.
3. Ha az ügyfél **jogosult** a szolgáltatásra, akkor küld egy másik jegyet.
4. Ha ez megvan, az ügyfél kapcsolatba léphet a Szolgáltatás Szerverrel, és a **második jeggyel** bizonyítja, hogy jóváhagyták a szolgáltatás elérését.

- AS = Hitelesítési Szerver
- SS = szolgáltatás Szerver
- TGS = Jegy Kiadó Szerver
- TGT = Jegy Kiadó Jegy



Egyetlen **meghibásodási pont**: Ez megköveteli a központi szerver részéről a folyamatos rendelkezésre állást. Ha a Kerberos szerver leáll, senki nem tud bejelentkezni.

DES (Data Encryption Standard)

- Az USA-ban 1976-ban szabványosították.
- Egy német emigráns, Horst Feistel „Lucifer” nevű módszerén alapul. Az NSA nyomásának ellenére végül az IBM egyik kutatóközpontjában sikerült kidolgoznia az algoritmust a '70-es évek elejére.
- Több verziója látott napvilágot (DESX, 3DES vagy TripleDES). Az alkalmazott kulcshossz a verziónak megfelelően többféle lehet: 8, 56, 64, 128, 168 bit, stb.
- **Nagy adatfolyamok gyors kódolására és dekódolására** kiválóan alkalmas.

DES (Data Encryption Standard)

Működése:

1. Az üzenet átalakítása **bináris** számsorra.
2. A számsor tördelése **64 számjegyű** szakaszokra.
3. Minden szakaszon egyenként végrehajtja az alábbiakat:
 - a 64 számjegy **megkeverése** és két **félszakaszra** bontása (Bal_0 és Jobb_0);
 - a Jobb_0 számjegyeinek „**kiforgatása**” (behelyettesítési rendszer szerinti megcserélése);
 - $\text{Jobb_1} = \text{Jobb_0} + \text{Bal_0}$; $\text{Bal_1} = \text{eredeti Jobb_0}$
4. Az eljárást az aktuális félszakaszokra **16-szor** kell elvégezni.

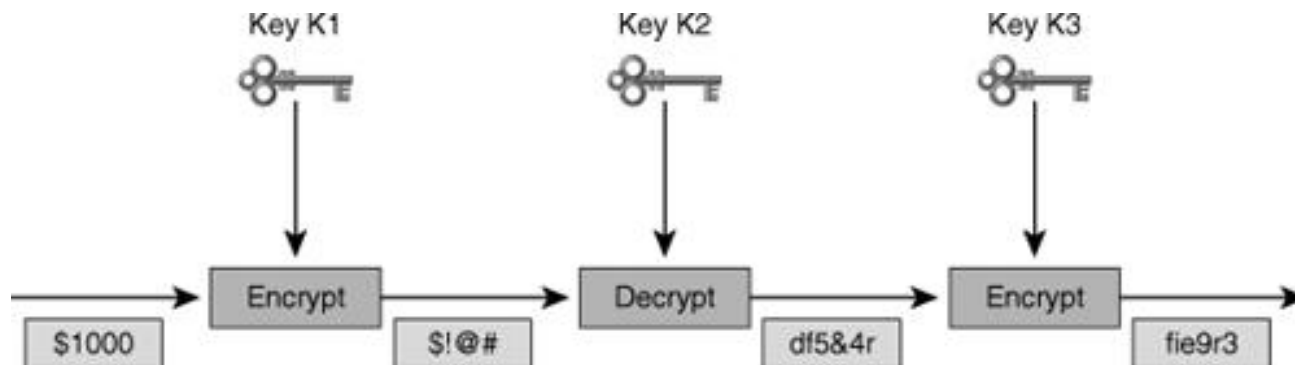
DES (Data Encryption Standard)

Mind a kódolás, mind a dekódolás gyors, évtizedekig használták eredményesen.

Mára azonban a számítógépek teljesítményének növekedése miatt elavultnak számít (brute-force módszerrel reális időn belül törhető).

3DES

- A DES egymás után háromszori alkalmazása, de elég 112 bites kulcs is
- Nem elég gyors az új kódolókhöz képest



- EDE (Encrypt-Decrypt-Encrypt) Method – 3DES-EDE Method:
 - Data is encrypted using K1.
 - Data is decrypted using K2.
 - Data is encrypted using K3.
- If $K1 = K3$, Key Yields 112-Bit Key Length
- If $K1 \neq K3$, Key Yields 168-Bit Key Length

RC2, RC4

Az 56 bites DES-nél nagyobb biztonságot nyújt. Az RC4 az RC2 továbbfejlesztett változata.

Mindkét eljárás **többféle bithosszúságú kulccsal** dolgozik. Az alap Windows NT-be a 40 bites változat került bele, de a Service Pack 6-ban megjelent az 56 bites is.

Az USA-ba szánt NT-ben Service Pack 3-tól 128 bites (RC4) lett a kulcs hossza. RC4 algoritmust használ a Windows a távelérésű kliens és kiszolgáló közötti kommunikáció során, de találkozunk vele Windows 2000 Server terminálszolgáltatásában is a titkosított adatforgalom beállításánál.

IDEA

(International DataEncryption Algorithm - nemzetközi adat titkosító eljárás)

- **64 bites** blokkmérettel, 128 bites kulccsal dolgozó blokkos rejtjelző algoritmus.
- Svájcban fejlesztették ki a '90-es évek elején.
- Kifejezetten **adatátvitelhez** tervezték, beleértve a digitalizált hang/kép valós idejű kódolását is.
- Szabadalmi bejegyzése van, és így (üzleti) felhasználásához **licenszdíjat** kell fizetni.
- Egy ideig a DES ellenfelének tűnt, de ma már kissé háttérbe szorult.

IDEA

- A 64 bites input blokkokat **további 4 16 bites** szegmensre osztja és ezekkel **8 menetben** végzi el a titkosítást.
- Az utolsó menetben kapott 4 titkosított szövegdarab **összefűzése** a **végleges titkosított** szöveg.
- A 128 bites kulcs kellő biztonságot ad, az algoritmus egyetlen ismert hibája a gyenge kulcsok használata lehet.

AES

- 1997. január 2-án a NIST (A szabványok és technológiák nemzeti hivatala) **pályázatot hirdetett** egy a DES-t felváltó új blokkrejtjelezést használó titkosító eljárás kifejlesztésére. A pályázatra rengeteg munka érkezett. Végül a döntőbe már csak öt munka kapott helyet:
 - **MARS** – IBM,
 - **RC6** – RSA
 - **Rijndael** – Joan Daemen és Vincent Rijmen
 - **Serpent** – Ross Anderson, Eli Biham, Lars Knudsen
 - **Twofish** – Bruce Schneier, John Kelsey, Niels Ferguson, Doug Whiting, David Wagner, Chris Hall

AES

- Végül a 2000 őszén a NIST a **Rijndael algoritmus 128 bites változatát** nyilvánította győztesnek és ez lett az új szimmetrikus kulcsú rejtjelező szabványnak az AES-nek (*Advanced Encryption Standard*) az alapja az Egyesült Államokban.
- A választást a jó hatásfok mellett azzal indokolták, hogy ez az algoritmus **korlátozott erőforrással rendelkező** eszközökön is megfelelő teljesítményt biztosít.
- Az AES-ben megvalósított Rijndael algoritmus egy blokkrejtjelezési eljárás amelyik bemenetként **128 bites blokkokat** használ. De maga a Rijndael konfigurálható 192 illetve 256 bites blokkok használatára is. A használt titkosítási kulcs hossza ennek megfelelően **128, 192** vagy **256** bit.

BLOWFISH

- A **DES**-hez és az **IDEA**-hoz hasonlóan a Blowfish egy **változó kulcshosszúságú** szimmetrikus blokk-titkosítás.
- **Bruce Schneier** fejlesztette ki 1993-ban. Célja egy nagy teljesítményű, szabadon hozzáférhető alternatíva biztosítása volt a létező titkosítási algoritmusok mellett.
- Az algoritmust nyilvánosságra hozatala óta sokan elemezték, és lassan a szakmai közönség is kezdi **erős titkosító** algoritmusnak tekinteni. A **kulcsméret 32-448 bit** lehet, a **blokkok mérete 64 bit**.
- A Blowfish algoritmus egy egyszerű titkosító függvény **16 iterációját** hajtja végre.

Titkosítás, hitelesítés 3



ASZIMETRIKUS KULCSÚ TITKOSÍTÁS

Az **aszimmetrikus kulcsú** (más néven nyilvános kulcsú) kriptográfiánál a kódolás és a dekódolás nem ugyanazzal a kulccsal történik.

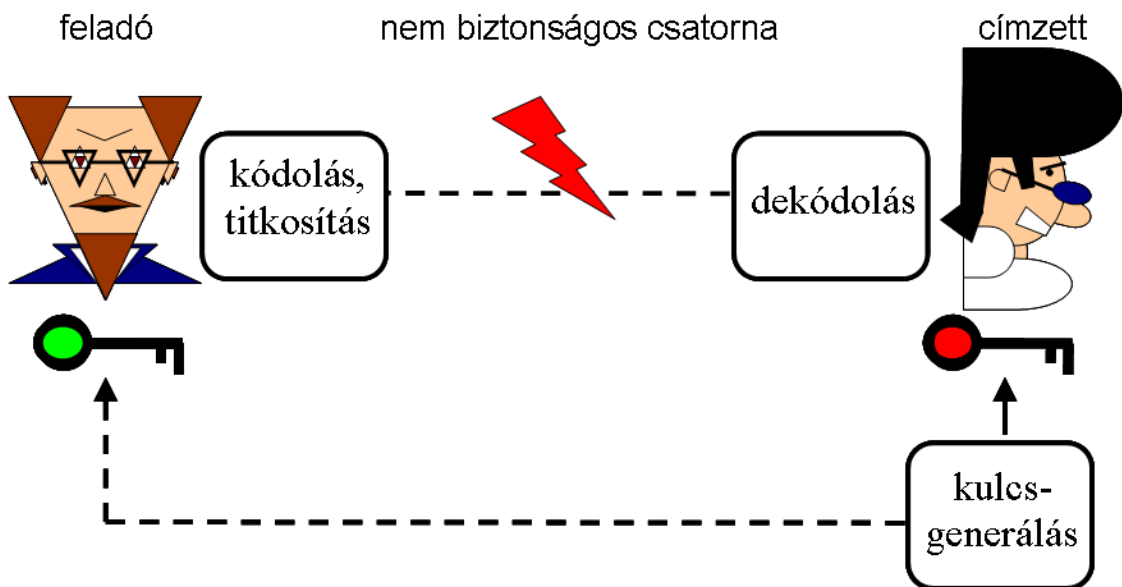
Minden félnek van egy **nyilvános kulcsa** és egy **magánkulcsa**.

A magánkulcs soha nem kerül ki birtokosa tulajdonából, de bárki hozzáférhet mások nyilvános kulcsához.

A nyilvános kulcsot nem kell titokban tartani, azt bárki megismerheti.

Ha titkosított üzenetet szeretnénk küldeni valakinek, **meg kell szereznünk az ő nyilvános kulcsát**, és azzal kell kódolnunk a neki szóló üzeneteket. Az így kódolt üzeneteket a címzett a saját magánkulcsával fejtheti vissza.

A kulcsok matematikailag összefüggnek, ám a titkos kulcsot gyakorlatilag nem lehet meghatározni a nyilvános kulcs ismeretében. Egy, a nyilvános kulccsal kódolt üzenetet **csak a kulcspár másik darabjával**, a titkos kulccsal lehet visszafejteni.



Nyilvános kulcsú (más néven aszimmetrikus kulcsú) kriptográfia esetén a kódolás és a dekódolás különböző kulcsokkal történik. Ekkor **elegendő az egyik kulcsot titokban tartanunk**, a másik kulcsot akár nyilvános csatornán is továbbíthatjuk.

Módszer:

1. Minden szereplő elkészít magának egy **T** és egy **M** kulcspárt, melyek **egymás inverzei**.
2. A **T** kulcsot **nyilvánosságra** hozza, az **M** kulcsot viszont **titokban** tartja.
3. Legyen **A** kulcspárja **T_A M_A**,
B kulcspárja pedig **T_B M_B**.
4. Ekkor **A** az **u** üzenet helyett a **v=T_B (M_A (u))** értéket küldi el **B**-nek, aki ezt a következőképpen fejtí meg: **u=T_A (M_B (v))**.

Hitelesség és letagadhatatlanság

A titkos kulccsal kódolt információt bárki olvashatja a nyilvános kulcs segítségével, és biztos lehet abban, hogy a titkos kulcs birtokosa volt a feladó.

Hitelesség: az üzenetet a feladó készítette.

Letagadhatatlanság: a titkos kulcs titokban volt, a hozzá tartozó nyilvános kulccsal dekódolható üzenetet nem készíthette senki más, csak a tulajdonosa.

Digitális aláírás

- A nyilvános kulcsú titkosítás legfontosabb felhasználási területe.
- Ha a saját magánkulcsunkkal kódolunk egy dokumentumot, az így kapott adatról – a nyilvános kulcsunk alapján – bárki megállapíthatja, hogy azt mi hoztuk létre. E műveletet **aláírásnak** nevezzük.
- Az aláírandó dokumentumból először egy lenyomatkészítő függvénnyel lenyomatot képeznek, majd ezen az aláíró fél titkos kulcsával végeznek műveletet, ennek az eredménye a **digitális aláírás**.

Digitális aláírás

- Az ellenőrző fél szintén elkészíti a dokumentum lenyomatát (ismert az algoritmus), valamint a kapott digitális aláírást visszafejti a küldő fél nyilvános kulcsával - ekkor szintén a dokumentum lenyomatát kellene eredményül kapni. Ha a dekódolt lenyomat megegyezik a kapott dokumentumból számítottal, akkor azt bizonyítja, hogy:
 - Az üzenet és az aláírás **integritását**
 - A **hitelességet** és a **letagadhatatlanságot**.

Az elektronikus dokumentumok fajtái

- **Elektronikus dokumentum:** bármilyen elektronikus formában létező adat, amit aláírással láttak el.
- **Elektronikus irat:** olyan elektronikus dokumentumok, amelyek szöveget tartalmaznak
- **Elektronikus okirat:** amely nyilatkozattételt, illetőleg nyilatkozat elfogadását, vagy nyilatkozat kötelezőnek való elismerését tartalmazza, azaz szerződésnek vagy jogi nyilatkozatnak tekinthető.

Az elektronikus aláírás fajtái

- **Elektronikus aláírás:** elektronikus dokumentumhoz az aláíró azonosítása céljából csatolt vagy azzal logikailag összekapcsolt elektronikus dokumentum.
- **Fokozott biztonsági elektronikus aláírás:** módosíthatatlan legyen és egyértelműen azonosítsa a az aláíró, de az alkalmazott konkrét technológiával kapcsolatban kikötést nem tartalmaz.
- **Minősített elektronikus aláírás:** biztonságos aláírás készítő eszközzel és minősített tanúsítványhoz rendelhető aláírás létrehozó adattal hozták létre.

Törvény

Ahogy a papír alapú aláírás bíróság előtt felhasználható bizonyíték, az elektronikus aláírás is az. Az **elektronikus aláírásról szóló 2001. évi XXXV. törvény** szerint a legalább **fokozott biztonságú elektronikus aláírással** ellátott dokumentum **megfelel az írásba foglalás követelményeinek**, a **minősített aláírással** ellátott dokumentum pedig – a polgári perrendtartásról szóló törvény értelmében – **teljes bizonyító erejű magánokirat** (akárcsak a két tanú előtt, vagy a közjegyző előtt aláírt dokumentum).

RSA titkosítás

- 1978 (Ronald Rivest, Adi Shamir, Leonard Adleman)
- PKCS (Public Key Cryptography Standards)
- Nyilvános kulcsú algoritmus
- Alkalmas titkosításra és digitális aláírásra is
- A kulcsméret tetszőleges

RSA kulcsgenerálás

1. Válasszuk ki P és Q prímszámokat!
2. $N=P*Q$ és $M(N)=(P-1)*(Q-1)$
3. Válasszunk egy véletlen E számot úgy, hogy relatív prím legyen $M(N)$ -re. (Különben nem lesz invertálható $M(N)$ -re és D sem lesz kiszámolható.)
4. Számoljuk ki E multiplikatív modulo inverzét $\phi(N)$ -re nézve, ez lesz D . (keressünk egy olyan D -t, amelyre **$ED = 1 \bmod \phi(N)$** teljesül vagyis az **ED szorzat $\phi(N)$ -nel osztva 1-et ad maradékul.**

Például 43 multiplikatív inverze 1590-re nézve 37, mert $43 \times 37 = 1591$, ami 1590-nel osztva 1-et ad maradékul.

Ezt így írjuk: $43 \times 37 = 1 \pmod{1590}$.

Általános jelöléssel: $a \times a^{-1} = 1 \bmod m$, ahol a^{-1} az a -nak m -re vonatkozó inverze.

RSA példa

1. Legyen **P=17** és **Q=23**!
2. **N=P*Q=391** és $M(N)=(P-1)*(Q-1)=352$
3. Legyen **E=21**, a $(21,352)=1$ teljesül.
4. Az E=21 multiplikatív inverze $\phi(N)$ -re: **D=285**, mert $285 \times 21 \bmod 352 = 1$.
5. Első lépésként átalakítjuk az üzenetet számokká. Ehhez használhatjuk az ASCII táblát, a számként felírt üzenet számjegyeinek csoportosítását.
6. Egy a fontos: minden üzenetdarabnak kisebbnek kell lennie, mint 391. Ha $p=239$ és $q=277$, választásunk eredményeképpen $N=66203$ lenne, akkor a betűket kettesével is csoportosíthatnánk.

RSA példa

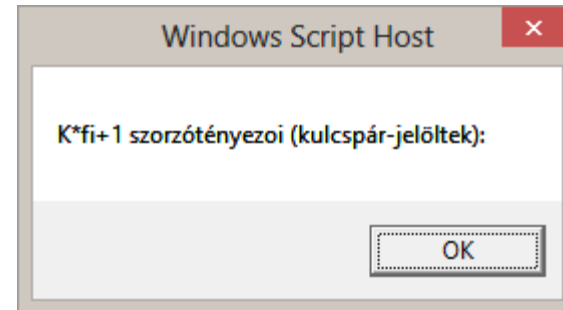
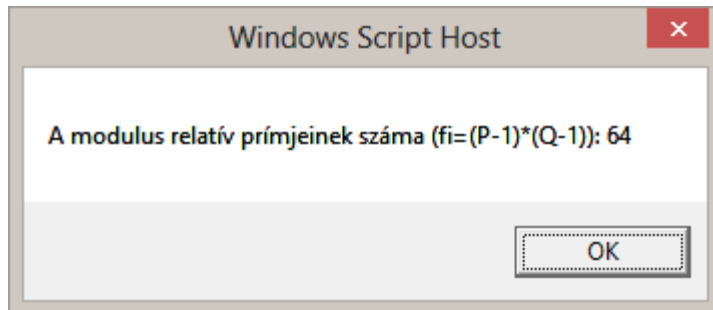
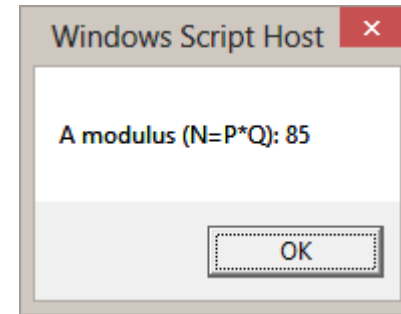
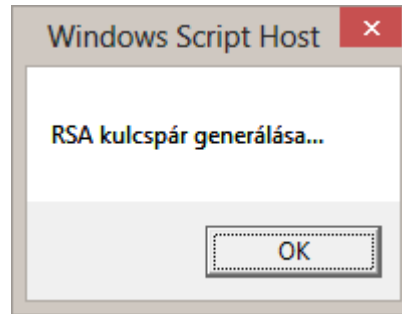
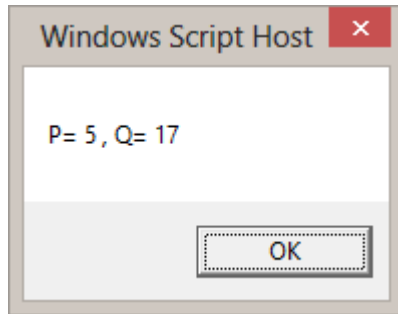
Az átkódolás és a hatványozások eredményét az alábbi táblázat mutatja:

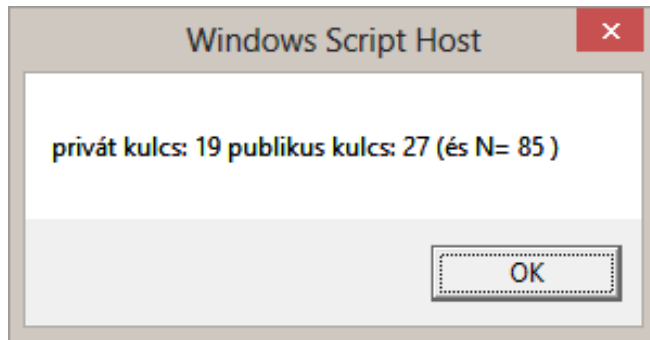
- A „T” ASCII kódja: **84**.
- Az ő titkosított párja: $84^{21} \bmod 391 = 135$, ezt kell elküldeni.
- A fogadó oldalon pedig a $135^{285} \bmod 391 = 84$ számítást kell elvégezni.

	m_i	M_i		M_i	m_i	
T	84	135	→	135	84	T
I	73	167		167	73	I
T	84	135		135	84	T
O	79	214		214	79	O
K	75	96		96	75	K
$M_i = m_i^{21} \bmod 391$				$m_i = M_i^{285} \bmod 391$		

RSA kulcsgenerátor

Fóti Marcell (Net Academia)



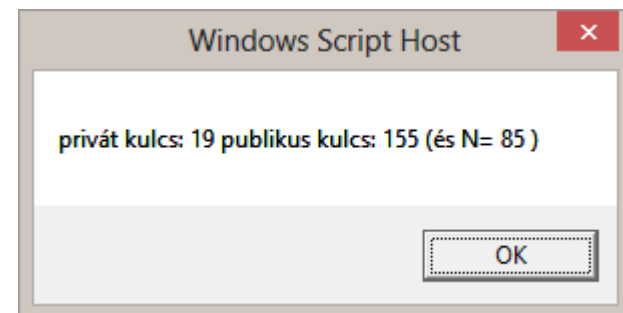
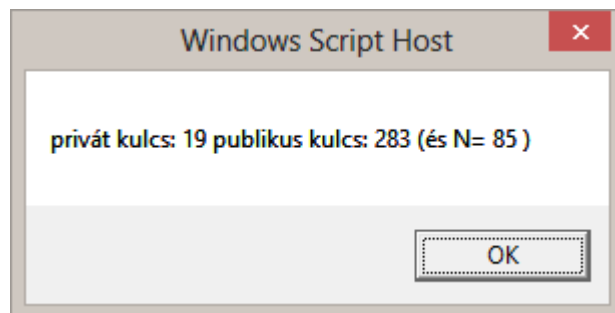
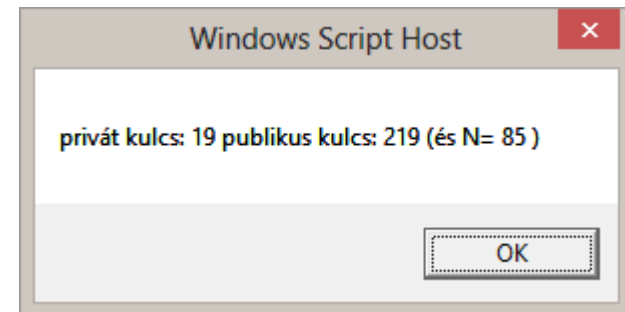
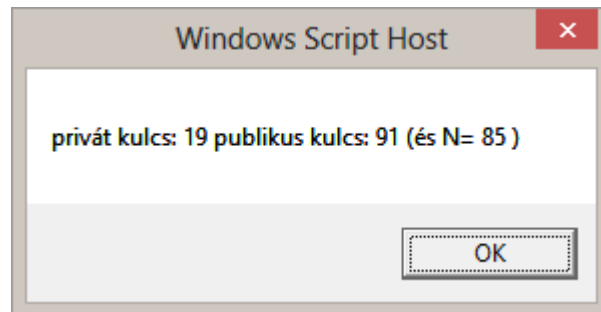


T – titkosítandó adat = „7”
N – modulus = $P \cdot Q = 5 \cdot 17 = 85$
C – titkosított üzenet

$$T^{\text{publikus kulcs}} \bmod N = C \quad \Rightarrow \quad 7^{27} \bmod 85 = \mathbf{48}$$

$\mathbf{=C}$

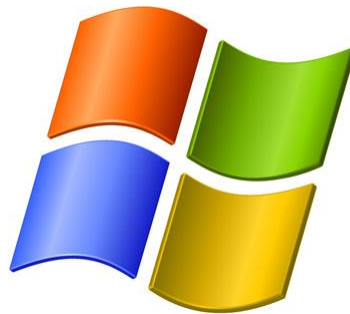
$$C^{\text{privát kulcs}} \bmod N = T \quad \Rightarrow \quad 48^{19} \bmod 85 = \mathbf{7 = T}$$



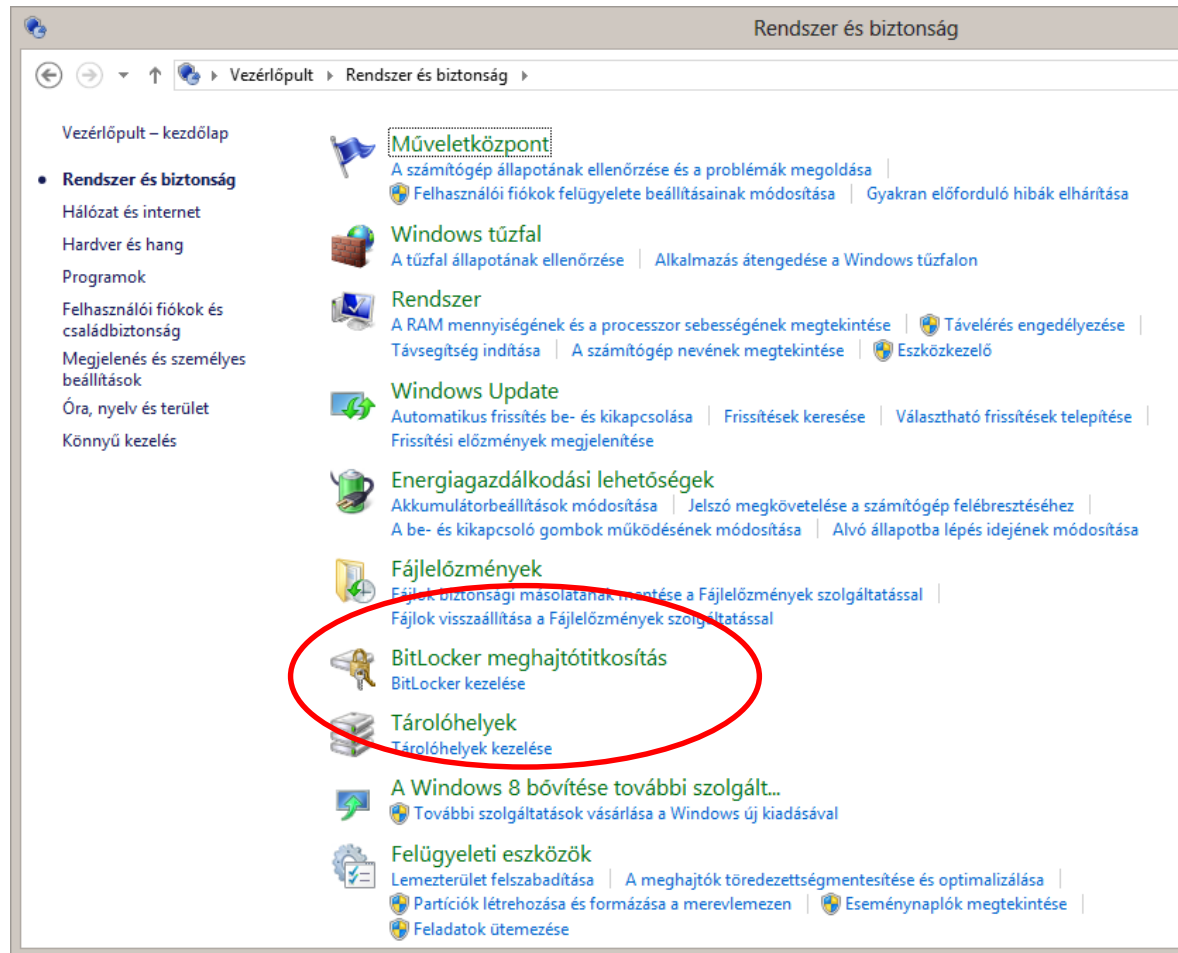
Titkosítási módszerek

BITLOCKER

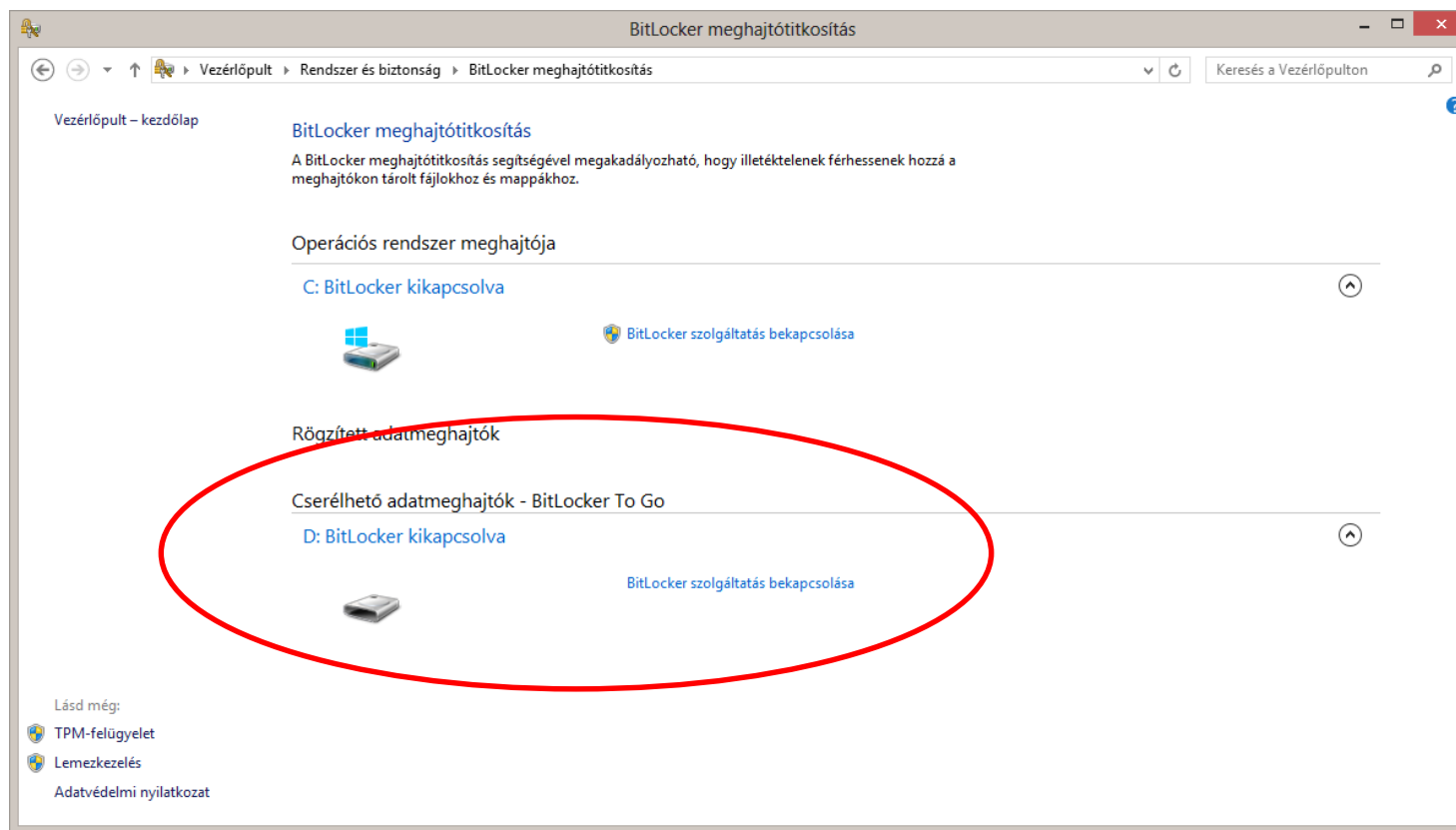
meghajtó titkosítás



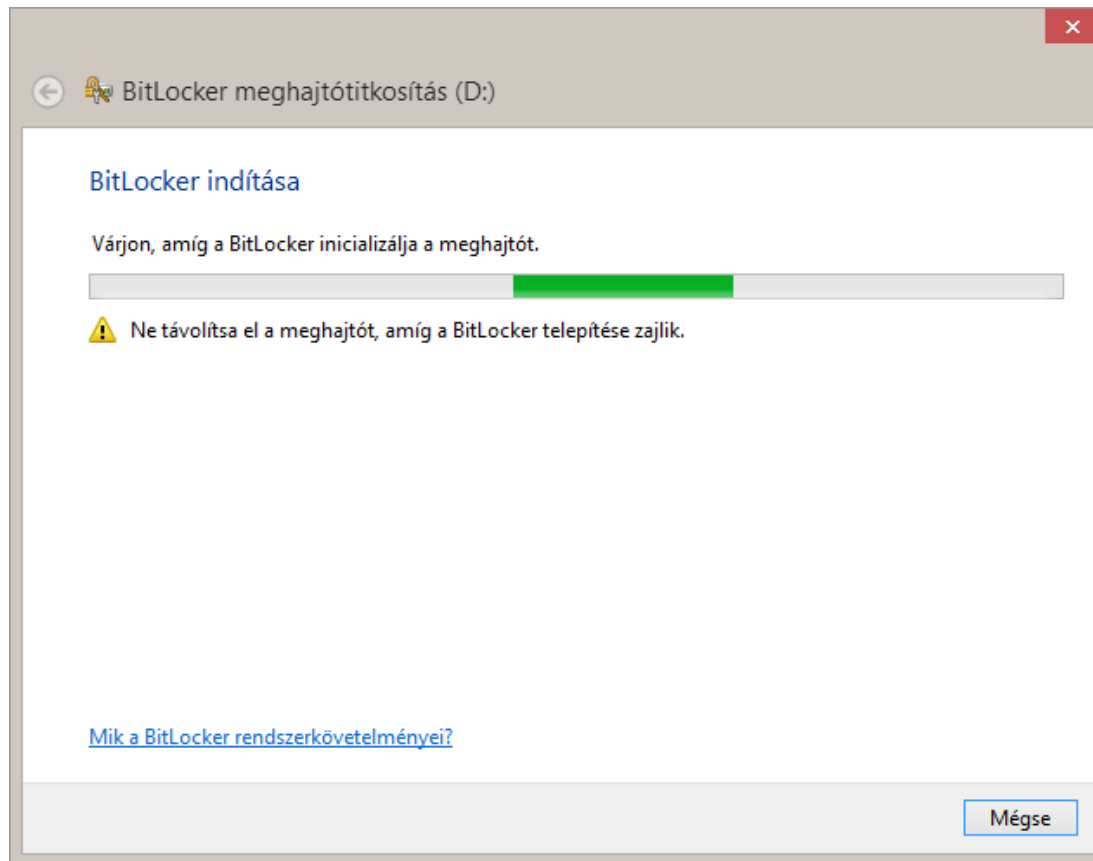
Vezérlőpult beállítás



Az operációs rendszer vagy egy cserélhető meghajtó titkosítása



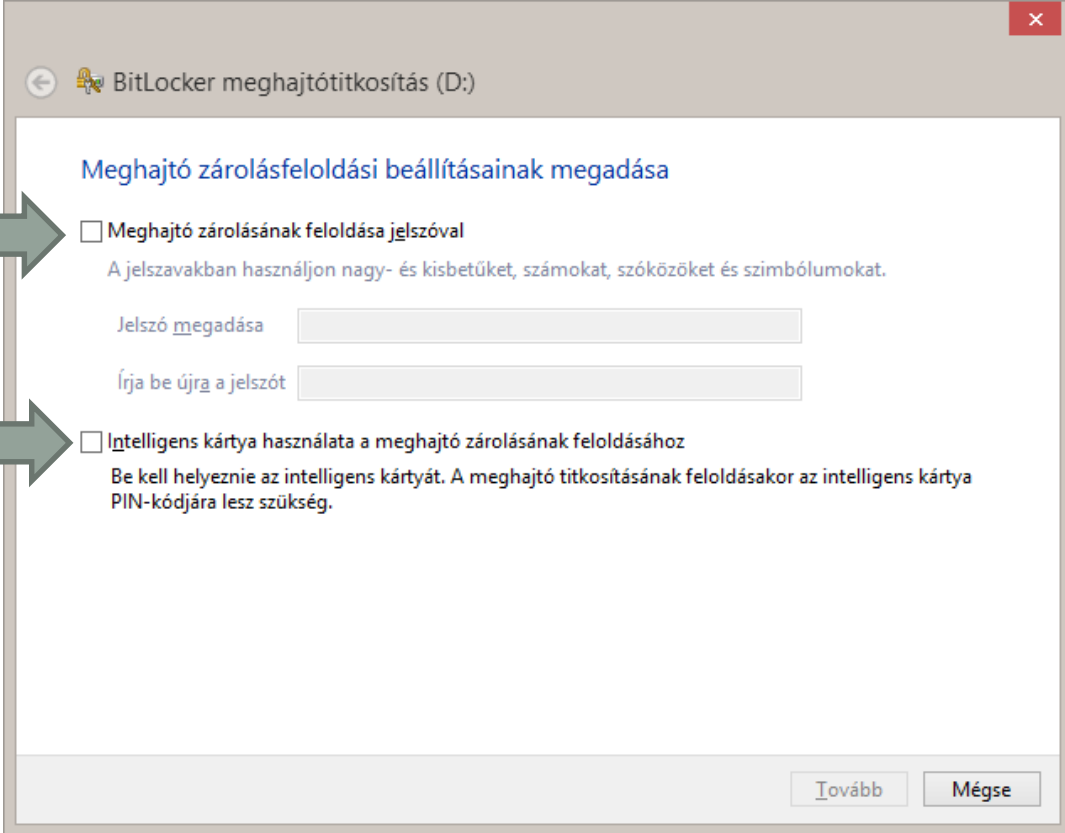
A titkosítandó meghajtó inicializálása



A titkosítás feloldása történhet

jelszóval
vagy

Intelligens kártyával



The screenshot shows a Windows BitLocker recovery window titled "BitLocker meghajtótitkosítás (D:)" with a back arrow and a lock icon. The main heading is "Meghajtó zárolásfeloldási beállításainak megadása". There are two options, each with an unchecked checkbox and a description. The first option is "Meghajtó zárolásának feloldása jelszóval" with the instruction "A jelszavakban használjon nagy- és kisbetűket, számokat, szóközöket és szimbólumokat." Below it are two input fields: "Jelszó megadása" and "Írja be újra a jelszót". The second option is "Intelligens kártya használata a meghajtó zárolásának feloldásához" with the instruction "Be kell helyeznie az intelligens kártyát. A meghajtó titkosításának feloldásakor az intelligens kártya PIN-kódjára lesz szükség." At the bottom right are two buttons: "Tovább" and "Mégse".

BitLocker meghajtótitkosítás (D:)

Meghajtó zárolásfeloldási beállításainak megadása

☐ Meghajtó zárolásának feloldása jelszóval
A jelszavakban használjon nagy- és kisbetűket, számokat, szóközöket és szimbólumokat.

Jelszó megadása

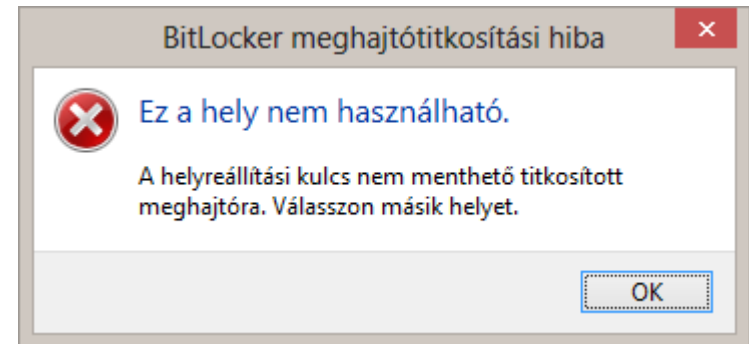
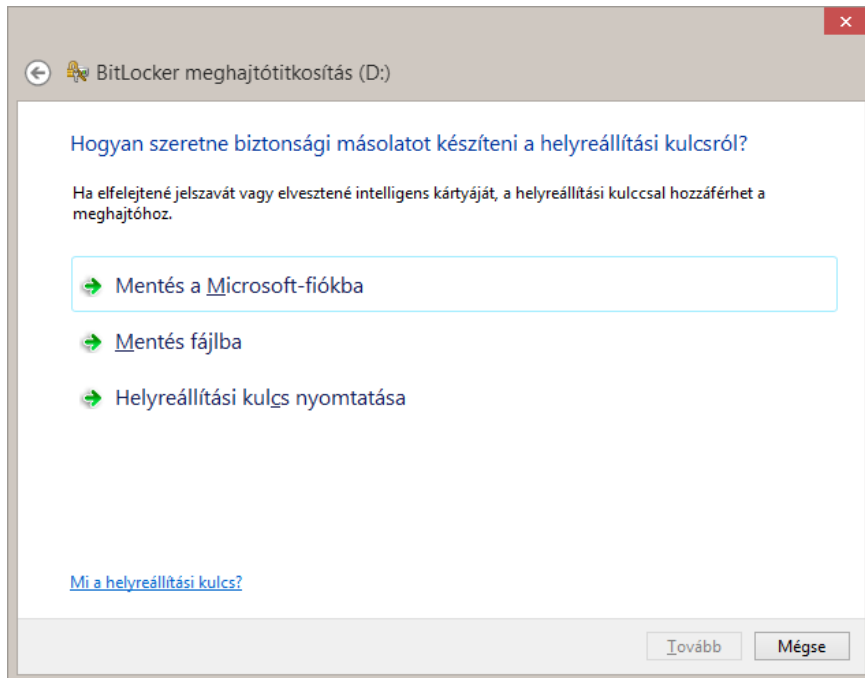
Írja be újra a jelszót

☐ Intelligens kártya használata a meghajtó zárolásának feloldásához
Be kell helyeznie az intelligens kártyát. A meghajtó titkosításának feloldásakor az intelligens kártya PIN-kódjára lesz szükség.

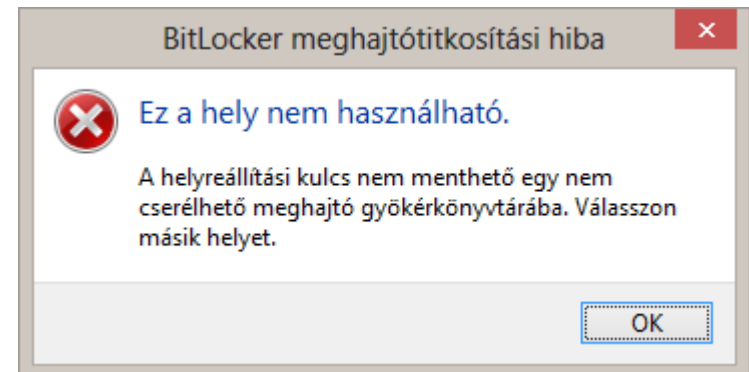
Tovább Mégse

Jelszó vagy Intelligens kártya elvesztése esetén **helyreállítási kulccsal** is megtörténhet a hozzáférés.

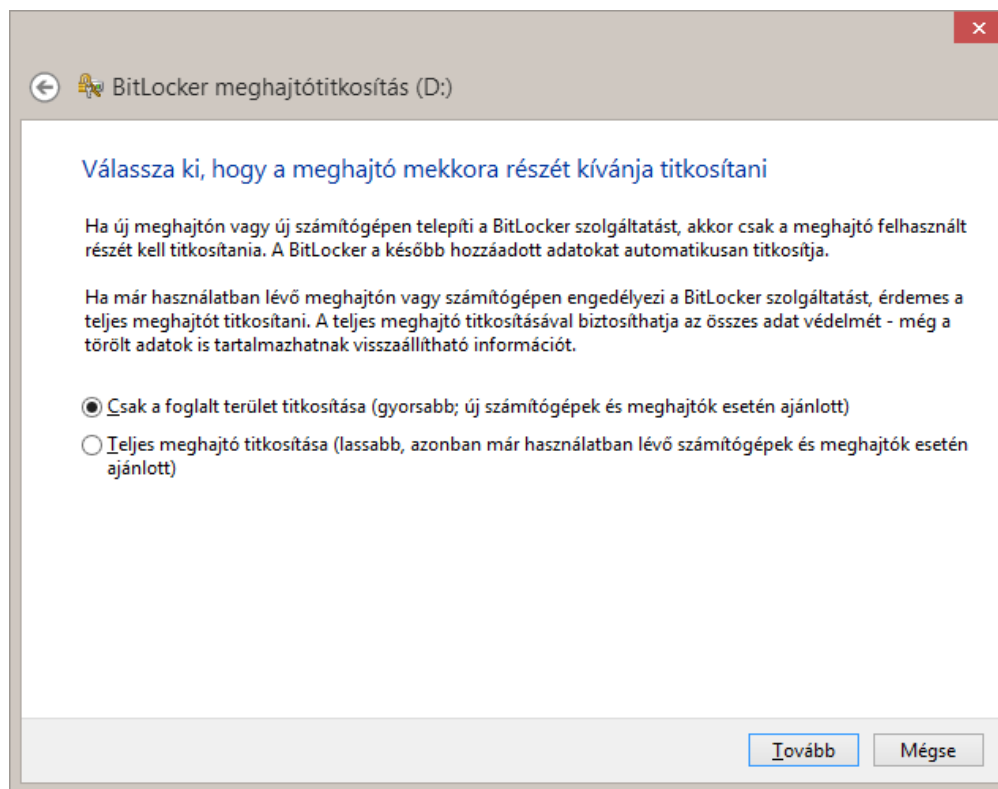
Nem menthető arra amit titkosítottunk:



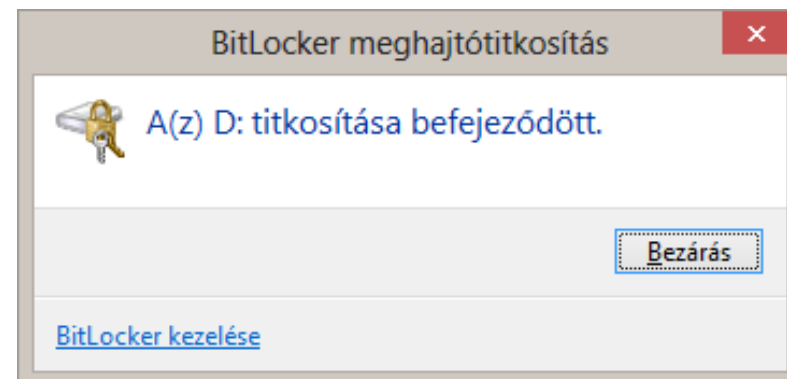
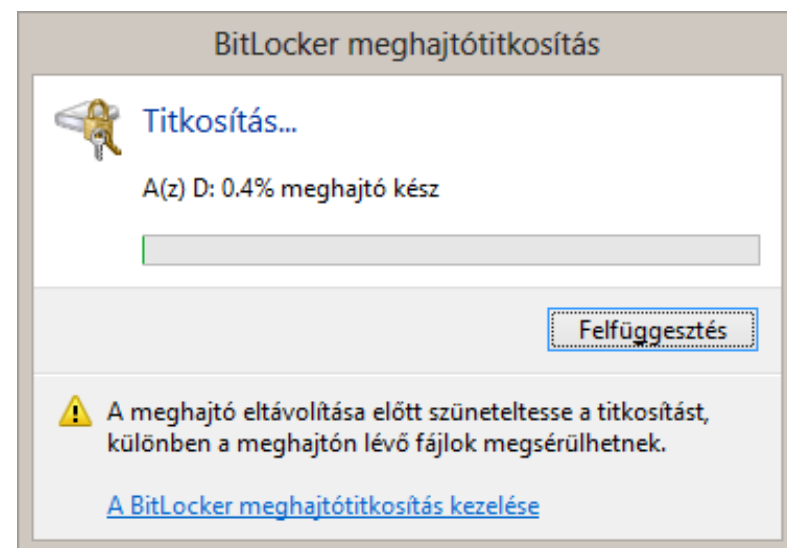
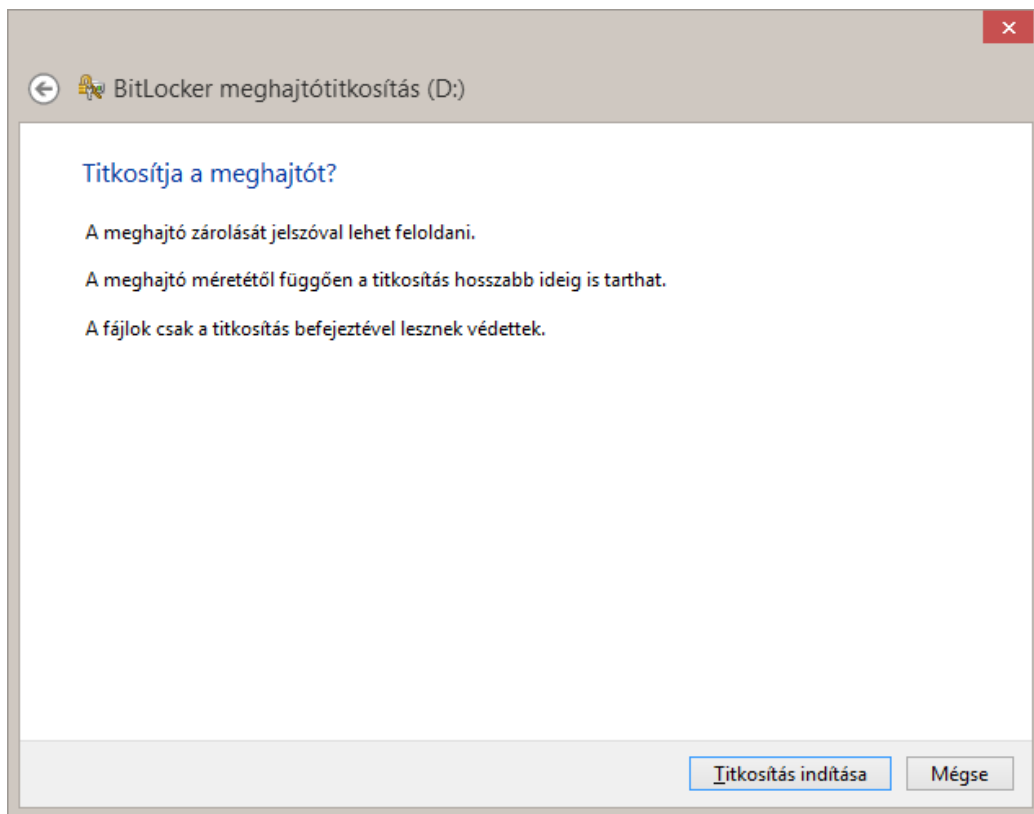
Gyökérkönyvtárba csak hordozható eszközre menthető:



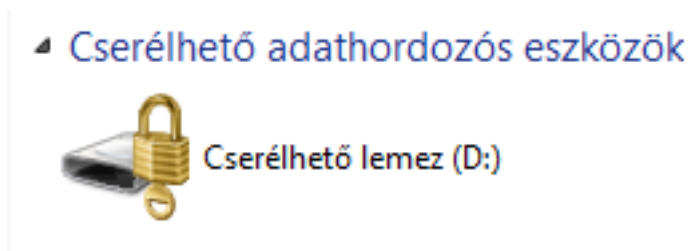
Titkosítható az **egész** meghajtó, vagy **csak a lefoglalt** terület.



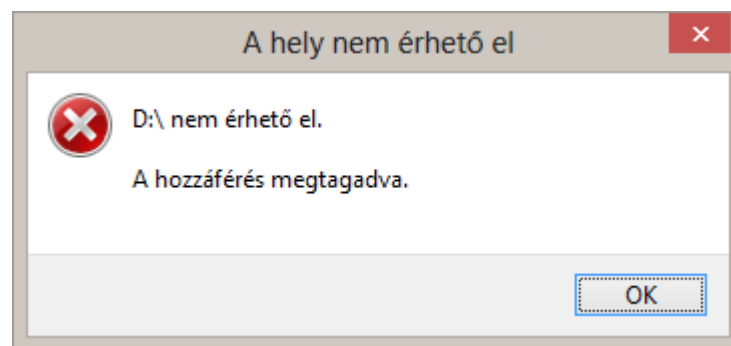
A titkosítás indítása



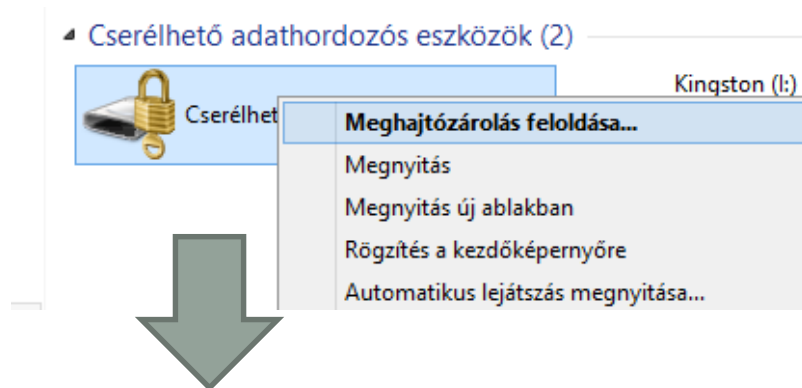
A meghajtók listájában megjelenő titkosított meghajtó jelölése:



Megnyitáskor **megtagadja** a hozzáférést:



A titkosított meghajtó **megnyitása**:



BitLocker (D:)

Adja meg a jelszót a meghajtó zárolásának feloldásához.

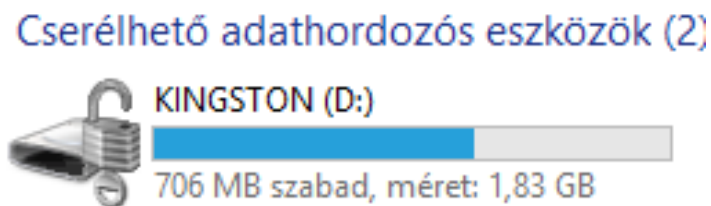
[További beállítások](#)

Zárolás feloldása

← BitLocker (D:)

A meghajtó zárolásának feloldásához írja be a 48 számjegyű kulcsot.
(Kulcsazonosító: BE7E28DF)

Zárolás feloldása



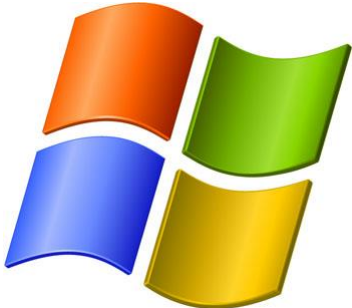
jelszóval

kulccsal



VeraCrypt

<https://veracrypt.hu/>



Előzmény - TrueCrypt

WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

This page exists only to help migrate existing data encrypted by TrueCrypt.

The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. Windows 8/7/Vista and later offer integrated support for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (click [here](#) for more information). You should migrate any data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

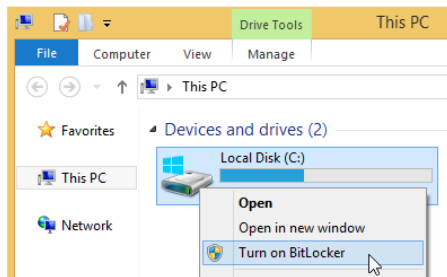
Migrating from TrueCrypt to BitLocker:

If you have the system drive encrypted by TrueCrypt:

1. Decrypt the system drive (open **System** menu in TrueCrypt and select **Permanently Decrypt System Drive**). If you want to encrypt the drive by BitLocker before decryption, [disable](#) Trusted Platform Module first and do not decrypt the drive now.
2. Encrypt the system drive by BitLocker. Open the Explorer:



3. Click the drive C: (or any other drive where system encryption is or was used) using the right mouse button and select **Turn on BitLocker**:



If you do not see the **Turn on BitLocker** menu item, click [here](#).

Alternatively, use search in the **Start** menu or screen:

VeraCrypt

A VeraCrypt egy nyílt forráskódú valós idejű titkosítást biztosító, **TrueCrypt-re** építő szoftver. Első letölthető verziója 2013. június 22-én került fel az internetre, azóta pedig számos újabb verziója jelent meg.

A program – egyezően a TrueCrypt-tel – egy valósidejű titkosító, vagyis a fájlok automatikusan, számunkra transzparens módon kerülnek titkosításra és feloldásra, amint azokat elmentjük, illetve betöltjük, ugyanis az alkalmazás magát a meghajtót szolgáltatja. Segítségével a teljes lemezünk lekódolható, de létrehozhatunk rejtett tárolókat is, amennyiben fontos a titkosított adat létezésének elrejtése is.

VeraCrypt

A VeraCrypt sok javítást eszközölt a TrueCrypt-hez képest, melyek között több fontos biztonsági probléma is orvoslásra került. A program 3 féle alap titkosítási algoritmust támogat (AES, Serpent, Twofish), ezen felül kombinálásukkal még további 5 válik elérhetővé (AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent). A hasheléshez használt algoritmusok között (RIPEMD-160, SHA-256, SHA-512, Whirlpool) megjelenik az SHA-256, mint újdonság a VeraCrypt repertoárjában. Továbbá növelték a hash algoritmusoknál használt iterációk számát, ami sebességben ugyan némi csökkenést eredményez, de cserébe bruteforce támadással legalább 10-szeresen (legfeljebb akár 300-szorosan is) több időbe telik a rendszer feltörése.

TrueCrypt

A titkosított adatállomány megnyitásához használhatunk **jelszót** vagy **kulcsfájlt**, illetve ezek kombinációját. A kulcsfájl egy olyan tetszőleges, a felhasználó által választott fájl, amit a titkosított kötet létrehozásakor illetve a későbbi megnyitás során a program használ.

Ez a fájl, mint egy kulcs, fog a későbbiekben működni.

Aki a fájlt birtokolja és a megnyitás során használja, az képes a védett adatokat megnyitni.

TrueCrypt

A TrueCrypt képes a **Windows operációs rendszert** tartalmazó partíció illetve meghajtó teljes titkosítására.

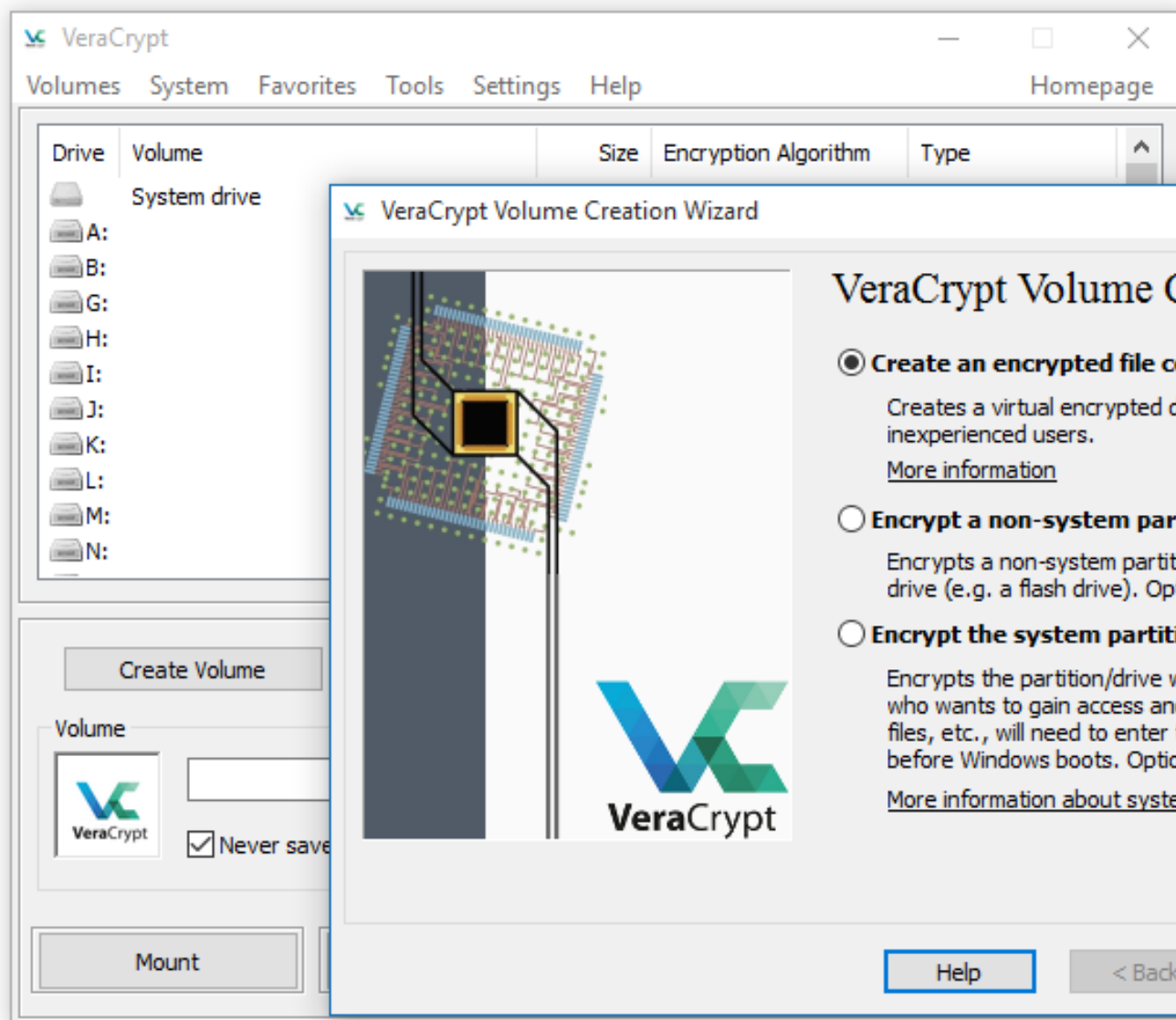
Ennek értelmében **rendszerindítás előtt** meg kell adni a szükséges jelszót, ahhoz hogy az betöltsön, illetve írni vagy olvasni lehessen a merevlemezre.

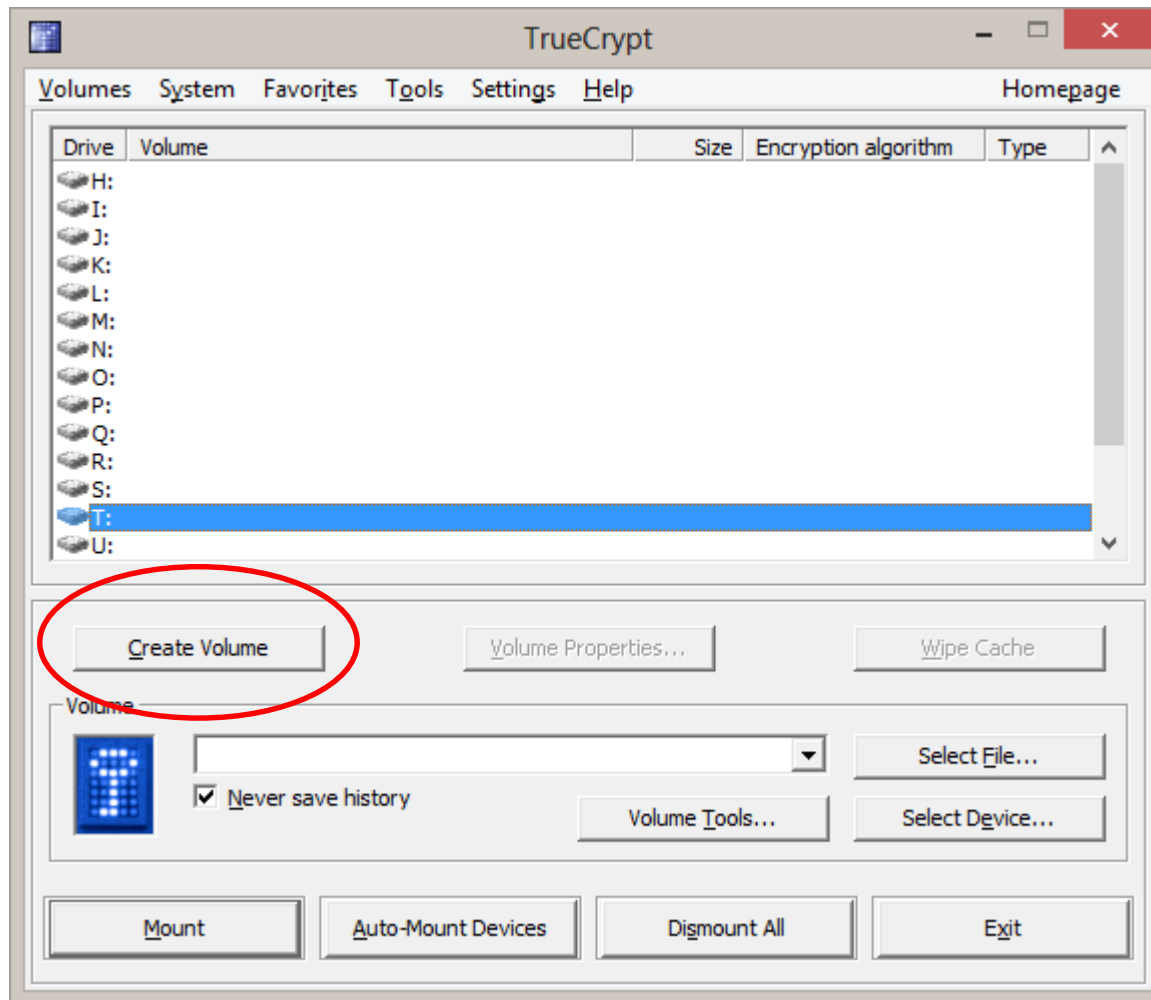
Ez a jogosultság ellenőrzés nem csak az operációs rendszert, hanem az egész tárterületet védi.

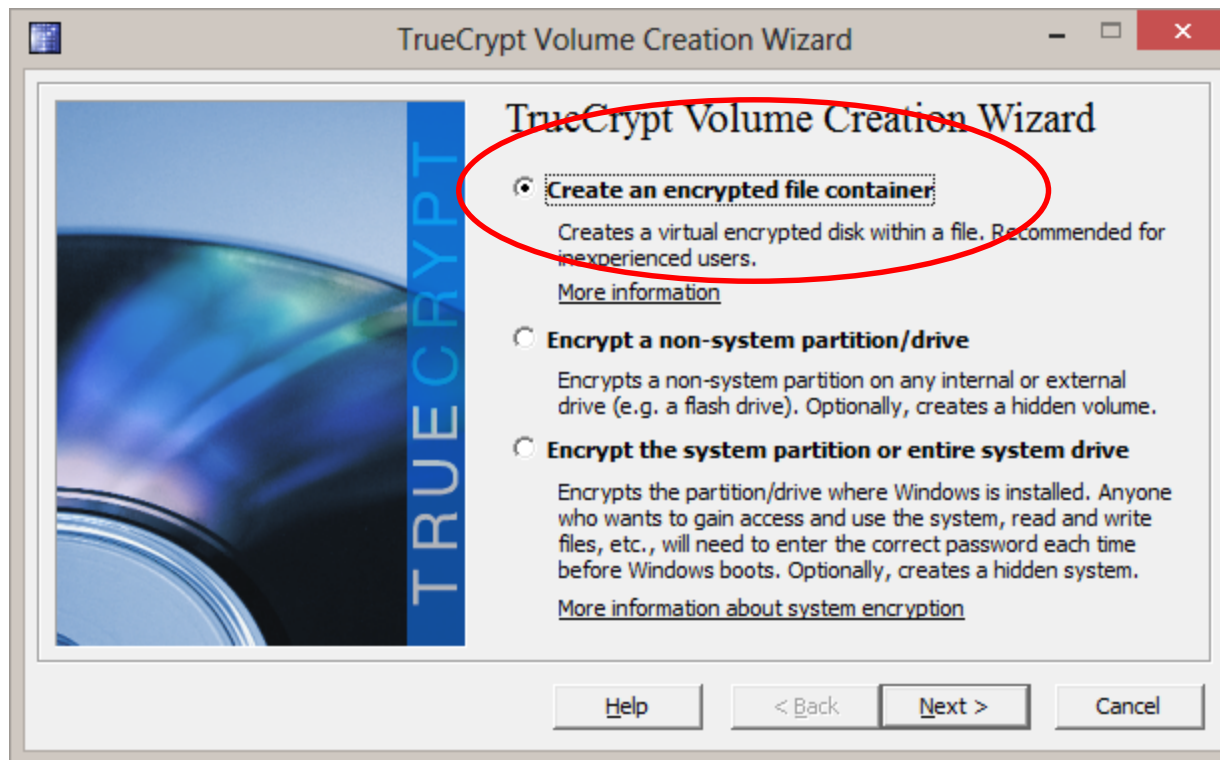
TrueCrypt

A TrueCrypt-tel titkosítani tudunk egész partíciót, valamint titkosított fájlokat hozhatunk létre, melyeket aztán úgy mountolhatunk, mint új merevlemez.

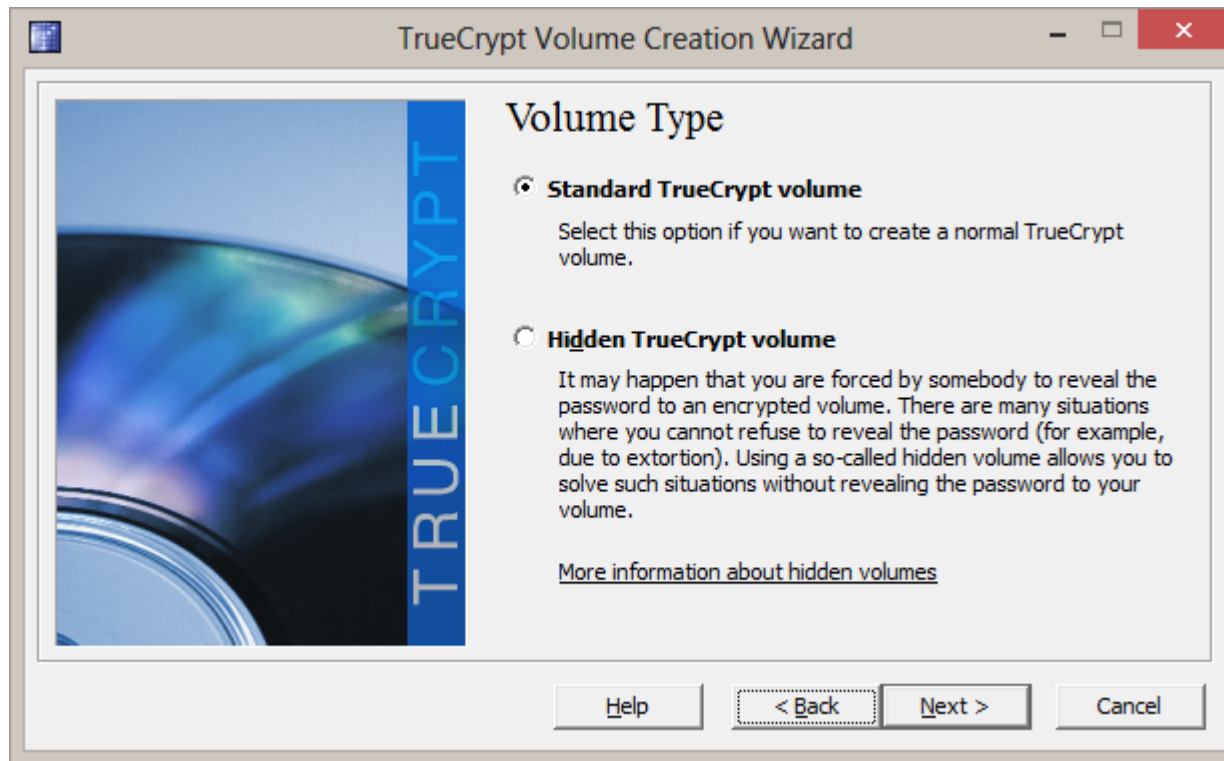
Ha az egész partíció titkosítva van, akkor van egy nagy hátránya: a teljes partíciót formattálni kell, tehát **MINDEN ADAT EL FOG VESZNI!**



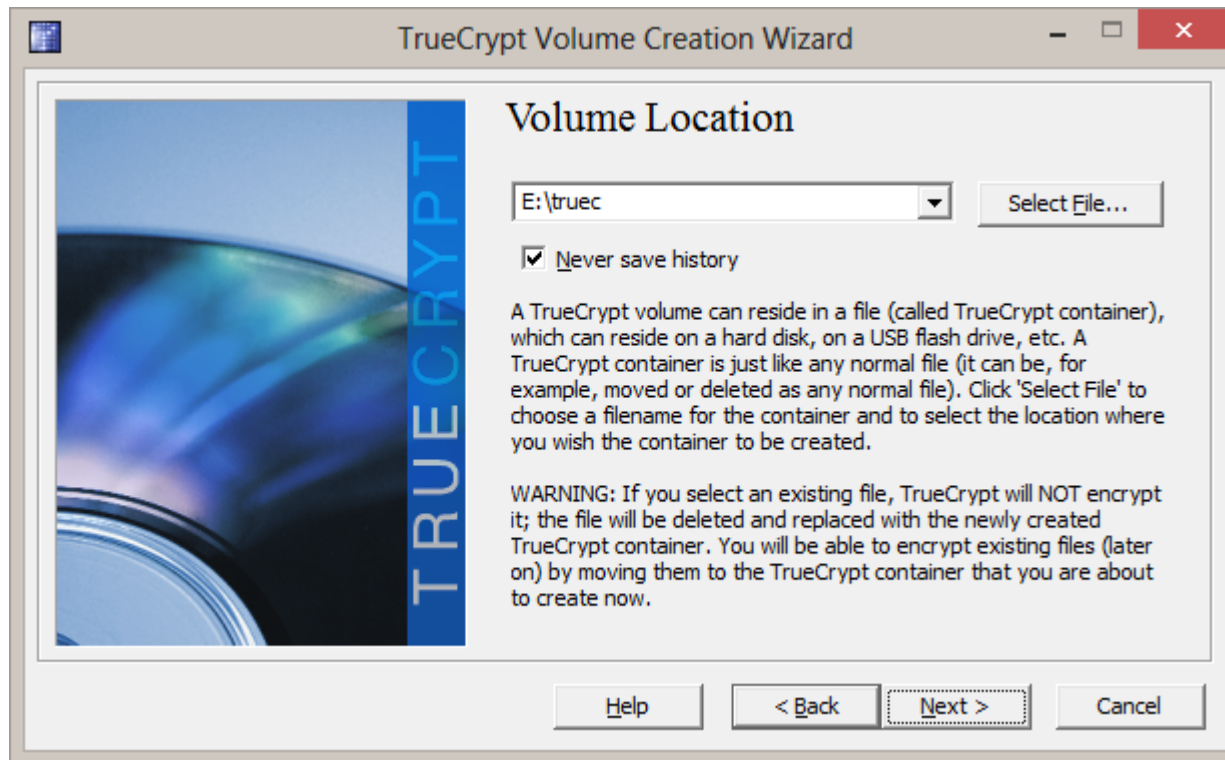




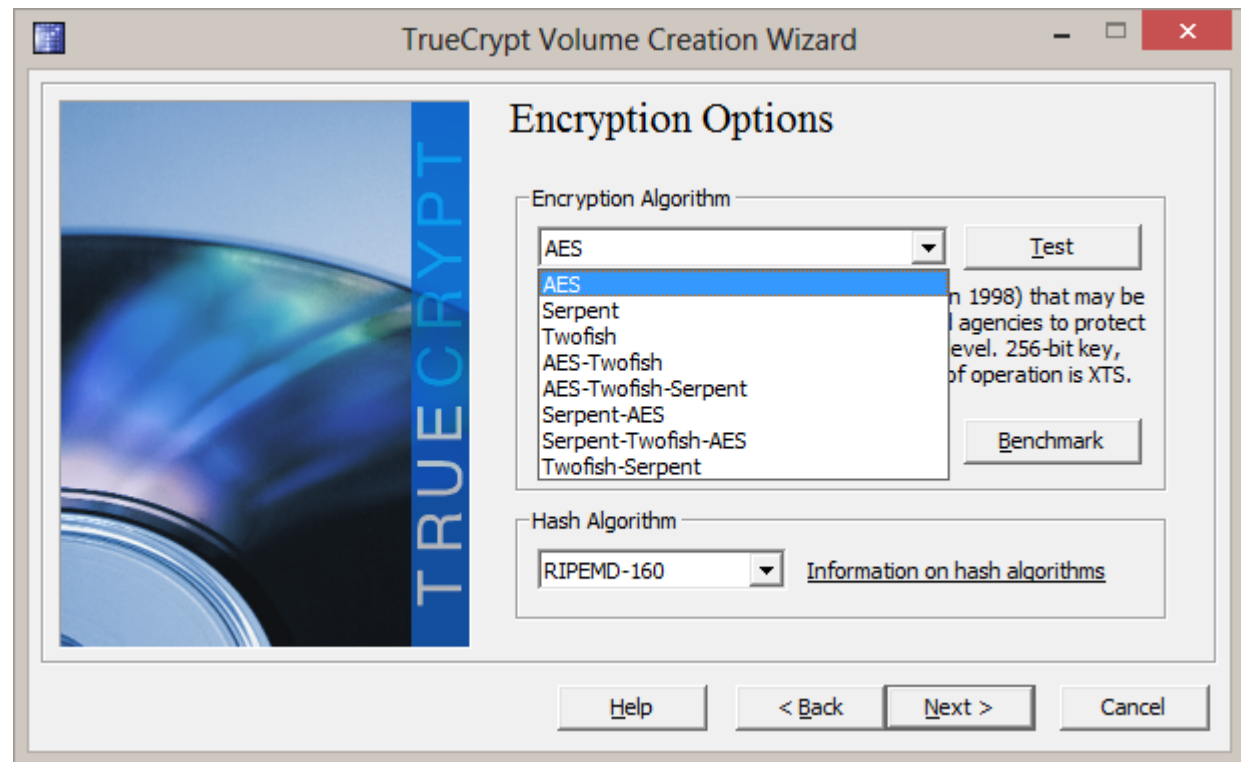
A **Hidden** konténer annyiban tud többet, hogy két jelszó tartozik hozzá. Gyakorlatilag egy konténer a konténerben.



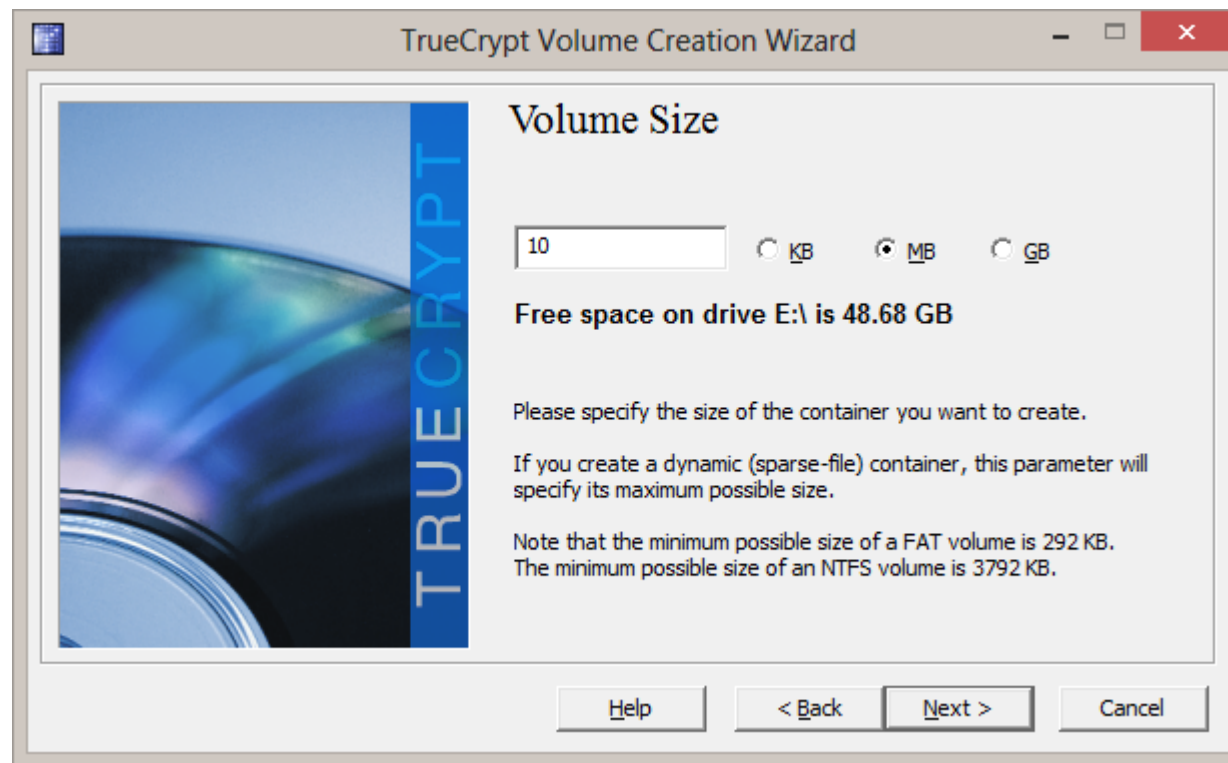
Hová mentjük el a konténert.




Kiválasztjuk a **titkosítási módszert** (algoritmust)



A konténer **méretének** megadása (FAT32-nél 2GB-nál nem lehet nagyobb)

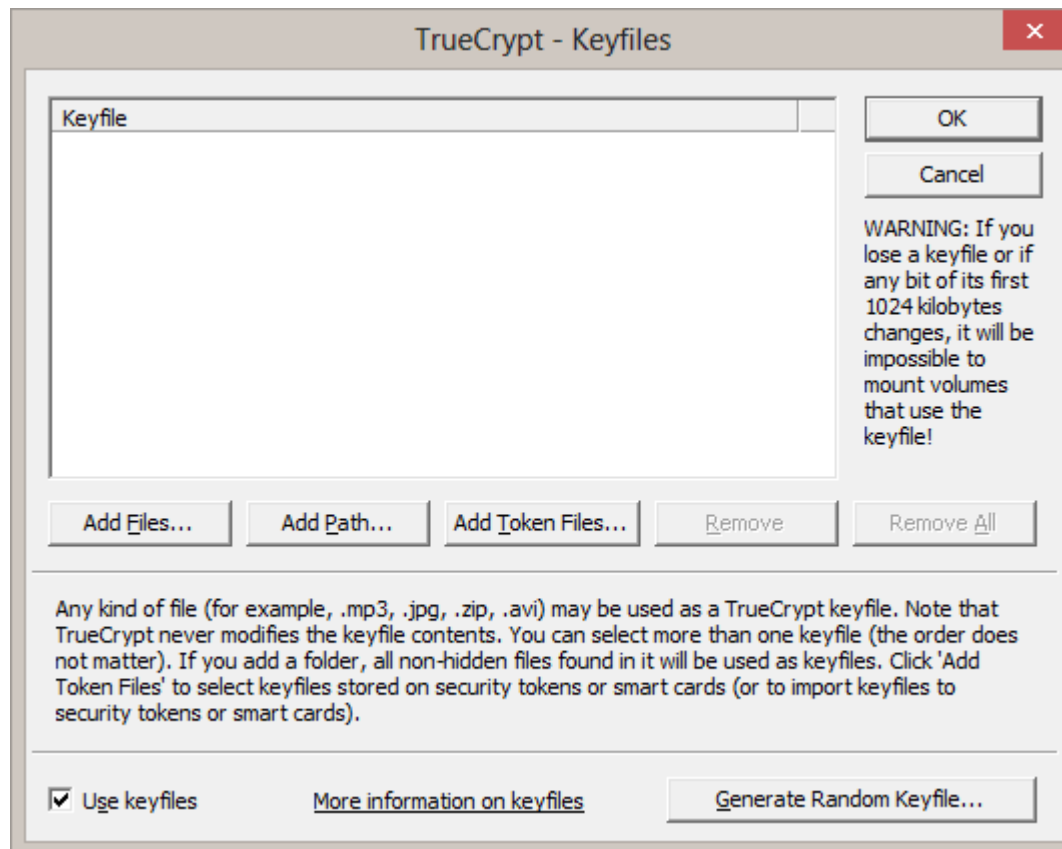


Jelszó megadása:

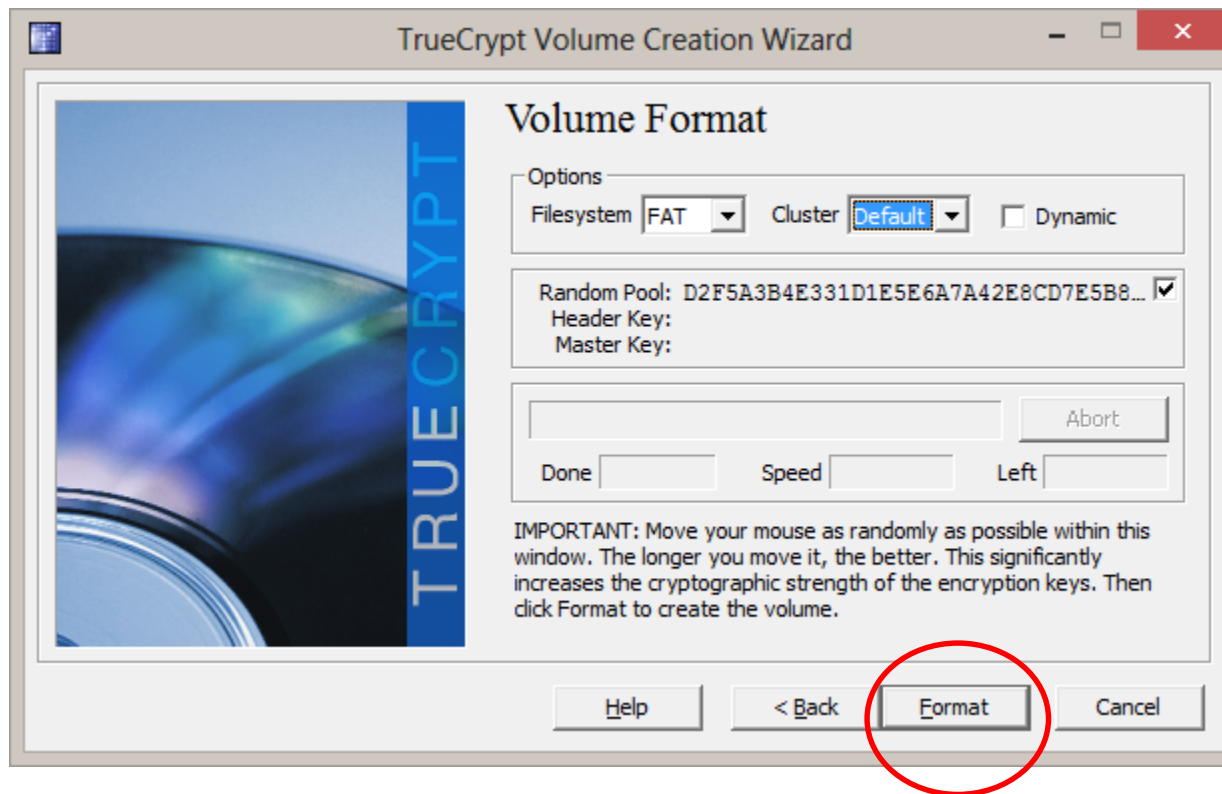


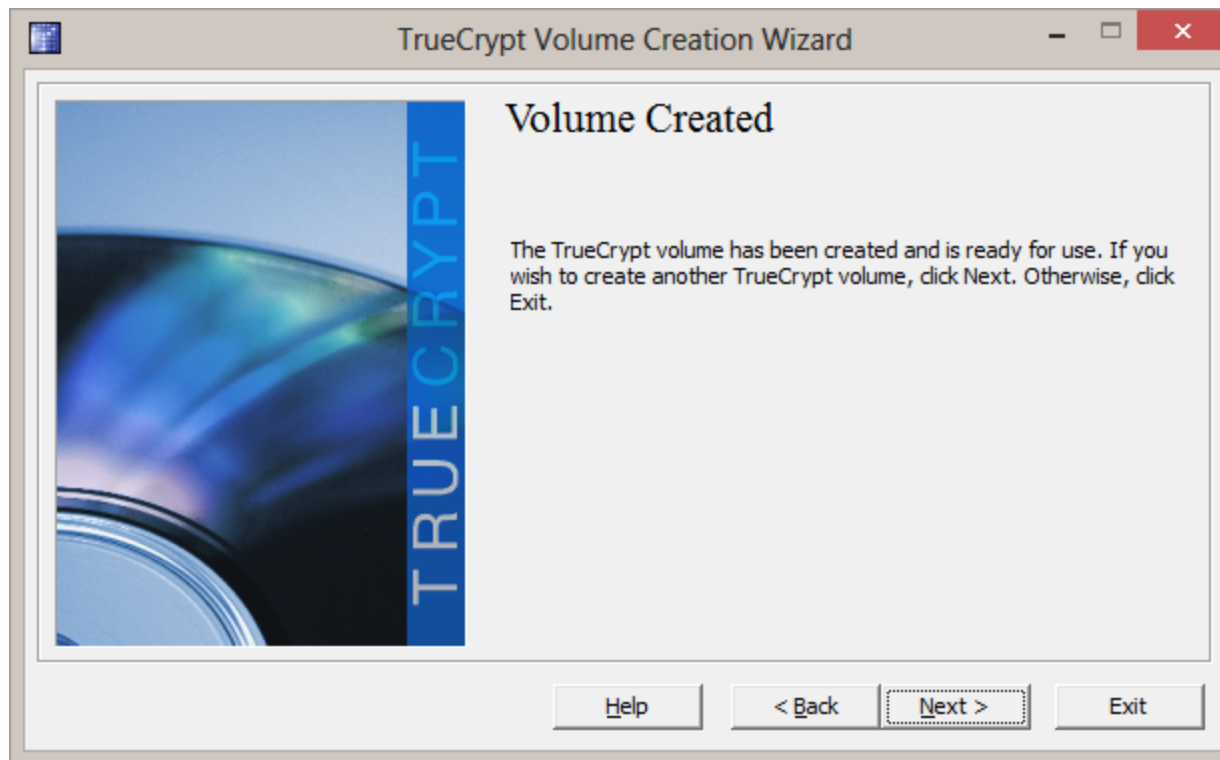
The image shows a screenshot of the TrueCrypt Volume Creation Wizard, specifically the 'Volume Password' step. The window has a title bar with the text 'TrueCrypt Volume Creation Wizard' and standard Windows window controls (minimize, maximize, close). On the left side of the window, there is a vertical blue bar with the word 'TRUECRYPT' written in white capital letters. The main area of the window is titled 'Volume Password' and contains the following elements:

- A 'Password:' label followed by a text input field.
- A 'Confirm:' label followed by a text input field.
- Two checkboxes: 'Use keyfiles' and 'Display password'. The 'Display password' checkbox is currently checked.
- A 'Keyfiles...' button next to the 'Use keyfiles' checkbox.
- A paragraph of text providing instructions on how to choose a good password: 'It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.'
- Four buttons at the bottom: 'Help', '< Back', 'Next >', and 'Cancel'.

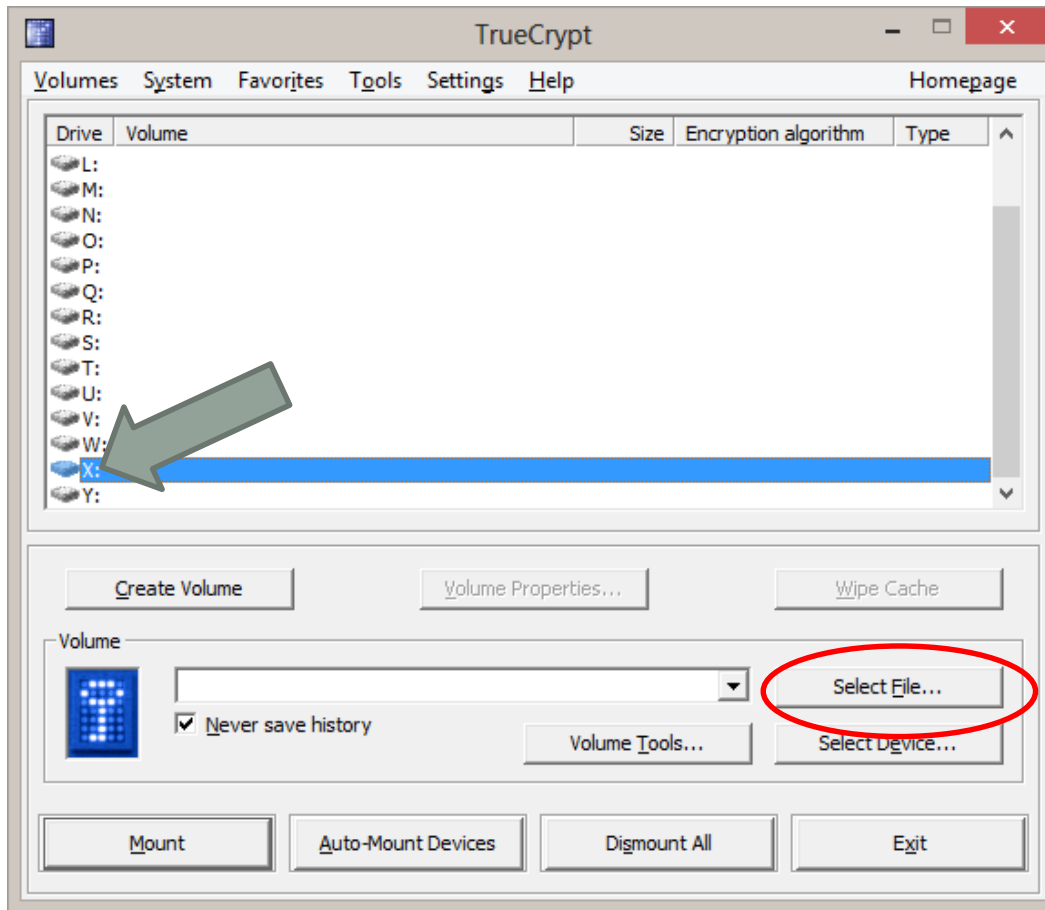


A program legenerálja a **jelszó-hest**,

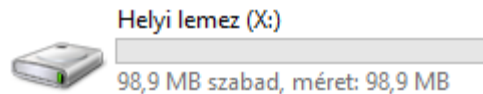
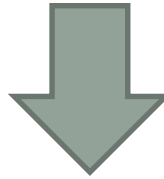
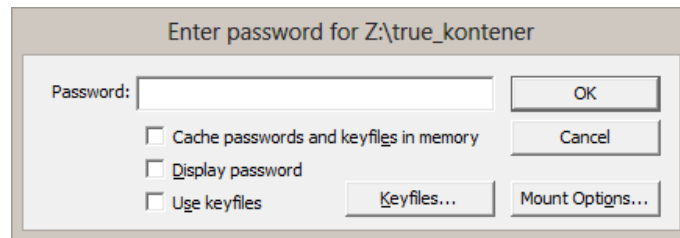




Kiválasztjuk a konténer **fájlunkat** és megadjuk a mountolni kívánt **meghajtót**.

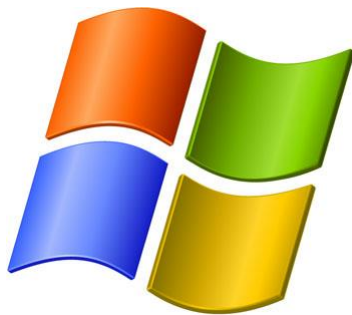


A jelszó vagy kulcsfájl megadása után megjelenik egy teljesen új meghajtó a rendszerünkben.



EFS

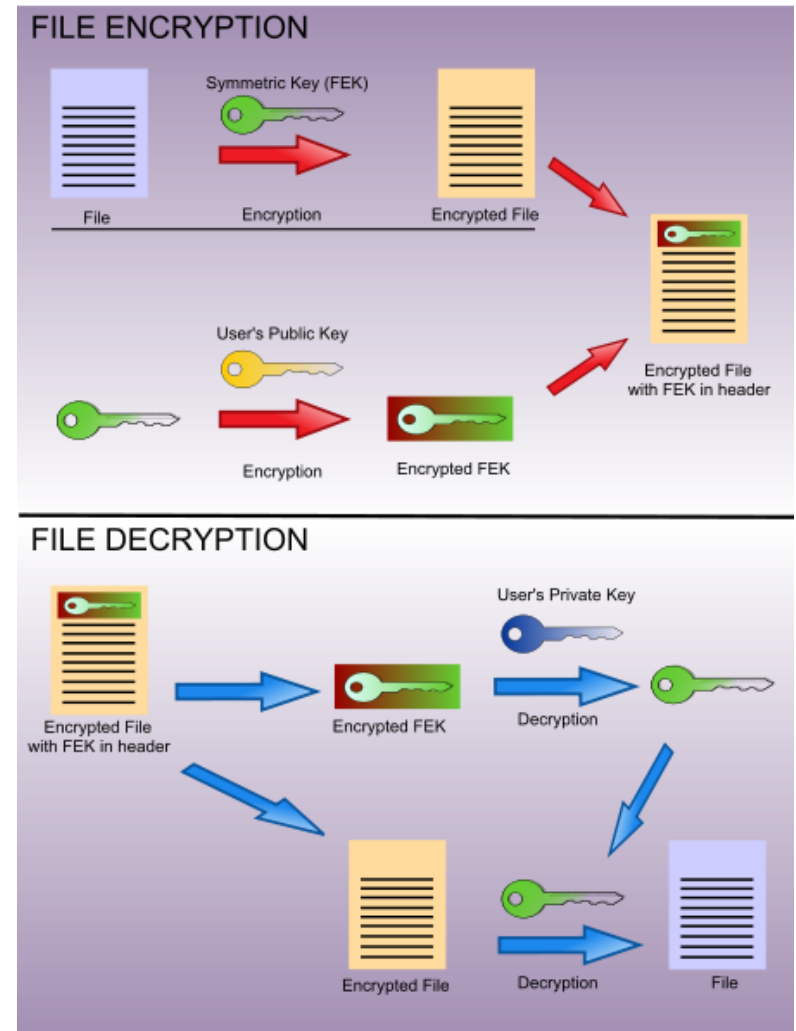
fájltitkosítás

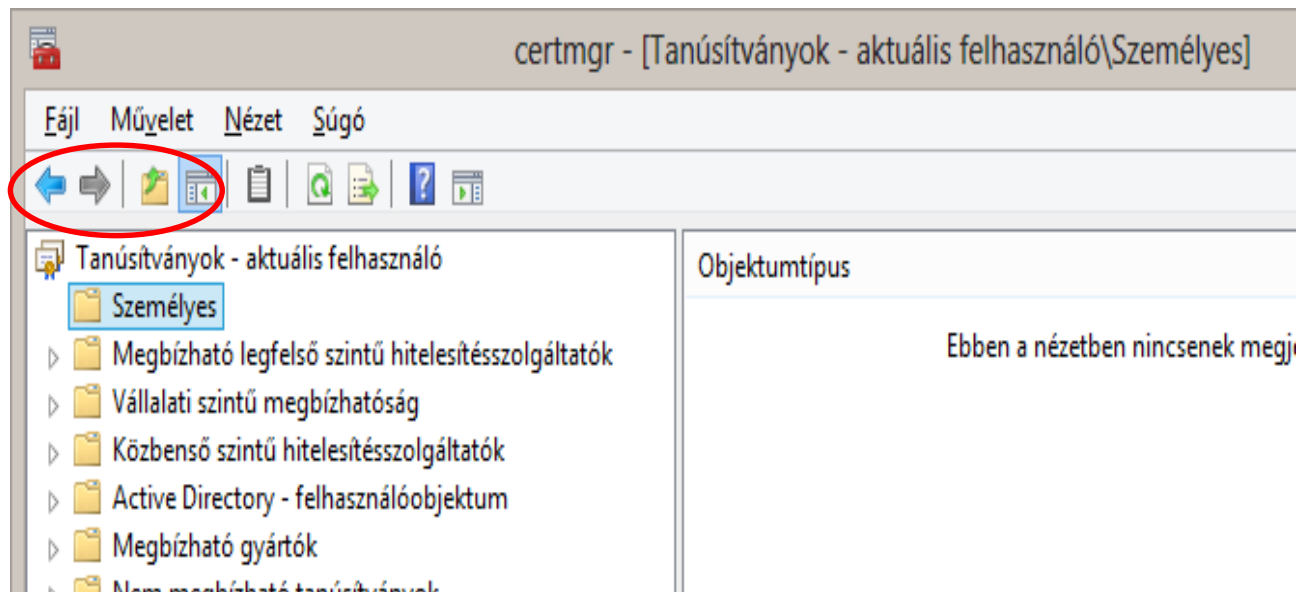
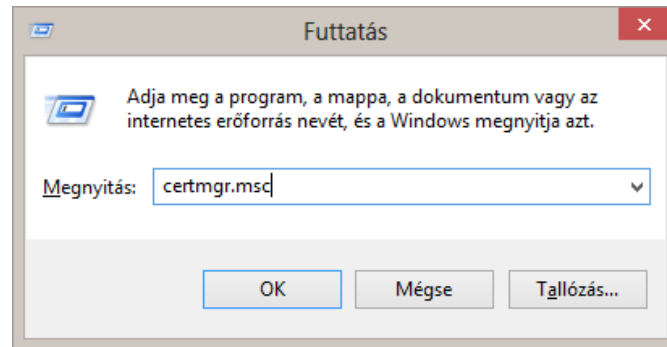


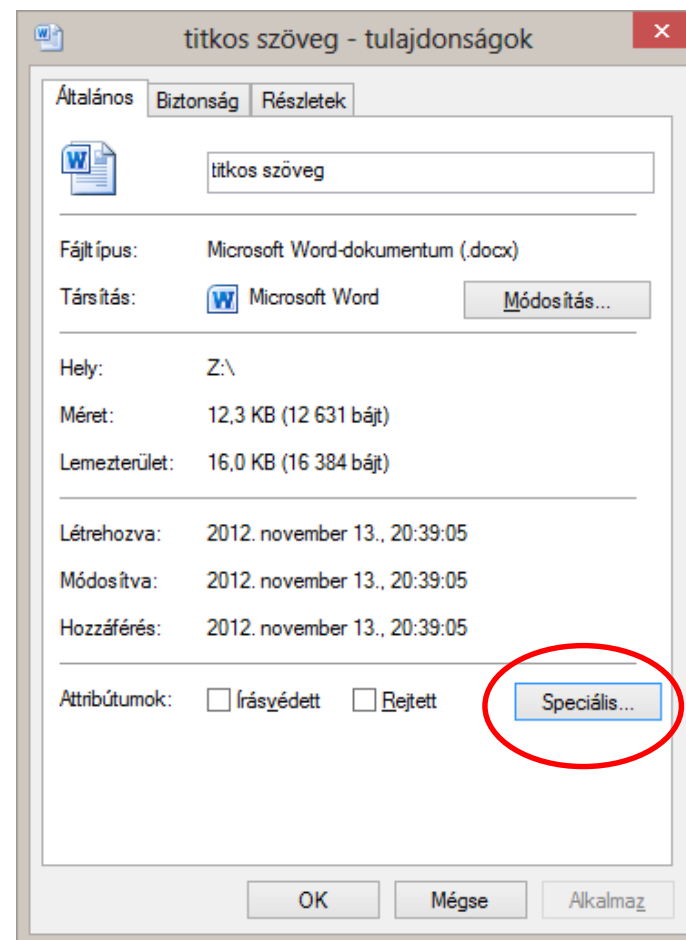
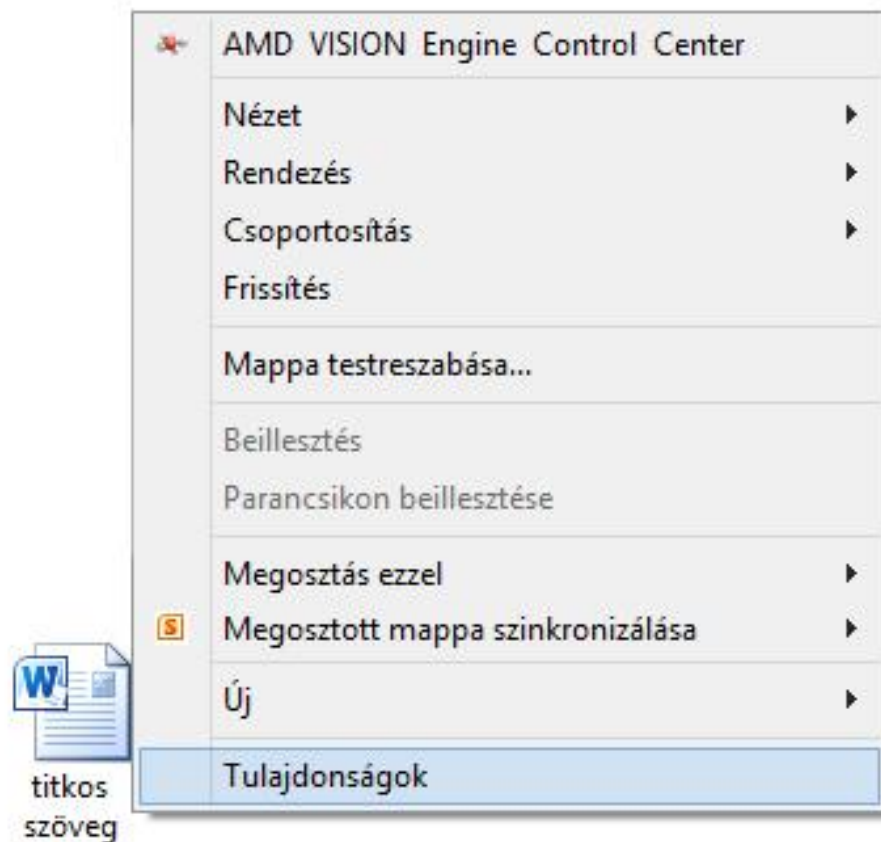
EFS (Encrypting File System)

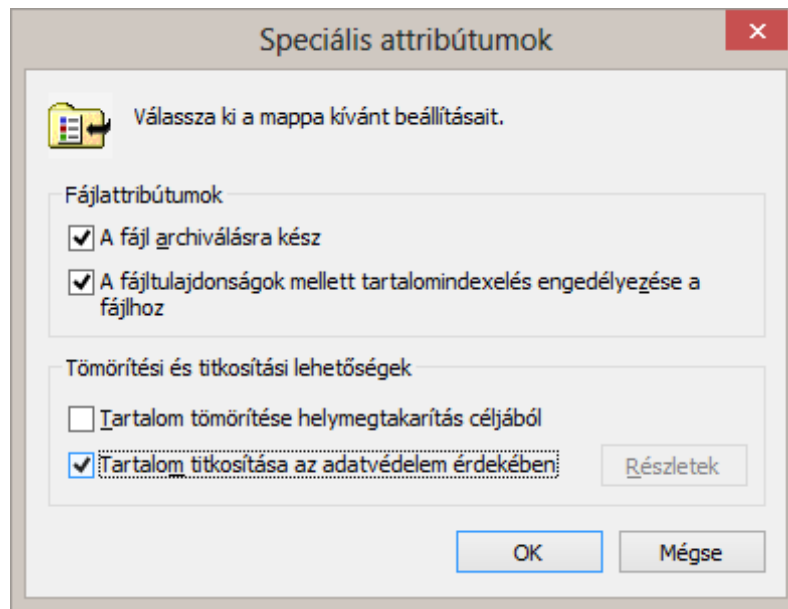
A titkosított fájlrendszer (EFS) egy olyan Windows szolgáltatás, amely lehetővé teszi, hogy a merevlemezen titkosított formátumban tárolja az információkat.

NTFS fájlrendszer !!!









titkos
szöveg





Titkosított fájlrendszer



Fájltitkosító tanúsítvány és kulcs biztonsági mentése

A biztonsági másolat elkészítését követően könnyebben elkerülheti, hogy végleg hozzáférhetlenné váljanak a titkosított fájlok akkor, ha elvesz vagy megsérül az eredeti tanúsítvány és a kulcs.



Biztonsági mentés most (ajánlott)

Célszerű biztonsági másolatot készíteni a tanúsítványról és a kulcsról cserélhető adathordozóra.



Biztonsági mentés később

A Windows emlékeztetni fogja a következő bejelentkezés alkalmával.

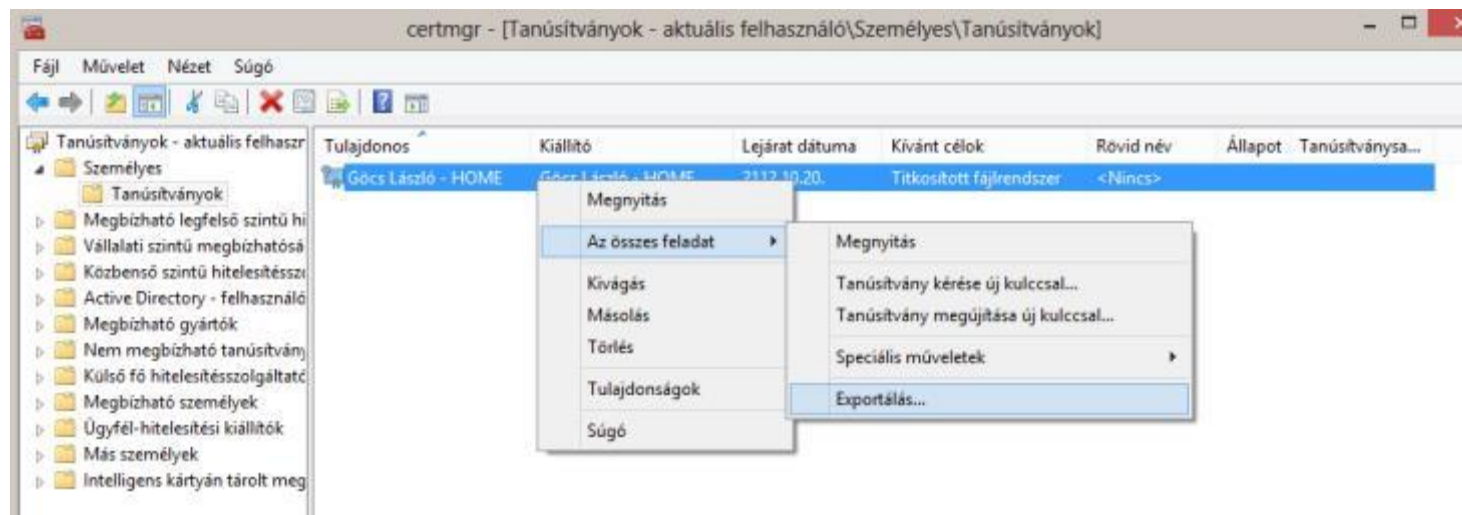
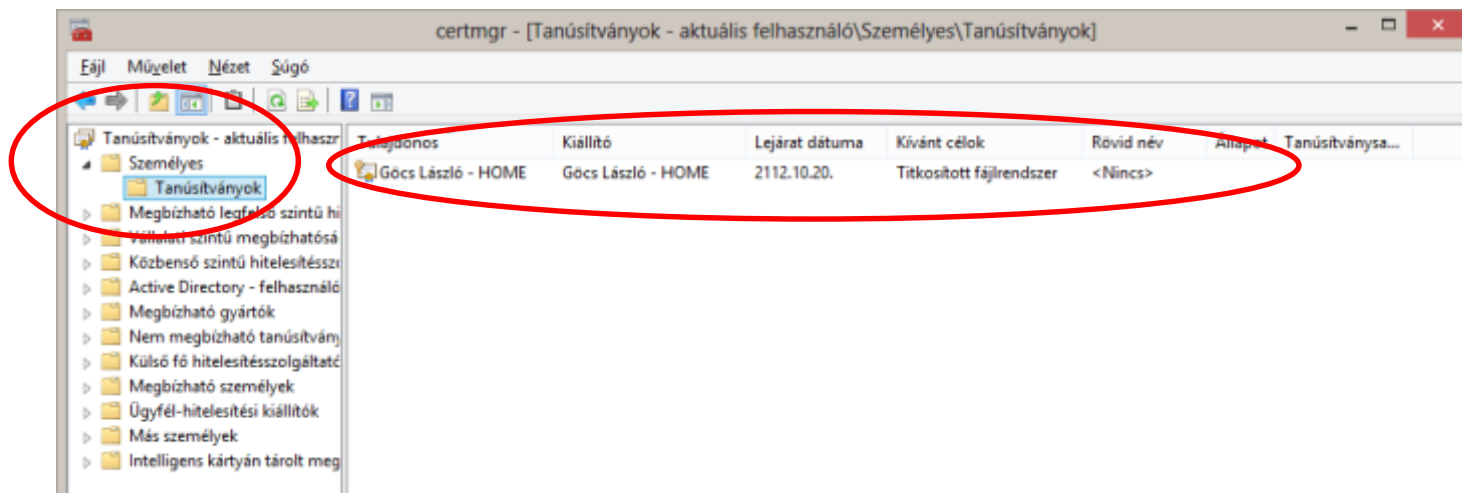




Sose készüljön biztonsági másolat

Ha így dönt, elveszítheti a hozzáférést a titkosított fájlokhoz.

Mégse

[Miért ajánlott biztonsági másolatot készíteni a tanúsítványról és a kulcsról?](#)



  Tanúsítványexportáló varázsló

A titkos kulcs exportálása

Exportálhatja a titkos kulcsot a tanúsítvánnyal együtt.

A titkos kulcsokat jelszó védi. Ha exportálni akarja a titkos kulcsot a tanúsítvánnyal, akkor egy későbbi oldalon meg kell majd adnia a jelszót.

Exportálja a tanúsítvánnyal a titkos kulcsát is?



☒ Igen, a titkos kulcs exportálását választom

☐ Nem, nem akarom exportálni a titkos kulcsomat

További tudnivalók [a titkos kulcsok exportálásáról](#)

Iovább

Mégse

  Tanúsítványexportáló varázsló

Biztonság

A biztonság megőrzése érdekében védje a titkos kulcsot jelszó használatával vagy rendszerbiztonsági taghoz rendelve azt.

☐ Csoport- vagy felhasználónevek (ajánlott)

Hozzáadás

Távolítás

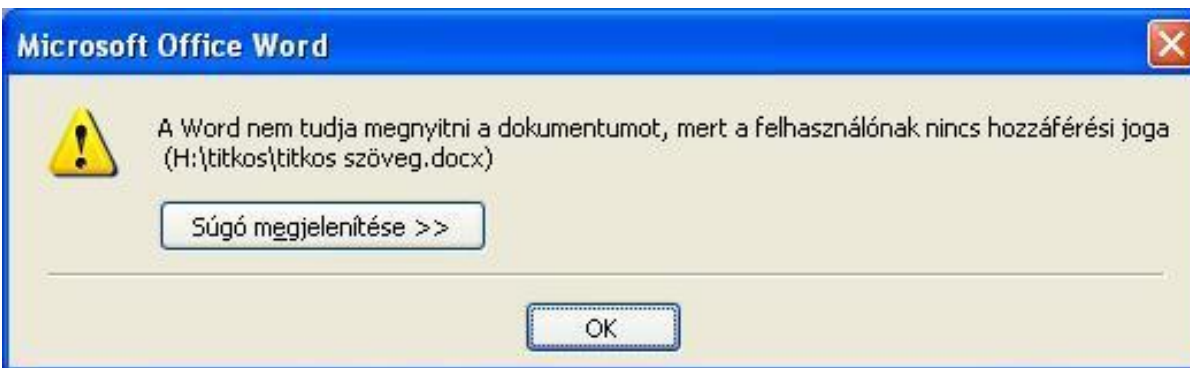
☒ Jelszó:

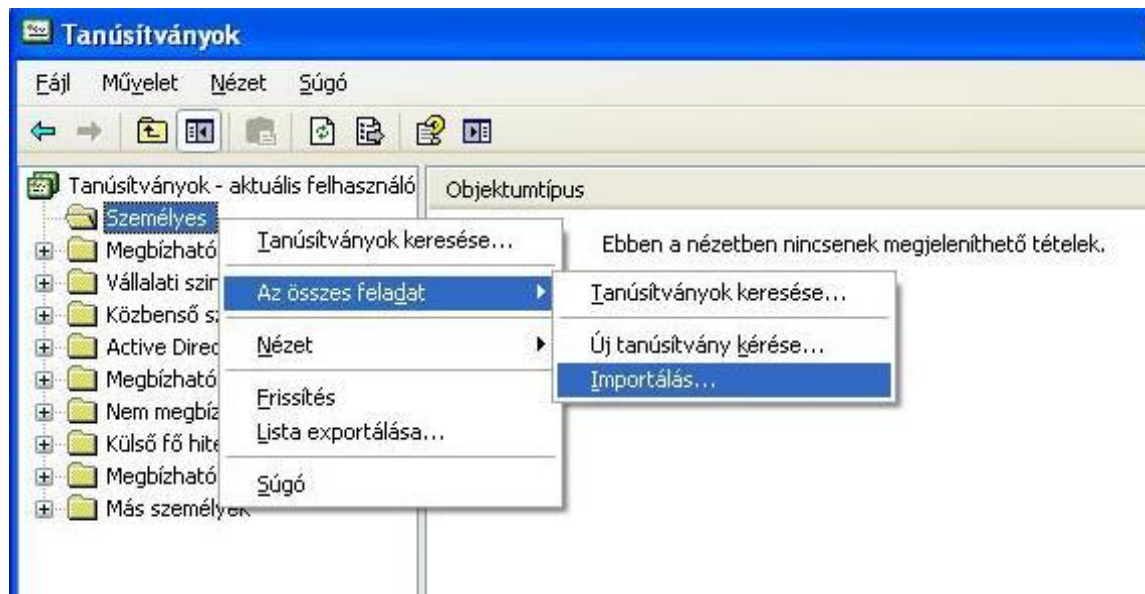
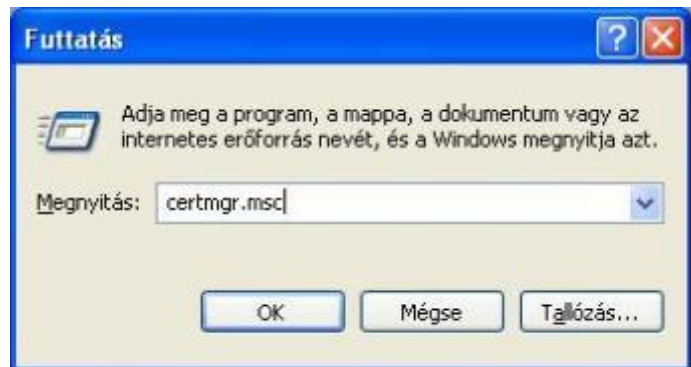
Jelszó megerősítése:

További tudnivalók [a titkos kulcsok védelméről](#)

Iovább

Mégse





Tanúsítványimportáló varázsló

Importálandó fájl

Adja meg az importálandó fájlt.

Fájlnév:

H:\titkos\kulcs.pfx

Tallózás...

Megjegyzés: Több tanúsítvány is tárolható egyetlen fájlban a következő formátumokban:

Személyes információcsere - PKCS #12 (.PFX, .P12)

Titkosított üzenetek szintaxisának szabványa - PKCS #7 tanúsítványok (*.P7B)

Microsoft szerIALIZED tanúsítványtároló (.SST)

< Vissza

Tovább >

Mégse

Tanúsítványimportáló varázsló

Jelszó

A biztonság kedvéért a személyes kulcsot jelszóval lehet védeni.

Adja meg a személyes kulcs jelszavát.

Jelszó:

☐

Személyes kulcs erős védelmének engedélyezése. Ha engedélyezi ezt a beállítást, akkor figyelmeztetést kap minden alkalommal, amikor egy alkalmazás használja a személyes kulcsot.

☐

A kulcs megjelölés exportálhatóként. Ez lehetővé teszi a kulcsok biztonsági mentését és átvitelét.

< Vissza

Tovább >

Mégse

