

INFORMATIKAI BIZTONSÁG ALAPJAI

Levelező - 3. konzultáció

Göcs László
főiskolai tanársegéd
*Neumann János Egyetem GAMF Műszaki és Informatikai Kar
Informatika Tanszék*

Titkosítás, hitelesítés



Titkosítás

A **titkosítás** vagy **rejtjelezés** a kriptografiának 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

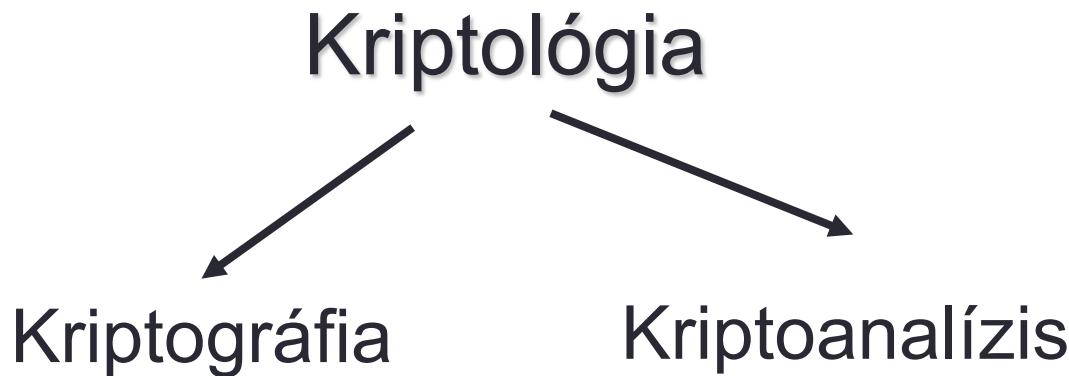
Lehetővé teszi:

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

A kriptográfia alapvető feladata

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

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



Kriptográfia

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

Kriptoanalízis

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

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, védeeltségét, 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 függvényel*, 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 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 különböző 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. Sérhetetlenség (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 küldődjék 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 (acess control)
pl. szoftverek, adatbázisok védelme, pay per view TV csatornák
- banki tranzakciók
- elektronikuskereskedelem
vevő+bank+bolt, mindenki csak a rá tartozó információkat lássa
- elektronikuspénztárca
- elektronikusszavazás (*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 kriptografiával, ahol a támadó észreveheti, feltörheti és módosíthatja az üzenetet, a szteganográfia célja, hogy a **nyílt szöveget úgy rejts 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, összegyűrták 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 gépelet 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 parázzsal "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 **ugyanezt 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, Purple, 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
- Blaise 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 kriptoanalízis 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 helyettesítéses módszer (monoalfabetikus helyettesítés)

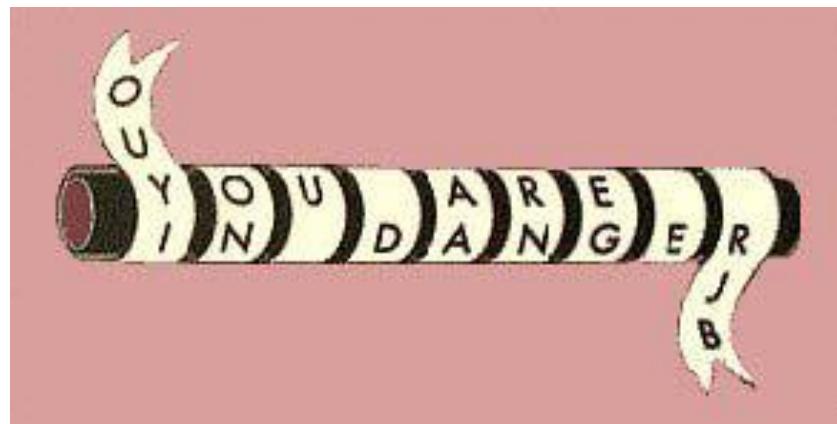
- minden betűt az ábécében a hárommal utána következővel helyettesített ($\text{Kulcs}=3$)
(általánosítottabb változatában $0 < \text{Kulcs} < 26$)
- xxxxxxxxxx szónak **LQIRUPDWLND** felel meg ?

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 spártaik
- 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

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

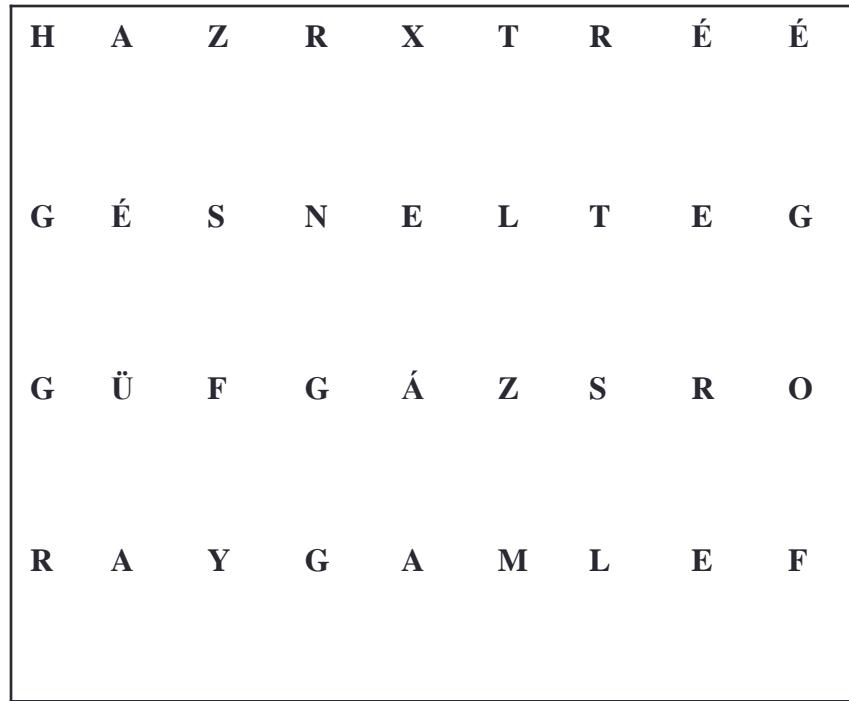
titkosírások több irodalmi műben
fontos szerepet kapnak.

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		

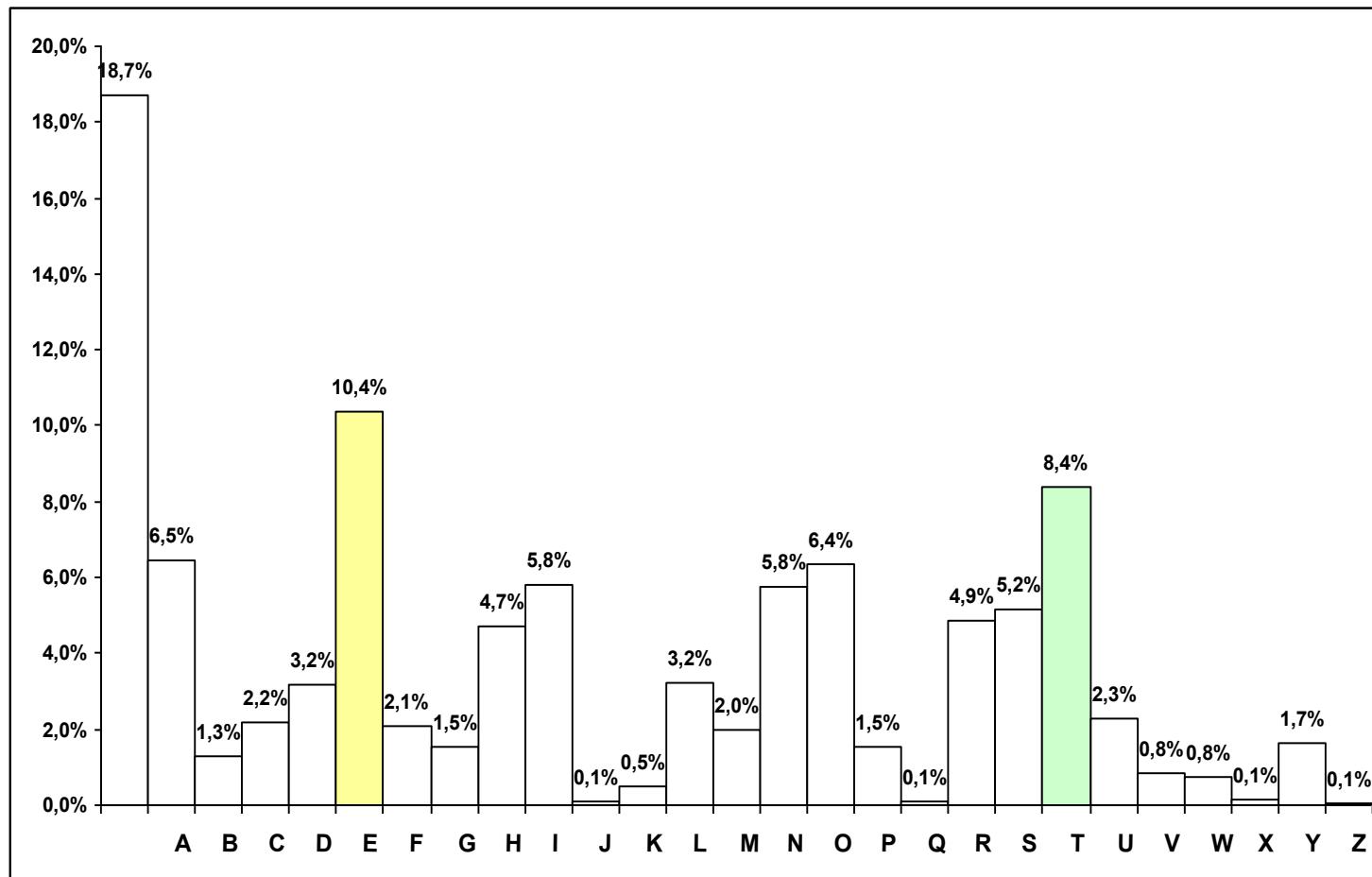
Ráhelyezve a szövegre a lyukak (X) helyén felbukkanó betűket leírva, majd a rostélyt negyed fordulattal elfordítva a következő szöveg jön ki:



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

...FELMAGYARORSZÁGFÜGGETLENSÉGÉRTXRZAH

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
- **GHYMESGHYMESGHYMESGHYMESGHYMESGHYM**
- **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?
NTATAXEOKSEUGRUOLLIANATIFIKKNXYMSKLN

- **GHYMES** GHYMES GHYMES GHYMES GHYMES GHYMES GHYMES
- 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



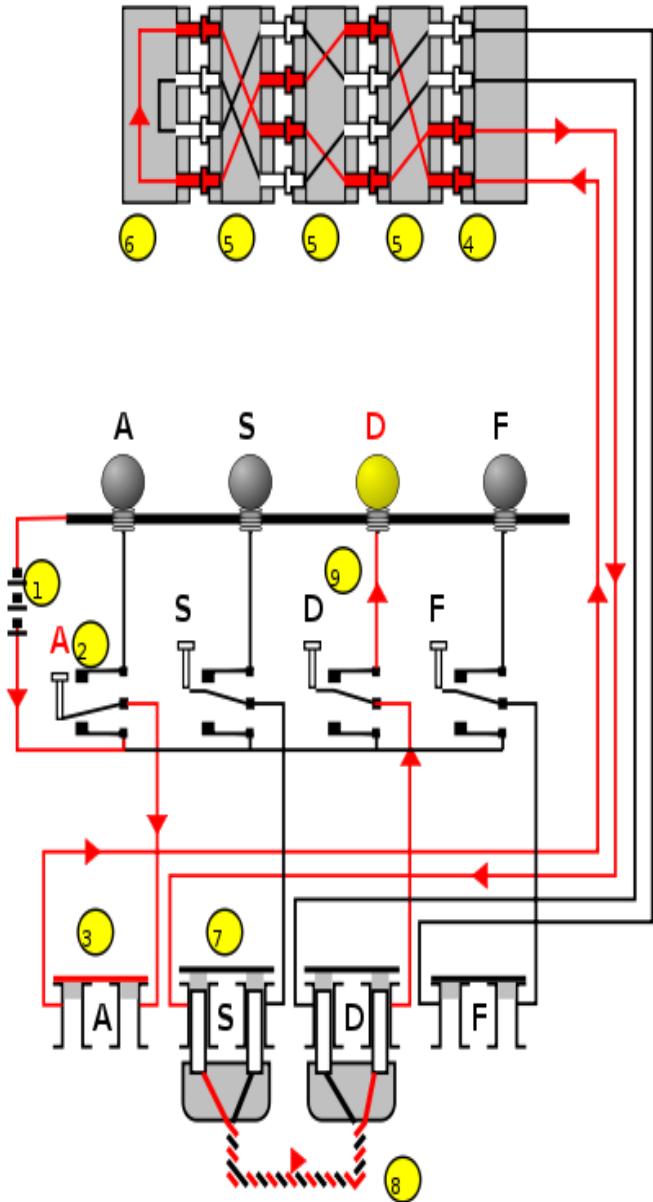
három forgó tárca
(rotor) + reflektor

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

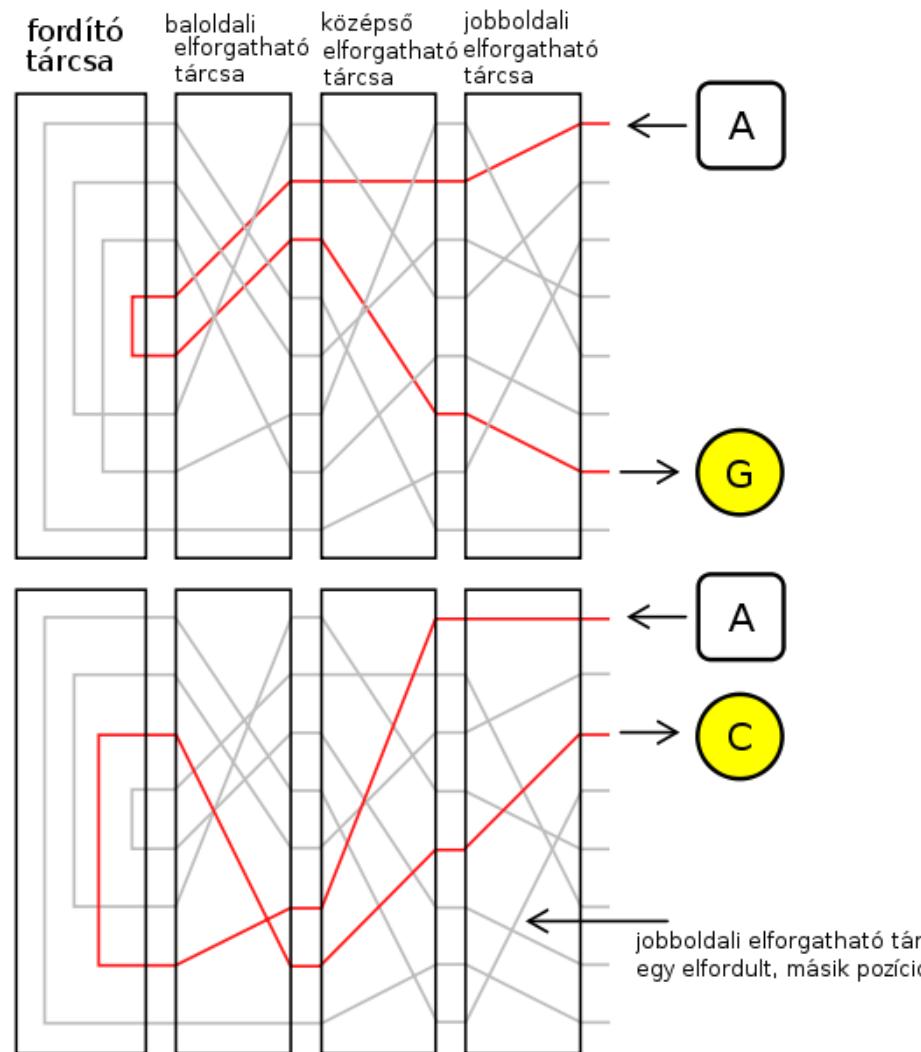
Billentyűzet 26 betű

Kapcsolótábla
stecker

ENIGMA



- minden tárcsának 26 beállítási helyzete van.
- A 26 harmadik hatványa 17.576.
- Ha ezt összeszorozzuk a tárcsakiválasztás lehetséges eseteinek számával (60), 1.054.560-at kapunk eredményül.
- Ha ezt az eredményt megszorozzuk a lehetséges kapcsolótábla csatlakozások számával ami kb. 150 millió!
- 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

Film: Kódjátszma (2014) "The Imitation Game"

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 nemzetseg, 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

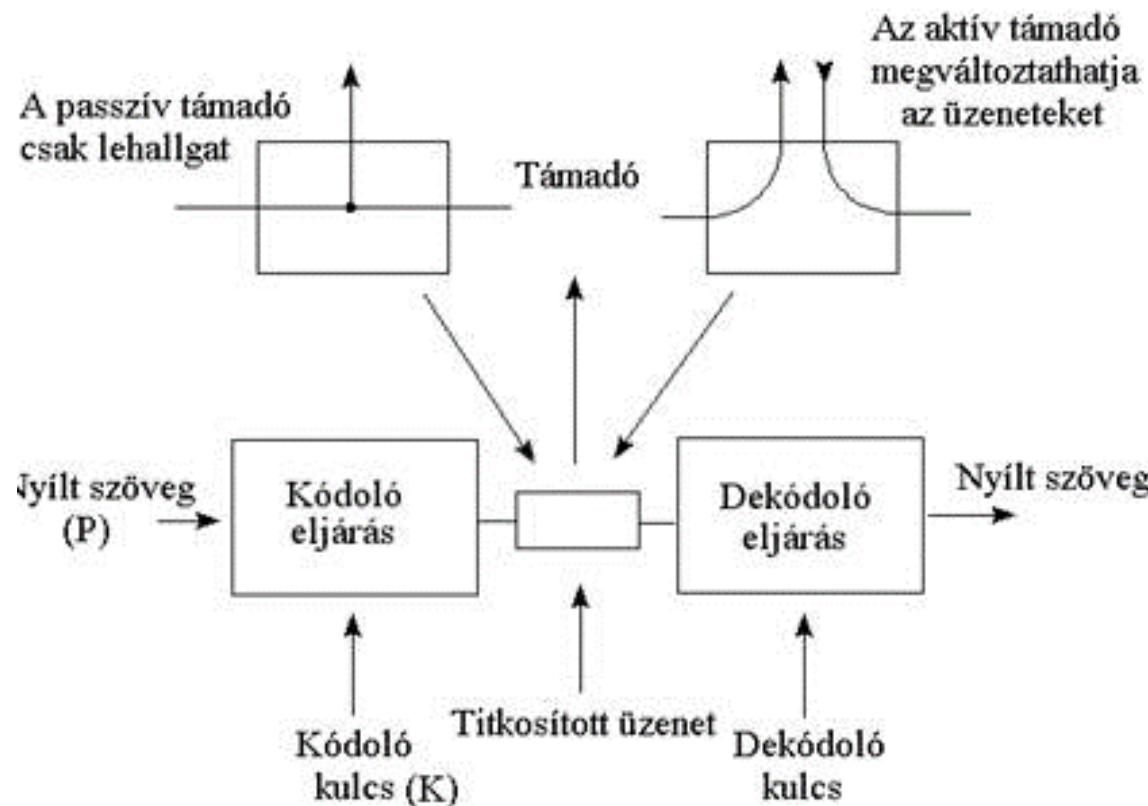
- Mit kell védeni?
Az információt.
- Melyik információt kell védeni?
Az értékeset.
- Mi az értékes információ?
Amit annak tartunk.
- Hol van az értékes információ?
Adathordozón vagy átviteli csatornán.
- Mitől kell védeni az értékes információt?
Megsemmisüléstől, eltulajdonítástól.

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 elrejti, **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 elérhetők, **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.

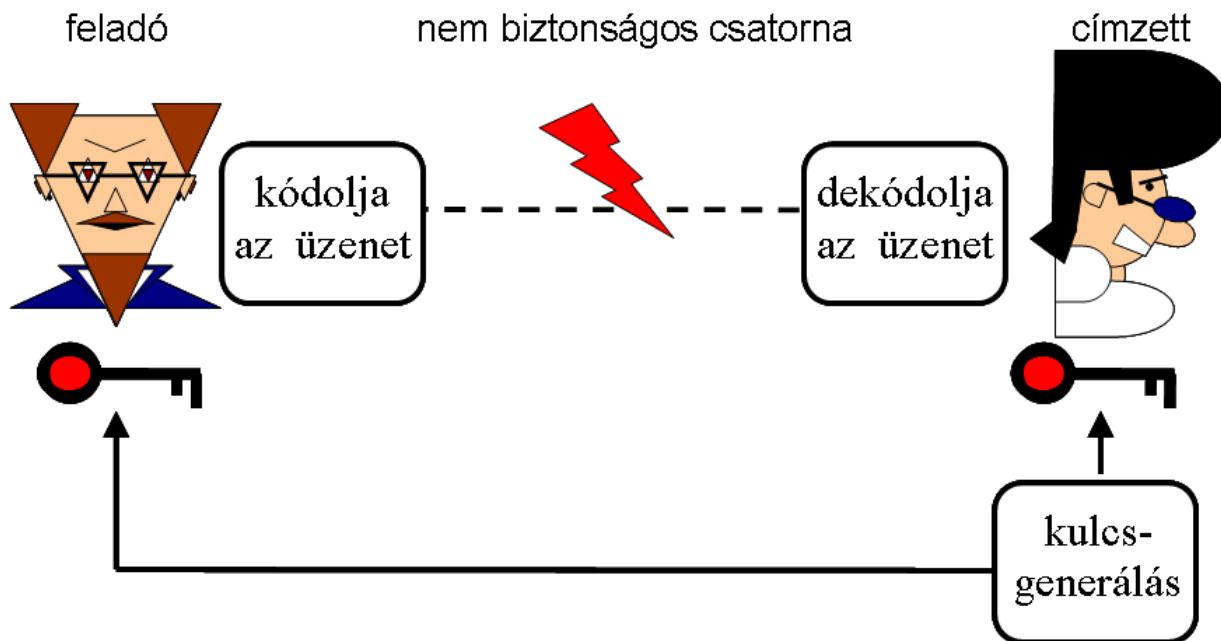
SZIMMETRIKUS KULCSÓ TITKOSÍTÁS

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,

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

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

- titkosított M üzenet a k kulcs ismeretében könnyen kiszámítható – ez a **titkosítás folyamata**.
- A titkosított M üzenetből könnyen kiszámítható az eredeti üzenet, de csak akkor, ha ismerjük a k kulcsot – ez az **üzenet megoldása**.
- A titkosított 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 C titkosító algoritmus **csak a k kulcs ismeretében** invertálható. Ez a tulajdonság garantálja a Kerckhoff's-elv betartását.

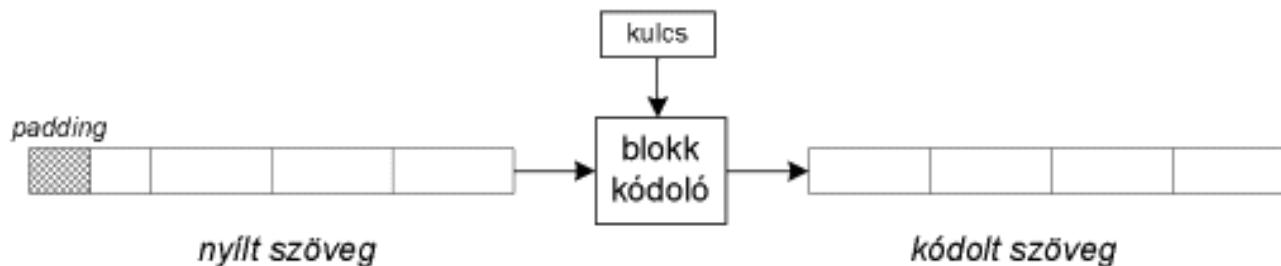
Az ilyen trükkös eljárásokat csapdafüggvényeknek (trapdoor functions) nevezzük. A vissza- felé vezető út, vagyis a titkosított üzenet visszaállítása, elolvasása az

$$m = D_k(M) = C^{-1}_k(M)$$

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

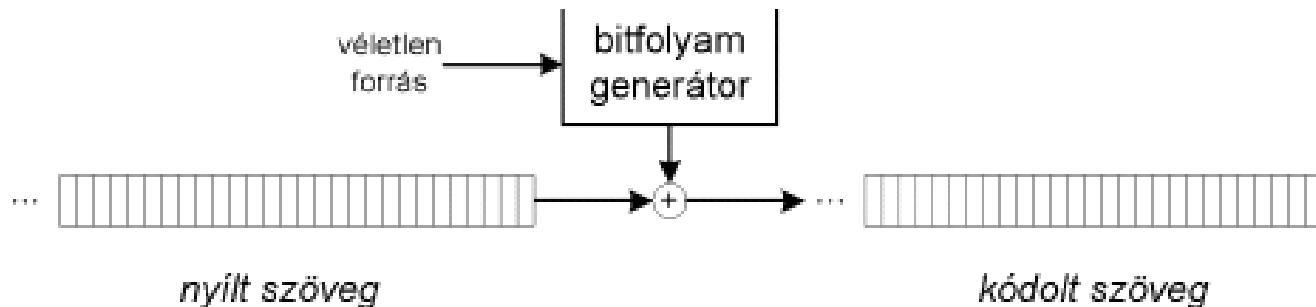
Blokk kódolók

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



Folyamat kódolók

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



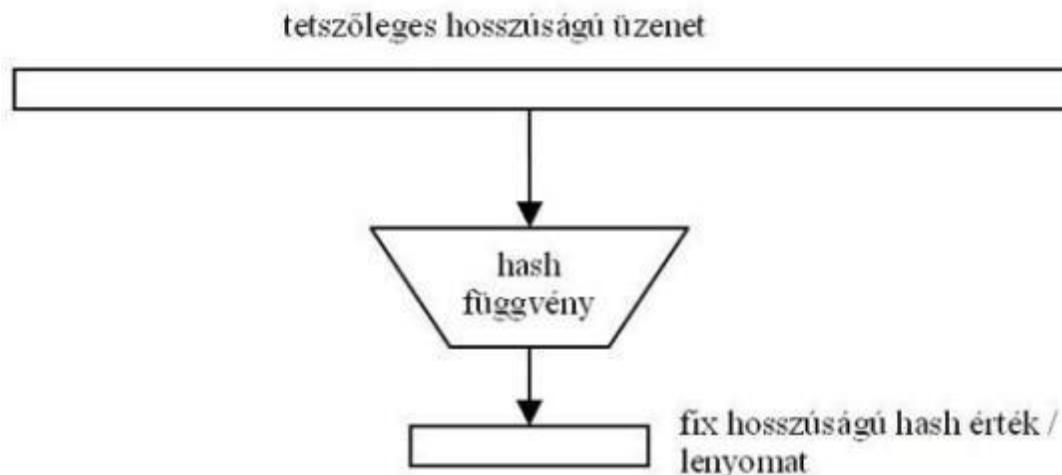
HASH függvények

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 használják a már nem biztonságos MD5 függvényt is. Az MD5 128 bites, a SHA-1 160 bites hash értéket állít elő, viszont minden kettő 512 bites blokkokban dolgozza fel az üzeneteket.

PROTOKOLOK

- **Rejtjelező struktúrák**

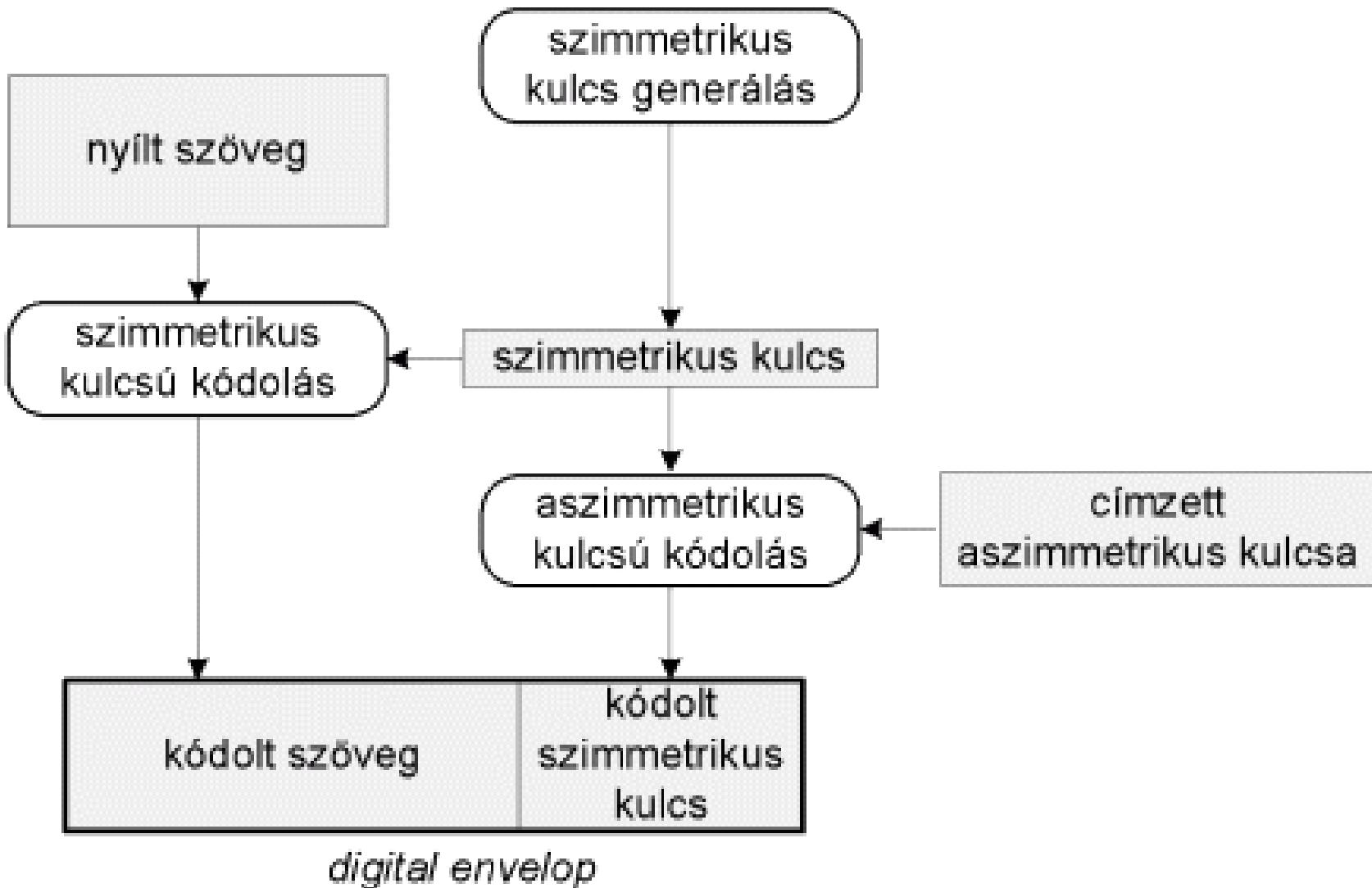
A szimmetrikus kulcsú kódolókat erősebbé tehetjük, ha egymást követő üzenetegységek kódolása során visszacsatolást is alkalmazunk, ezzel elérve azt, hogy ugyanannak az üzenet-részletnek más és más kódoltja lesz.

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)

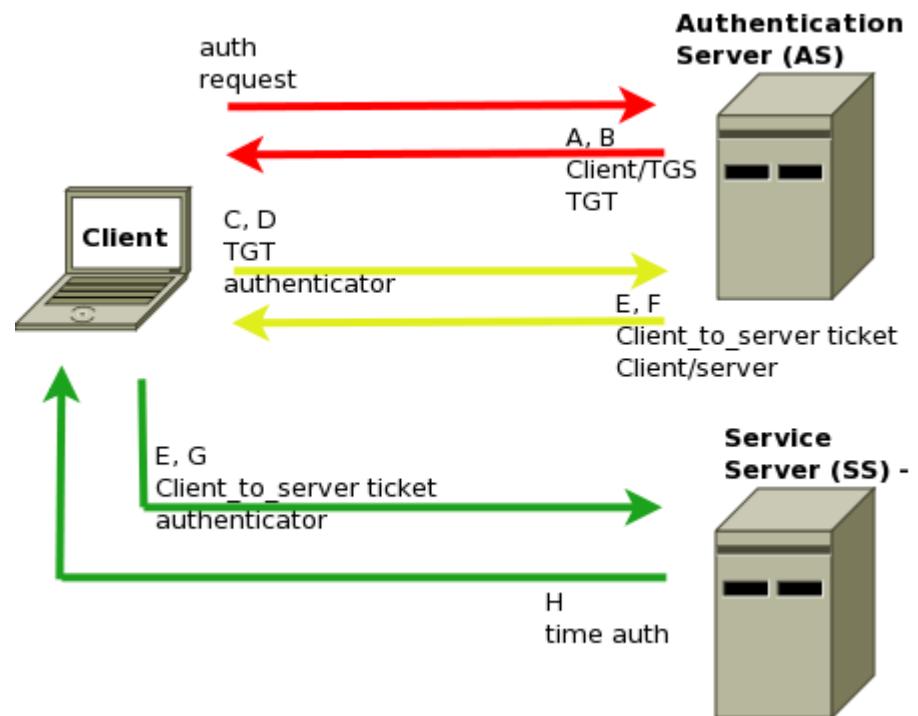
- A rendszerben kel lennie egy mindenki által megbízhatónak elfogadott szervernek (kulcselosztó központ), amellyel való kommunikációhoz **minden félnek létezik** már előre kiosztott, hosszú ideig használatos szimmetrikus kulcsa.
- A felek a **szerver közvetítésével** tudják kicserélni a kettőjük kommunikációjához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

KERBEROS (κερβερος)



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 kidolgozni 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** számsorrá.
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.

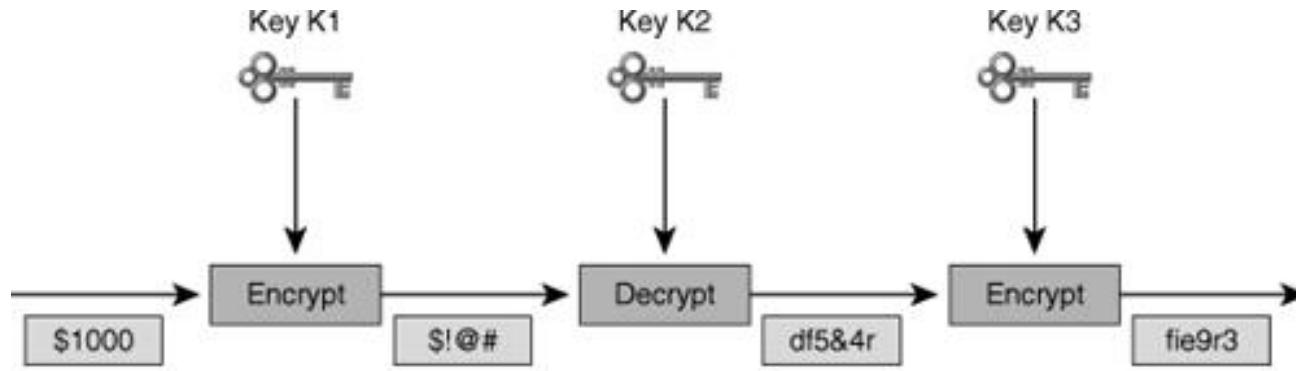
DES (Data Encryption Standard)

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 ≠ 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 egy egyszerű titkosító függvény **16 iterációját** hajtja végre.

Titkosítás, hitelesítés 3



ASZIMETRIKUS KULCSÚ TITKOSÍTÁS

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

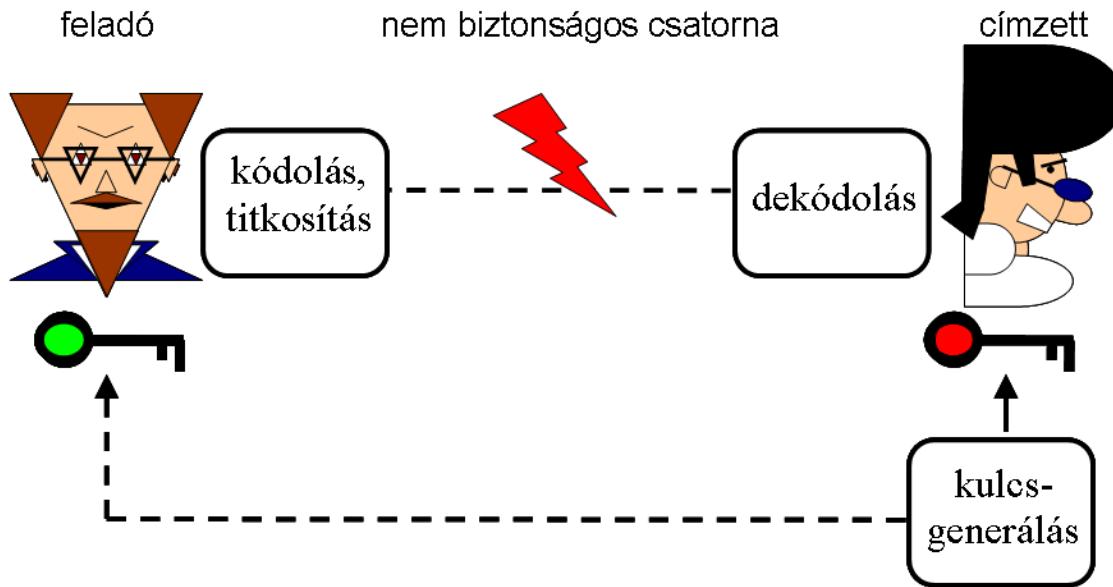
Minden félnek van egy **nyilvános kulcsa** és egy **magánkulcsa**.

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 ō 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 fejti 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 függvényel 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 algoritmusa), 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 aláírót, 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. $N=P \cdot Q$ és $M(N)=(P-1) \cdot (Q-1)$
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 $\varphi(N)$ -re nézve, ez lesz D. (keressünk egy olyan D-t, amelyre **$ED = 1 \text{ mod } \varphi(N)$** teljesül vagyis az **ED szorzat $\varphi(N)$ -nel osztva 1-et ad maradékul.**

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

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

Általános jelöléssel: $a \times a^{-1} = 1 \pmod{m}$, 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 **$\varphi (N)$ -re: D=285**, mert $285 \times 21 \text{ mod } 352 = 1$.
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

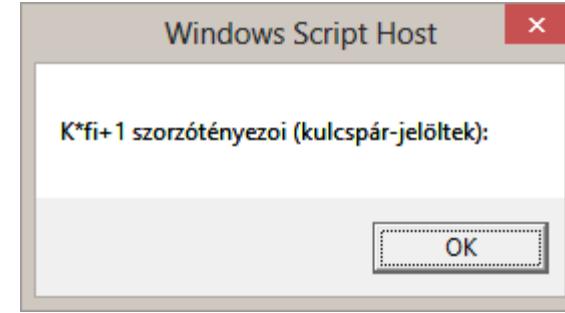
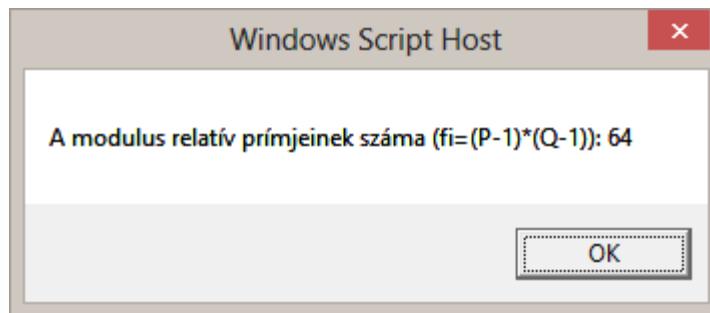
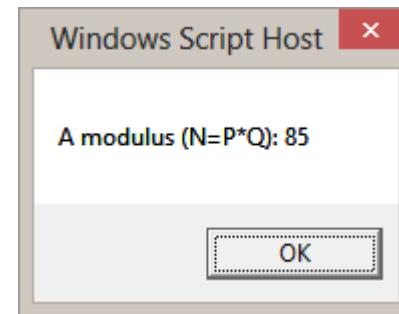
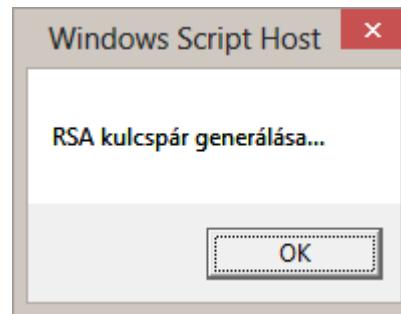
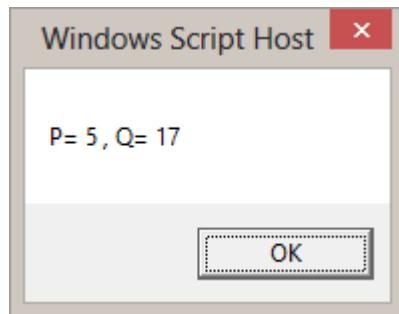
Az átkódolás és a hatványozások eredményét az alábbi táblázat mutatja:

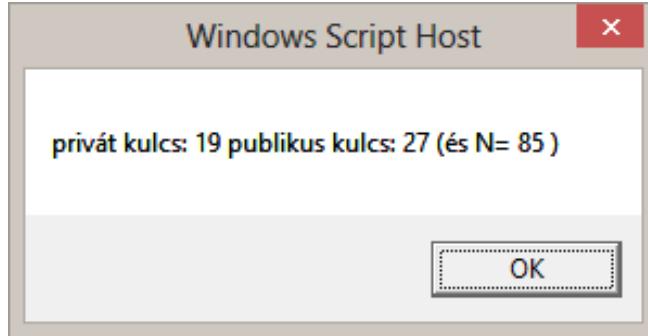
- A „T” ASCII kódja: **84**.
- Az Ő titkosított párja: **$84^{21} \text{ mod } 391 = 135$** , ezt kell elküldeni.
- A fogadó oldalon pedig a **$135^{285} \text{ mod } 391 = 84$** számítást kell elvégezni.

	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
$M_i = m_i^{21} \text{ mod } 391$			$m_i = M_i^{205} \text{ mod } 391$			

RSA kulcsgenerátor

Fóti Marcell (Net Academia)

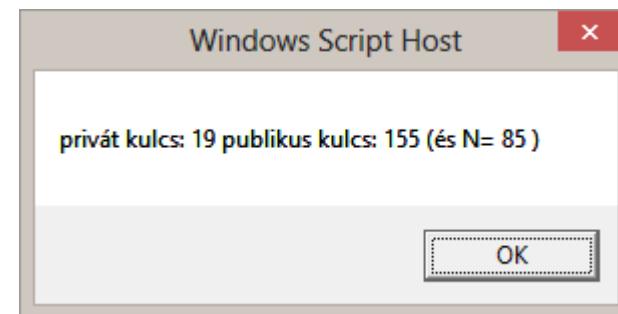
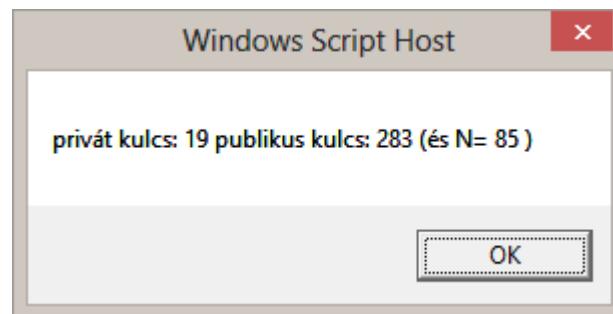
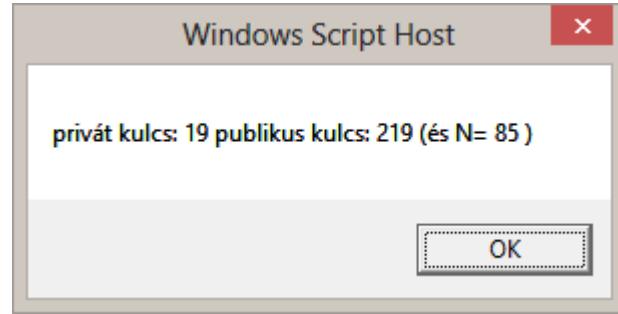
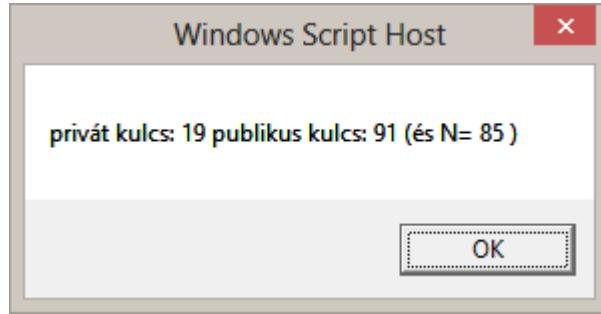




T – titkosítandó adat = „7”
N – modulus = $P \cdot Q = 5 \cdot 17 = 85$
C – titkosított üzenet

$$T^{\text{publikuskulcs}} \bmod N = C \rightarrow 7^{27} \bmod 85 = \mathbf{48} \\ = C$$

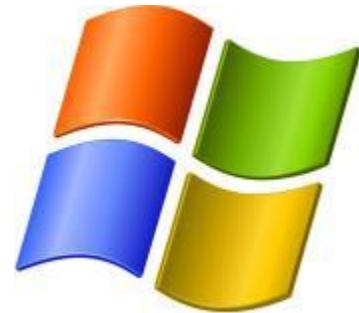
$$C^{\text{privátkulcs}} \bmod N = T \rightarrow 48^{19} \bmod 85 = \mathbf{7} = T$$



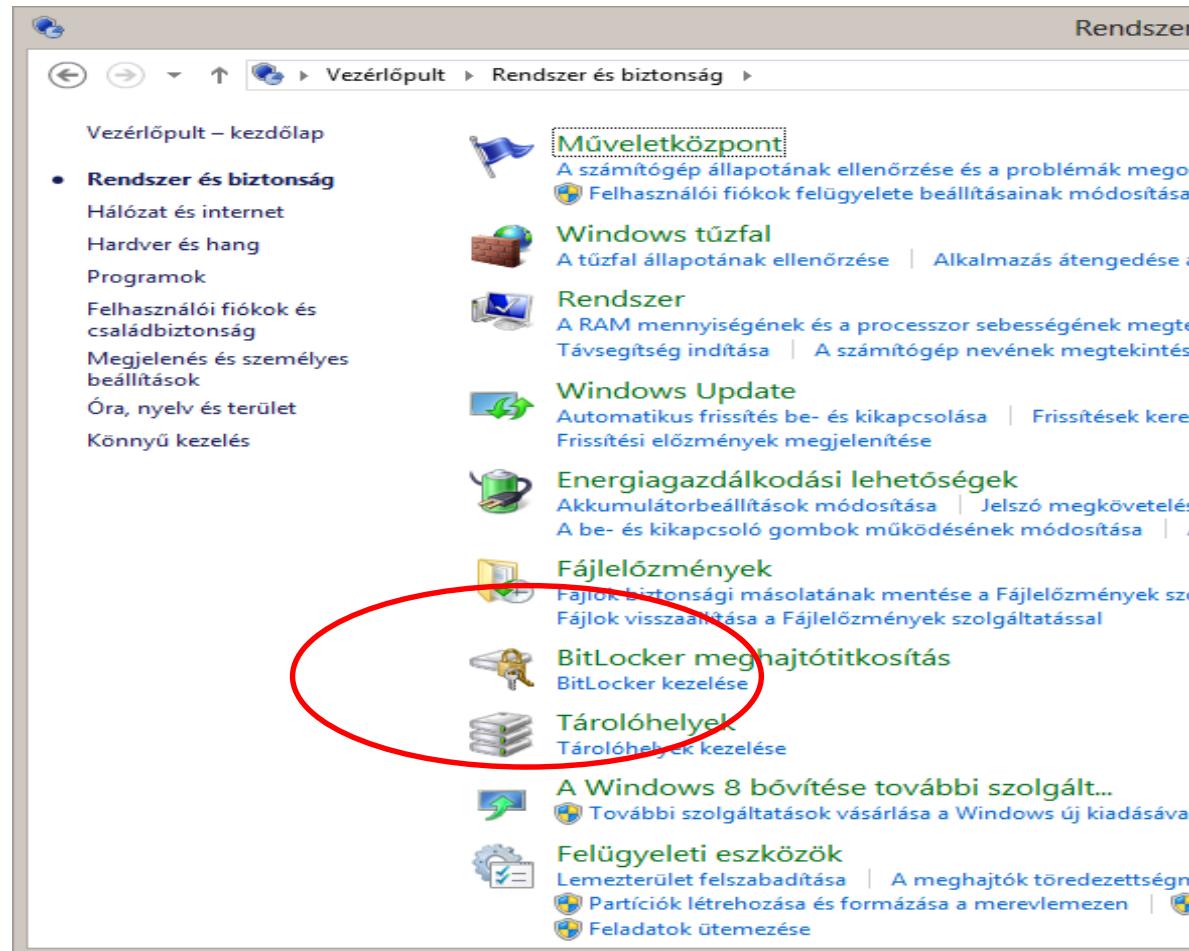
Titkosítási módszerek

BITLOCKER

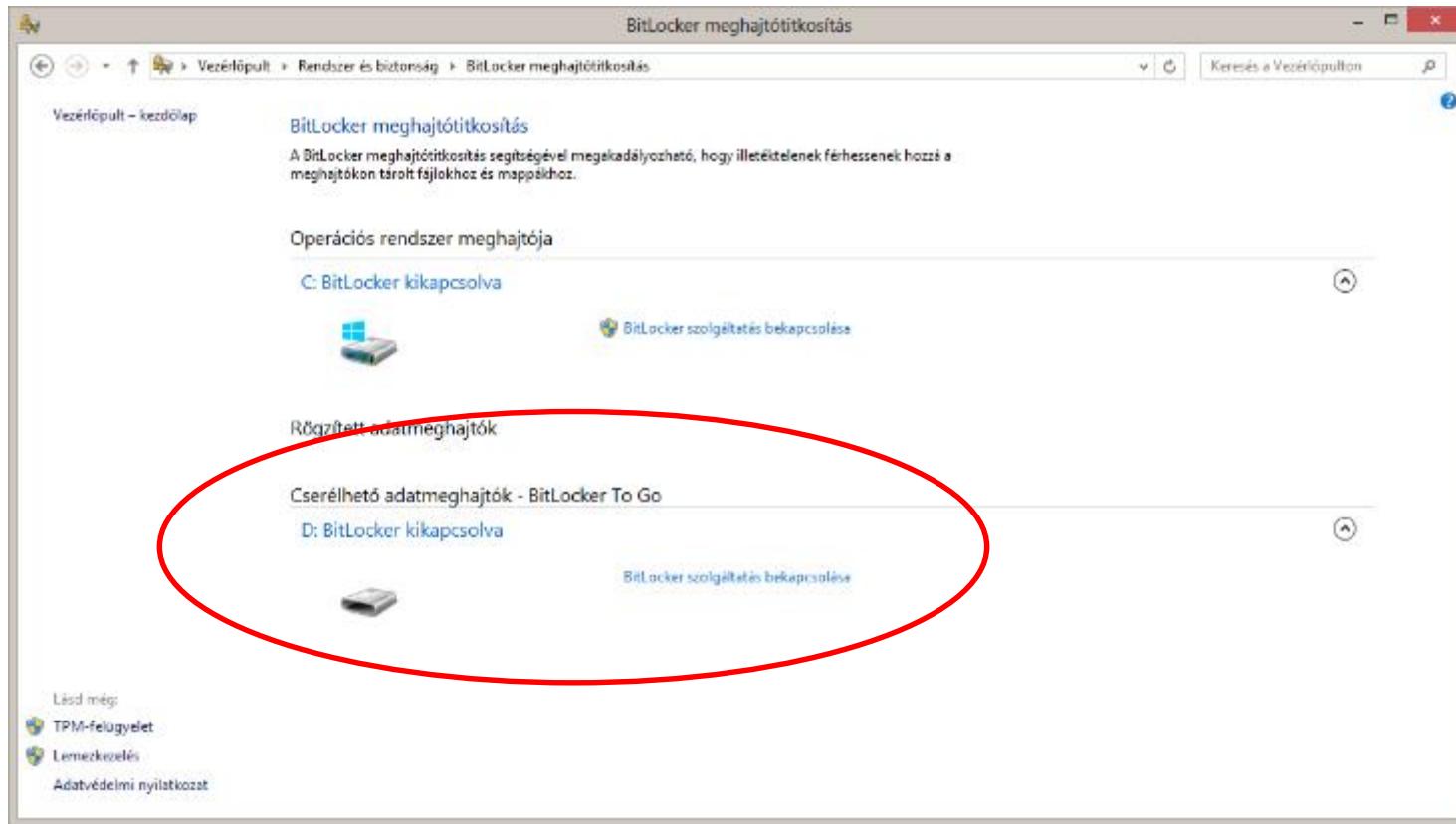
meghajtó titkosítás



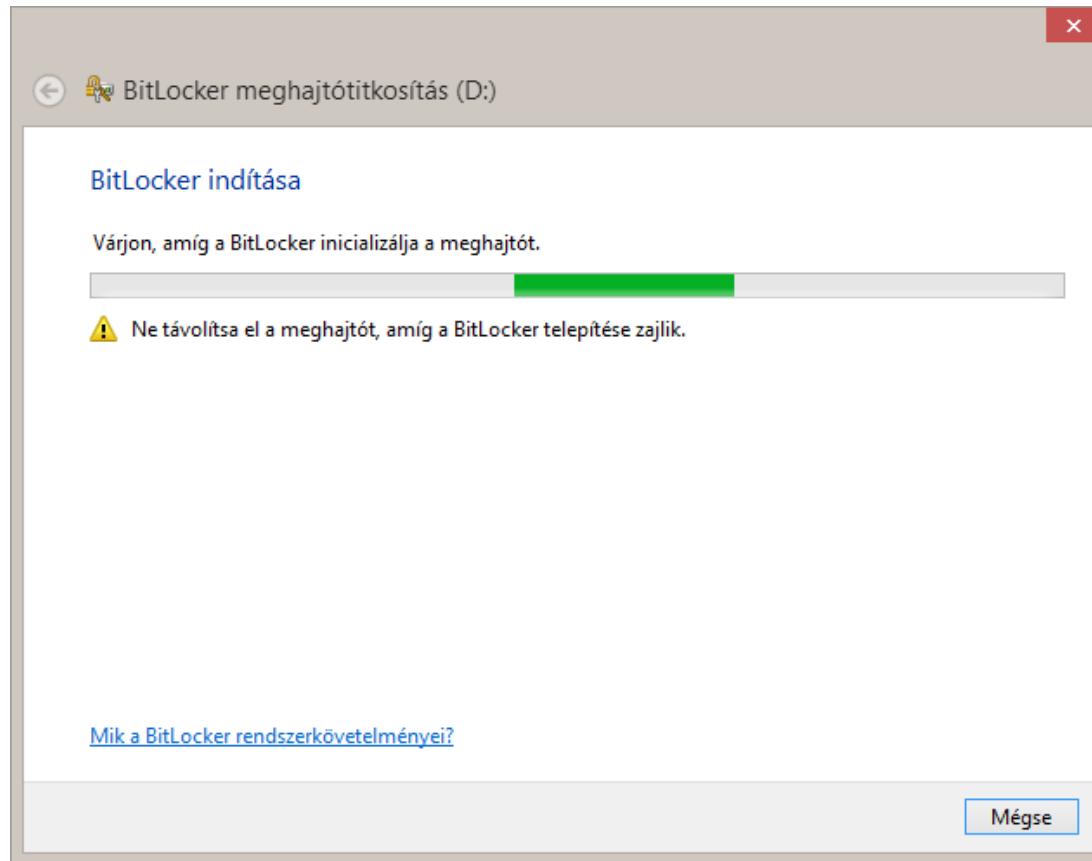
Vezérlőpult beállítás



Az operációs rendszer vagy egy cserélhető meghajtó titkosítása



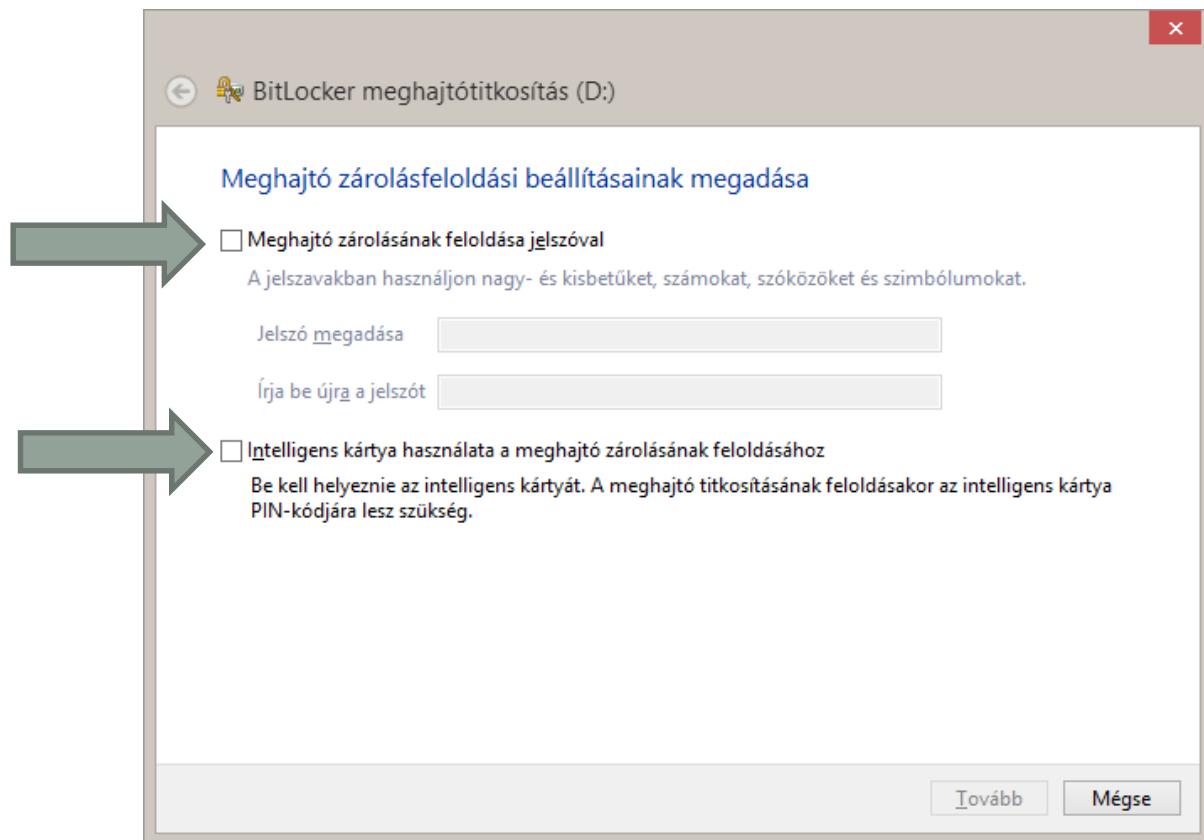
A titkosítandó meghajtó inicializálása



A titkosítás feloldása történhet

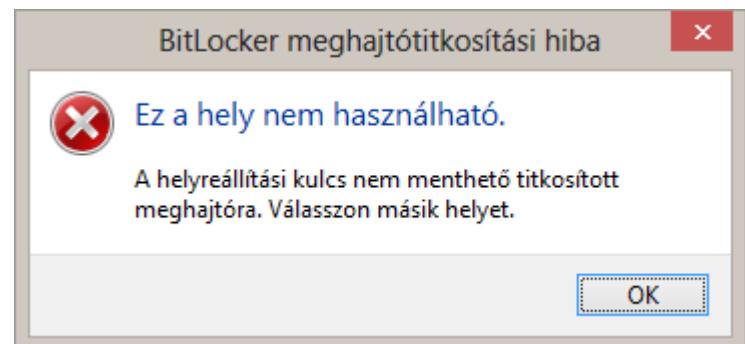
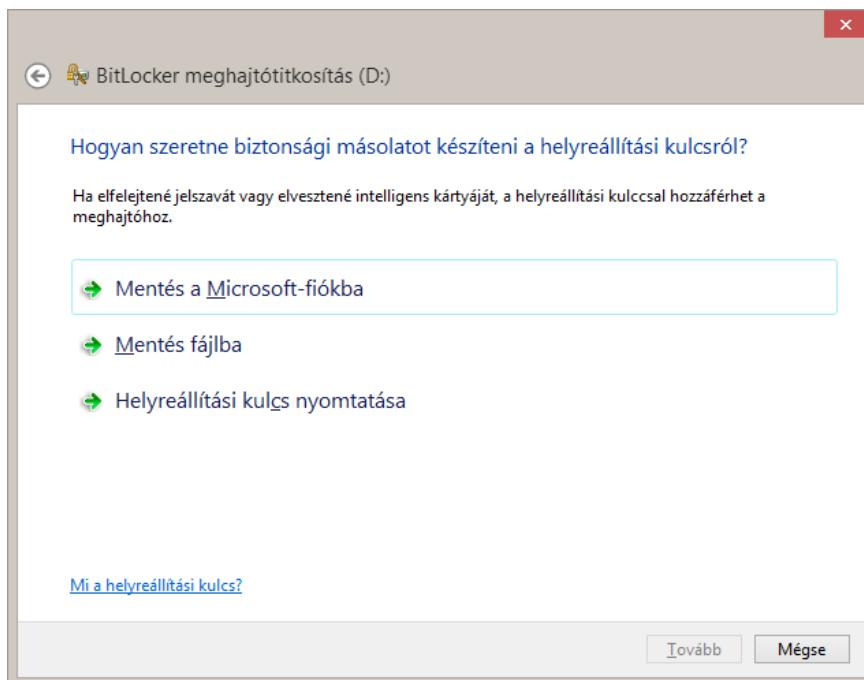
jelszóval
vagy

Intelligens kártyával

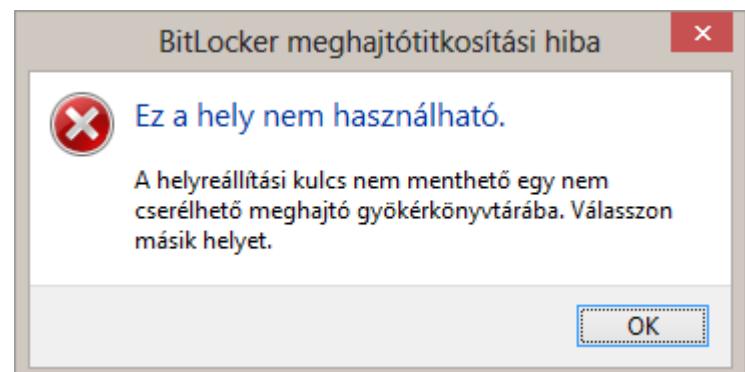


Jelszó vagy Intelligens kártya elvesztése esetén
helyreállítási kulccsal is megtörténhet a hozzáférés.

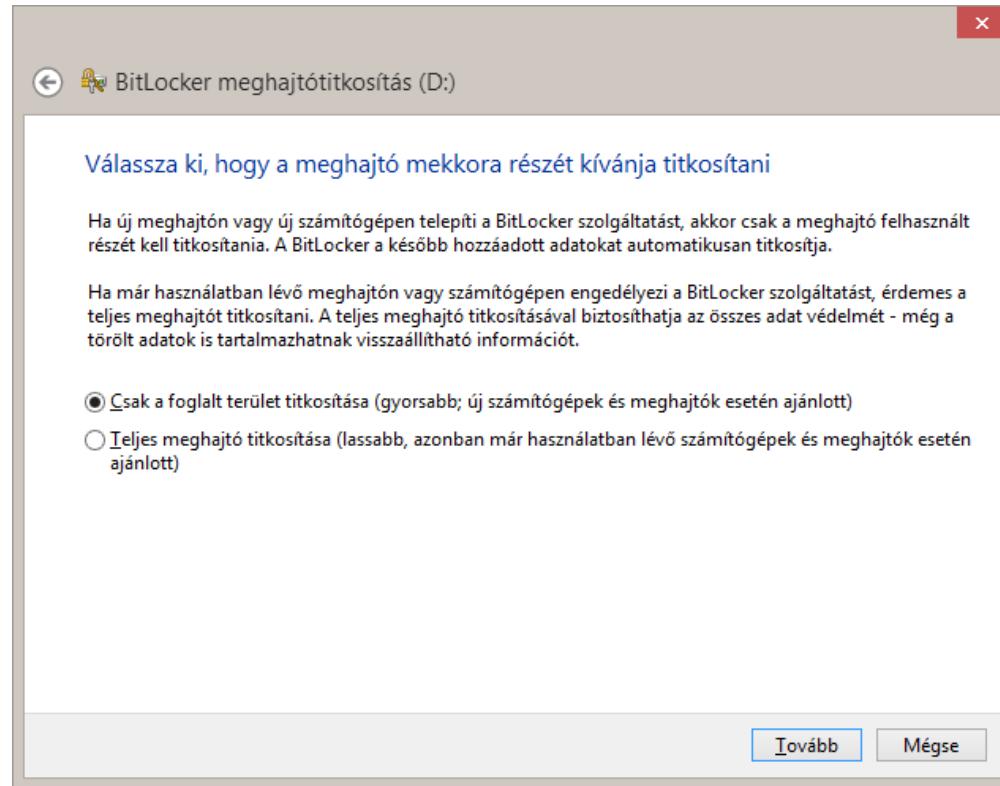
Nem menthető arra amit titkosítunk:



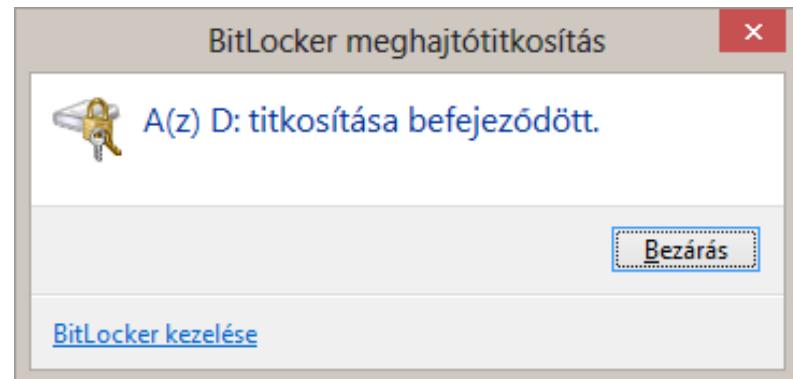
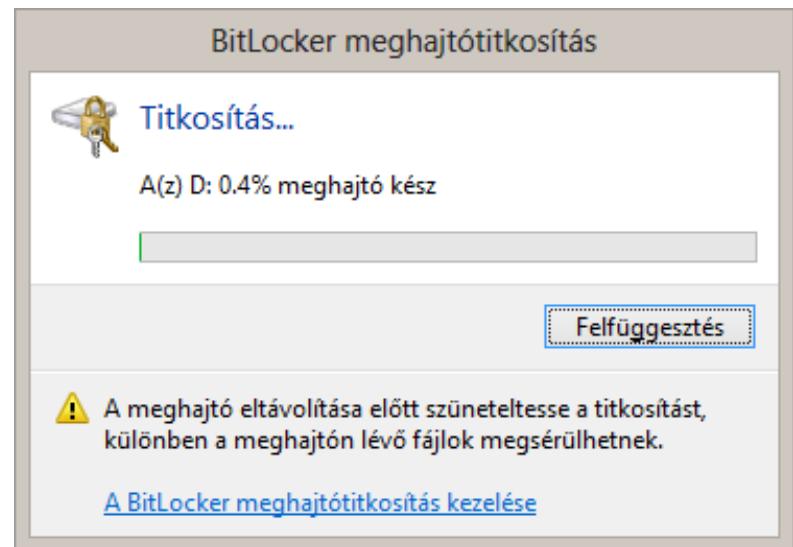
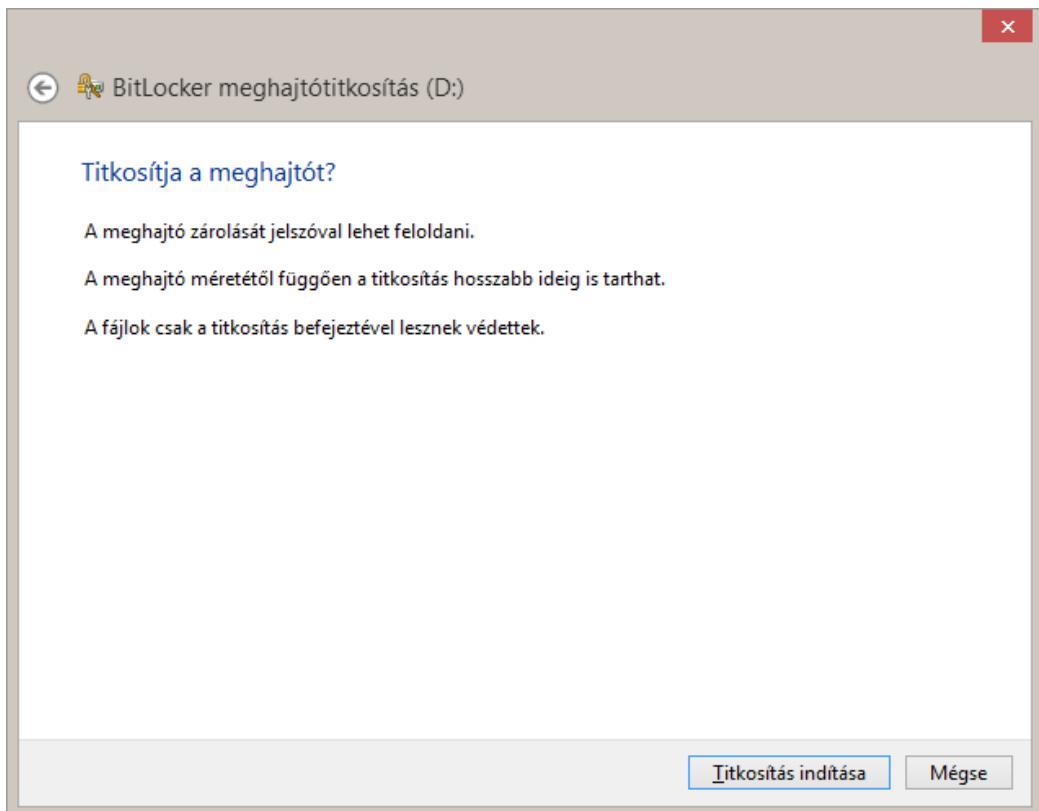
Gyökérkönyvtárba csak hordozható eszközre menthető:



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



A titkosítás indítása

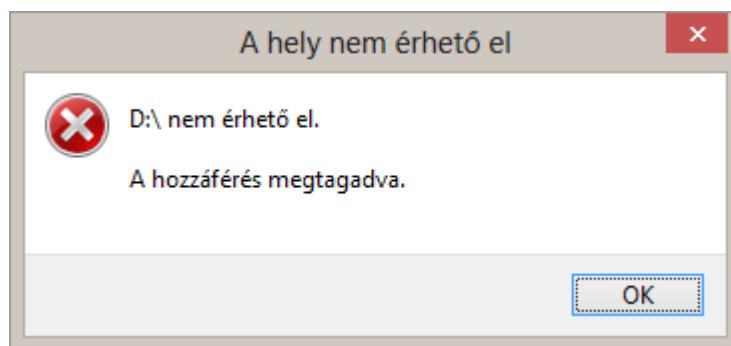


A meghajtók listájában megjelenő titkosított meghajtó jelölése:

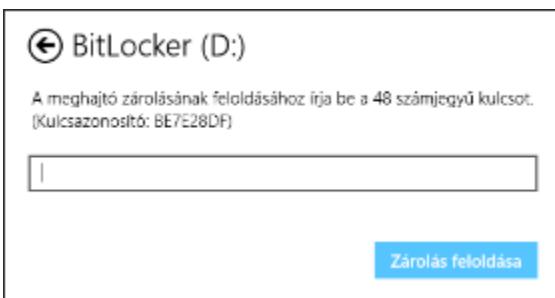
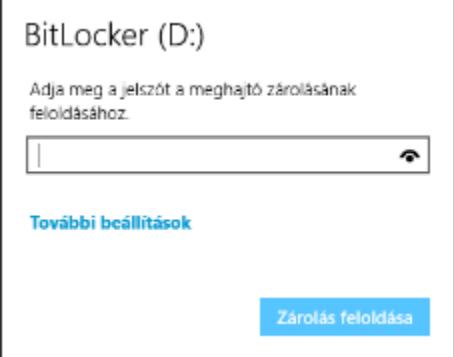
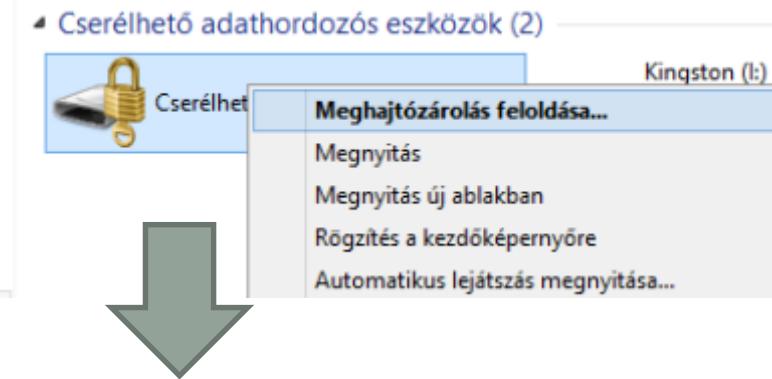
▲ Cserélhető adathordozós eszközök



Megnyitáskor **megttagadja** a hozzáférést:

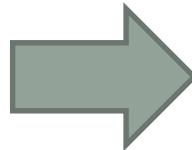


A titkosított meghajtó **megnyitása**:

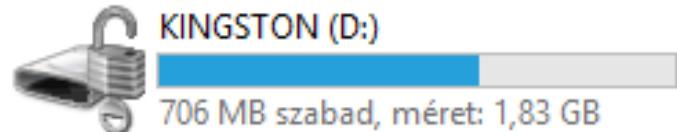


jelszóval

kulccsal



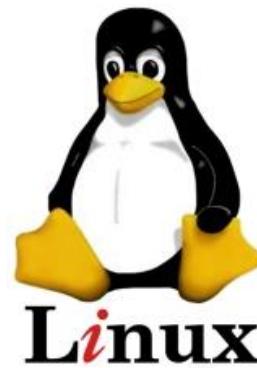
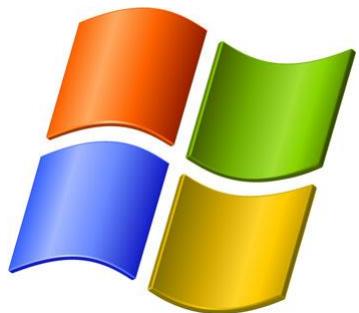
Cserélhető adathordozós eszközök (2)



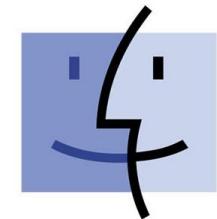


VeraCrypt

<https://veracrypt.hu/>



Linux



MacTMOs

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.

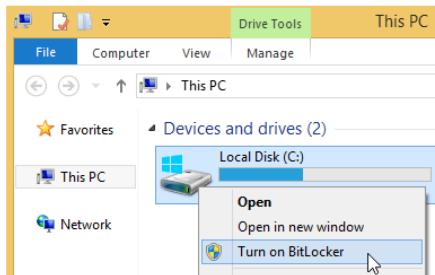
Migrating from TrueCrypt to BitLocker:

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 változat 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 sebességen ugyan némi csökkenést eredményez, de cserébe bruteforce támadással legalább 10-szeresen (legfeljebb akár 300-szorosan is) több időbe telik a rendszer feltörése.

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 későbbieken működni.

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

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.

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

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

VeraCrypt

Volumes System Favorites Tools Settings Help

Homepage

Drive	Volume	Size	Encryption Algorithm	Type
System drive				
A:				
B:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				

Create Volume

Volume

 VeraCrypt

Never save

Mount

Help < Back Next > Cancel

The screenshot shows the main VeraCrypt application window and its internal "Volume Creation Wizard" dialog. The main window has tabs for Volumes, System, Favorites, Tools, Settings, and Help, with a "Homepage" link. It lists various drives (A:N) and includes a "Create Volume" button and a "Mount" button. The "Volume Creation Wizard" dialog is open, featuring a stylized graphic of a shield or vault door. It displays three options: "Create an encrypted file container" (selected), "Encrypt a non-system partition/drive", and "Encrypt the system partition or entire system drive". Each option has a brief description and a "More information" link.

VeraCrypt Volume Creation Wizard

Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

[More information](#)

Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

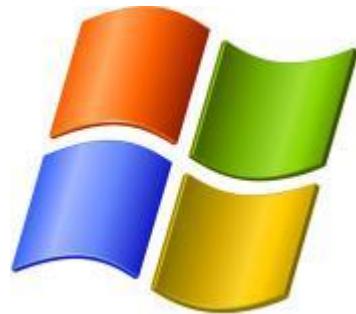
[More information about system encryption](#)

Help < Back Next > Cancel

This is a screenshot of the VeraCrypt Volume Creation Wizard. The title bar says "VeraCrypt Volume Creation Wizard". The main content area has three radio button options: "Create an encrypted file container" (selected), "Encrypt a non-system partition/drive", and "Encrypt the system partition or entire system drive". Each option has a brief description and a "More information" link. The "Create an encrypted file container" section is highlighted with a blue border. The VeraCrypt logo is visible at the bottom left of the wizard window.

EFS

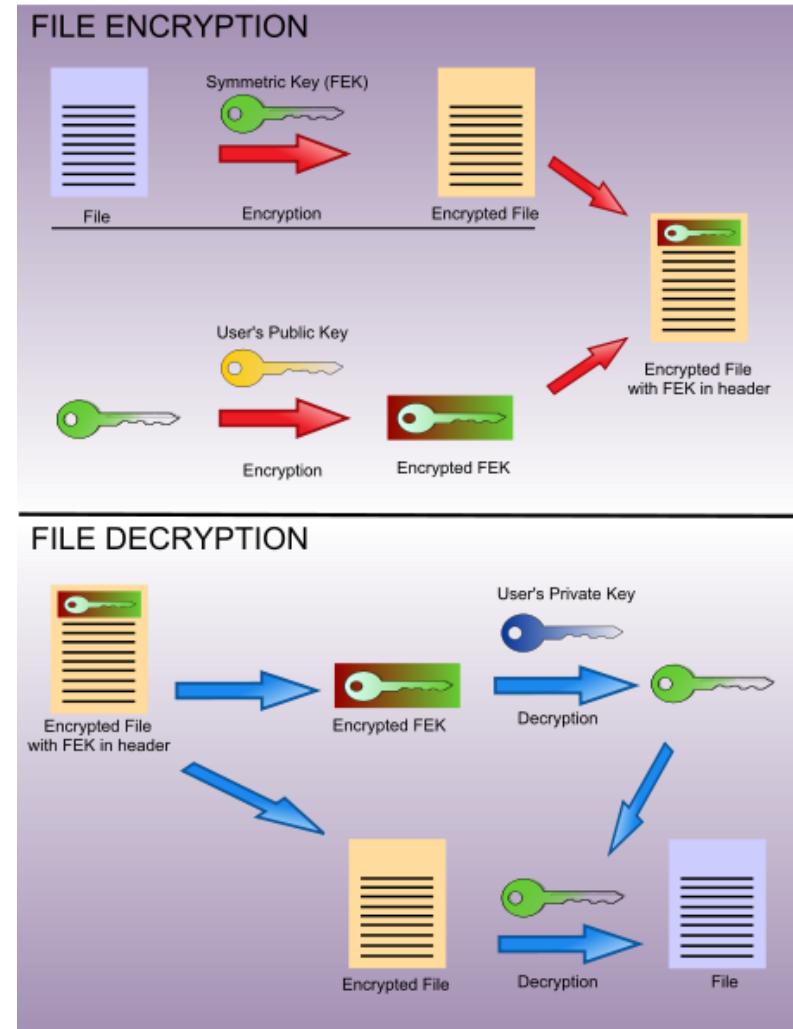
fájltitkosítás

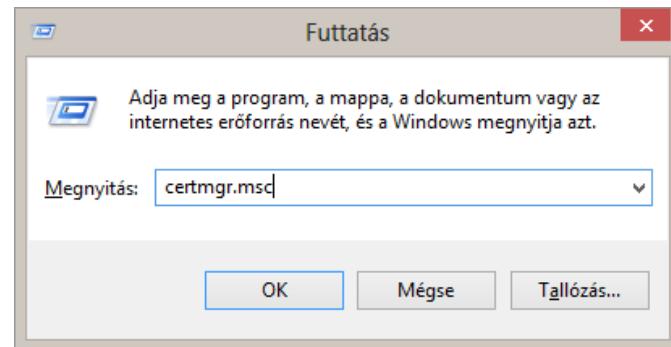


EFS (Encrypting File System)

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

NTFS fájlrendszer !!!





certmgr - [Tanúsítványok - aktuális felhasználó\Személyes]

Ejel Müvelet Nézet Súgó

The toolbar icons are circled in red.

Tanúsítványok - aktuális felhasználó

Személyes

- ▷ Megbízható legfelső szintű hitelesítésszolgáltatók
- ▷ Vállalati szintű megbízhatóság
- ▷ Közbenső szintű hitelesítésszolgáltatók
- ▷ Active Directory - felhasználóobjektum
- ▷ Megbízható gyártók
- ▷ Nem megbízható tanúsítványok

Objektumtípus

Ebben a nézetben nincsenek megjelenítendő objektumok.

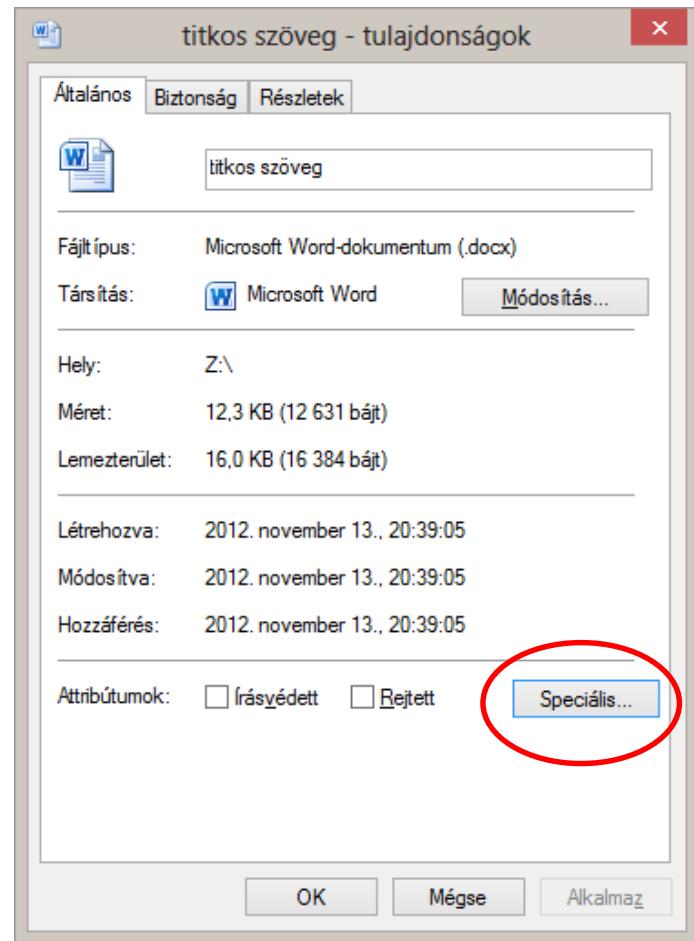


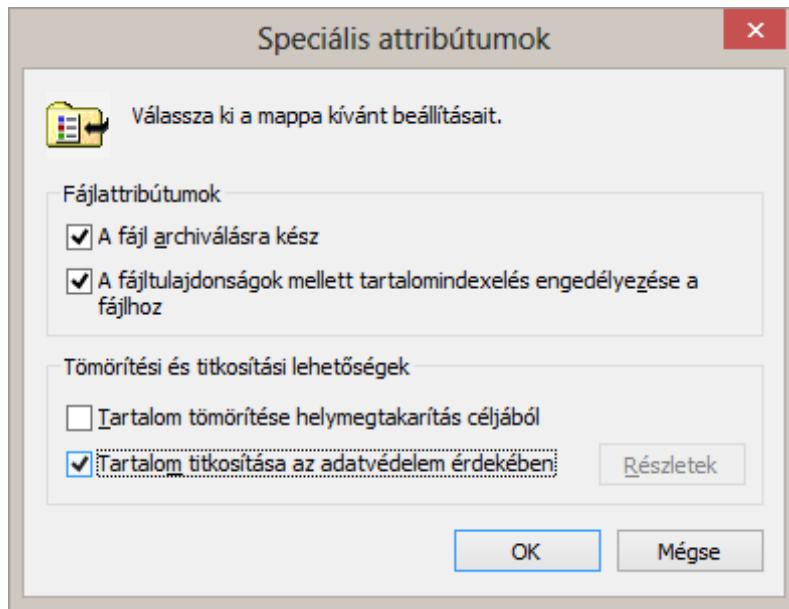
titkos
szöveg

AMD VISION Engine Control Center

- Nézet
- Rendezés
- Csoportosítás
- Frissítés
- Mappa testreszabása...
- Beillesztés
- Parancsikon beillesztése
- Megosztás ezzel
- Megosztott mappa szinkronizálása**
- Új

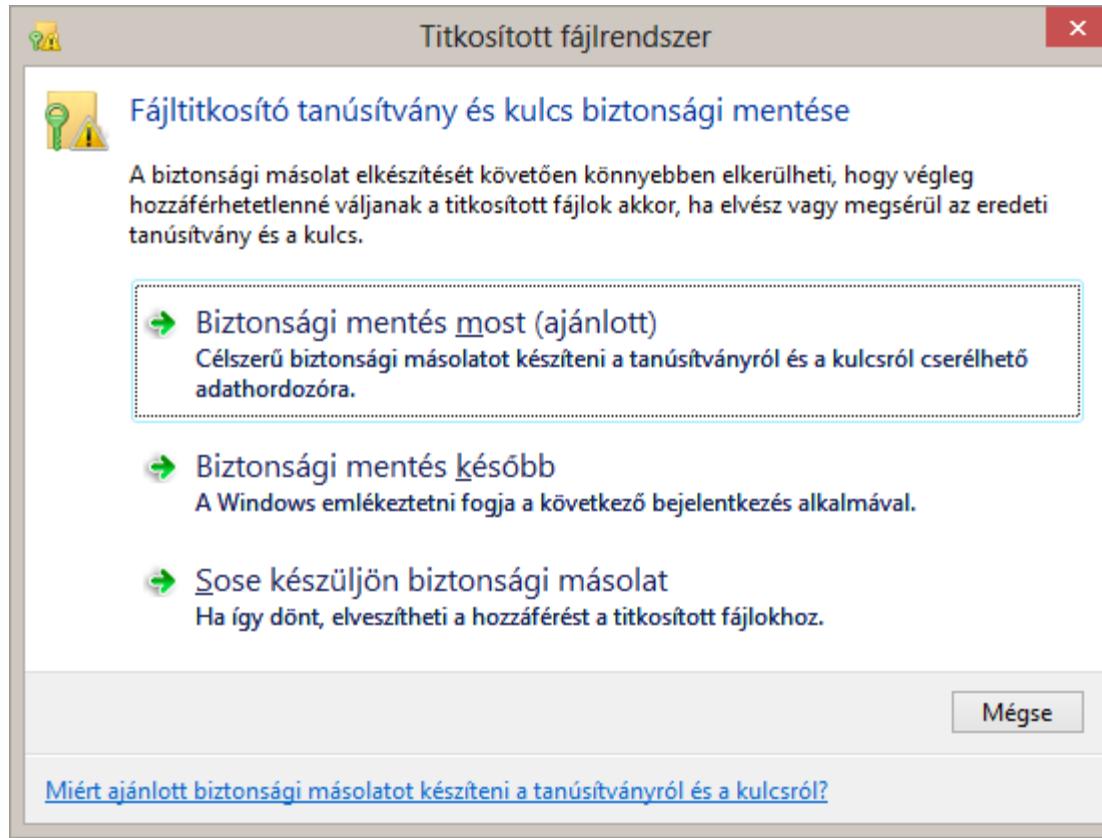
Tulajdonságok

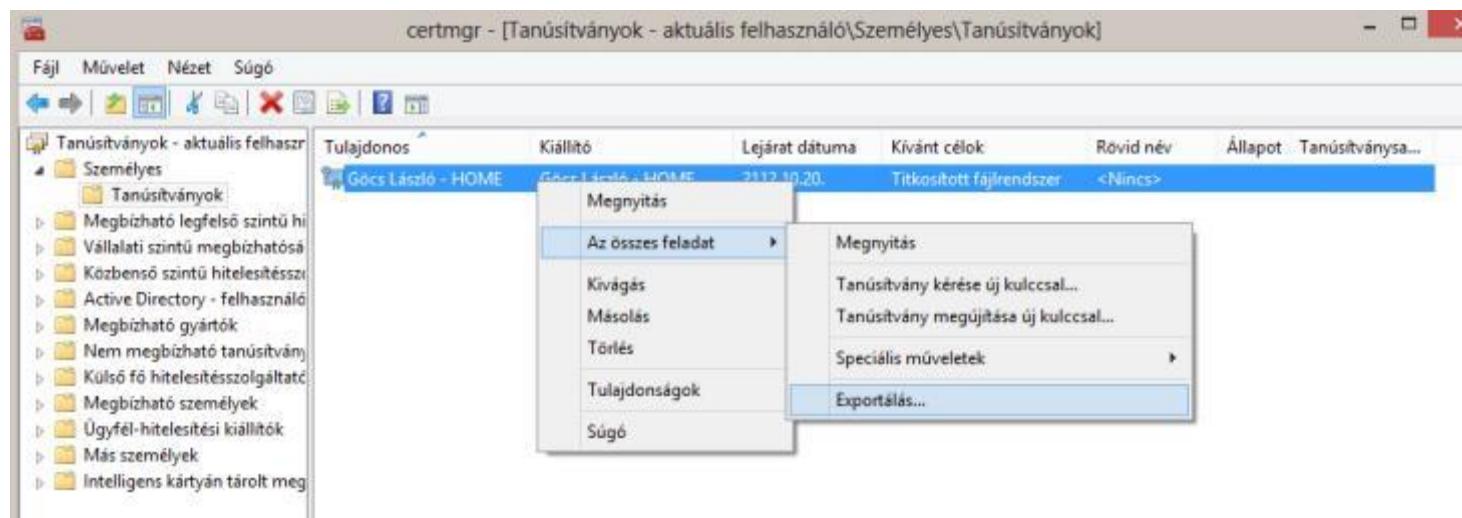
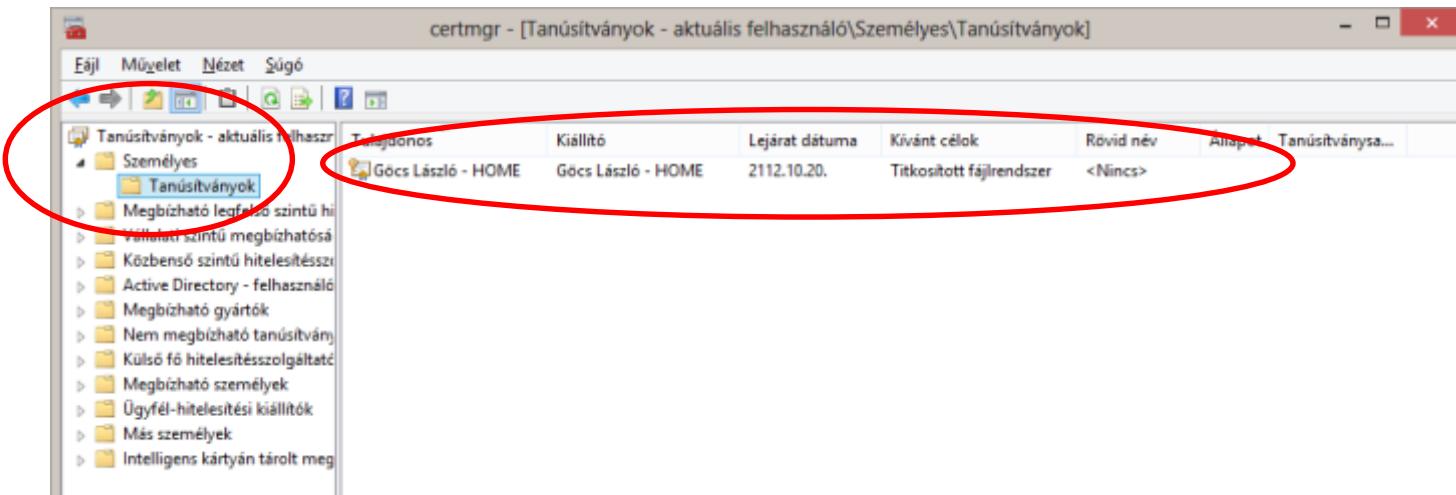


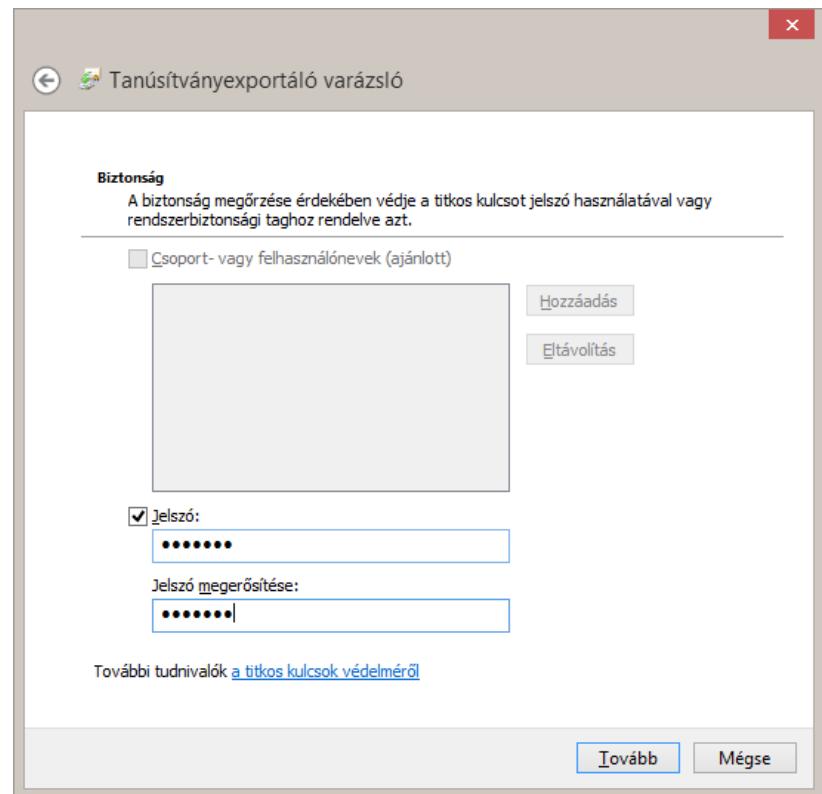
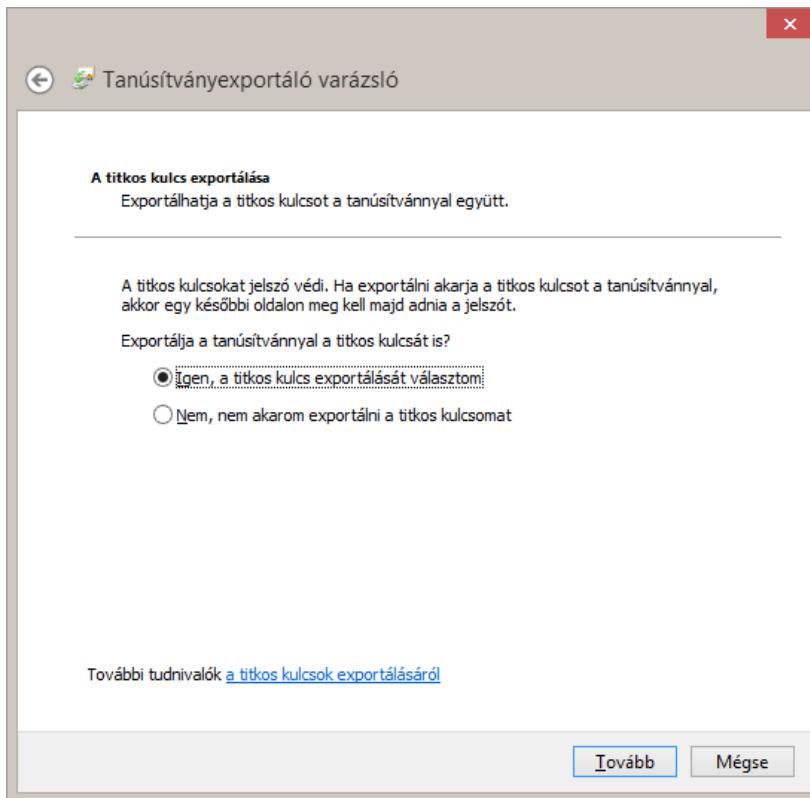


titkos
szöveg









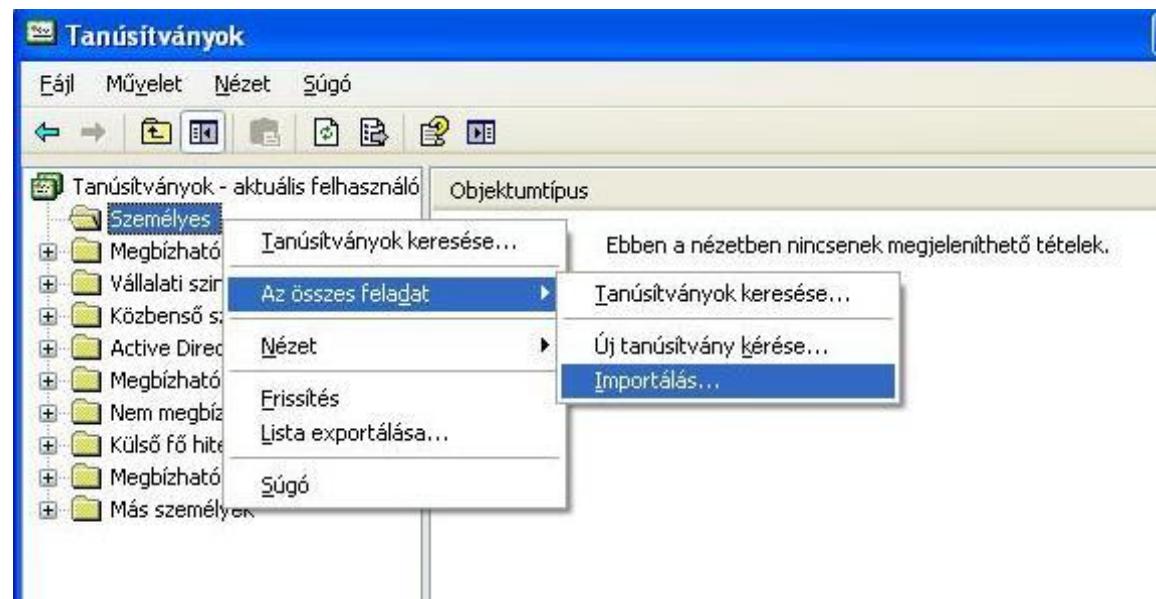
Microsoft Office Word



A Word nem tudja megnyitni a dokumentumot, mert a felhasználónak nincs hozzáférési jogja
(H:\titkos\titkos szöveg.docx)

[Súgó megjelenítése >>](#)

OK



Tanúsítványimportáló varázsló



Importálandó fájl

Adja meg az importálandó fájlt.

Fájlnév:

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

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

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

Microsoft sserializált tanúsítványtároló (.SST)

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

Tanúsítványok

Fájl Művelet Nézet Súgó

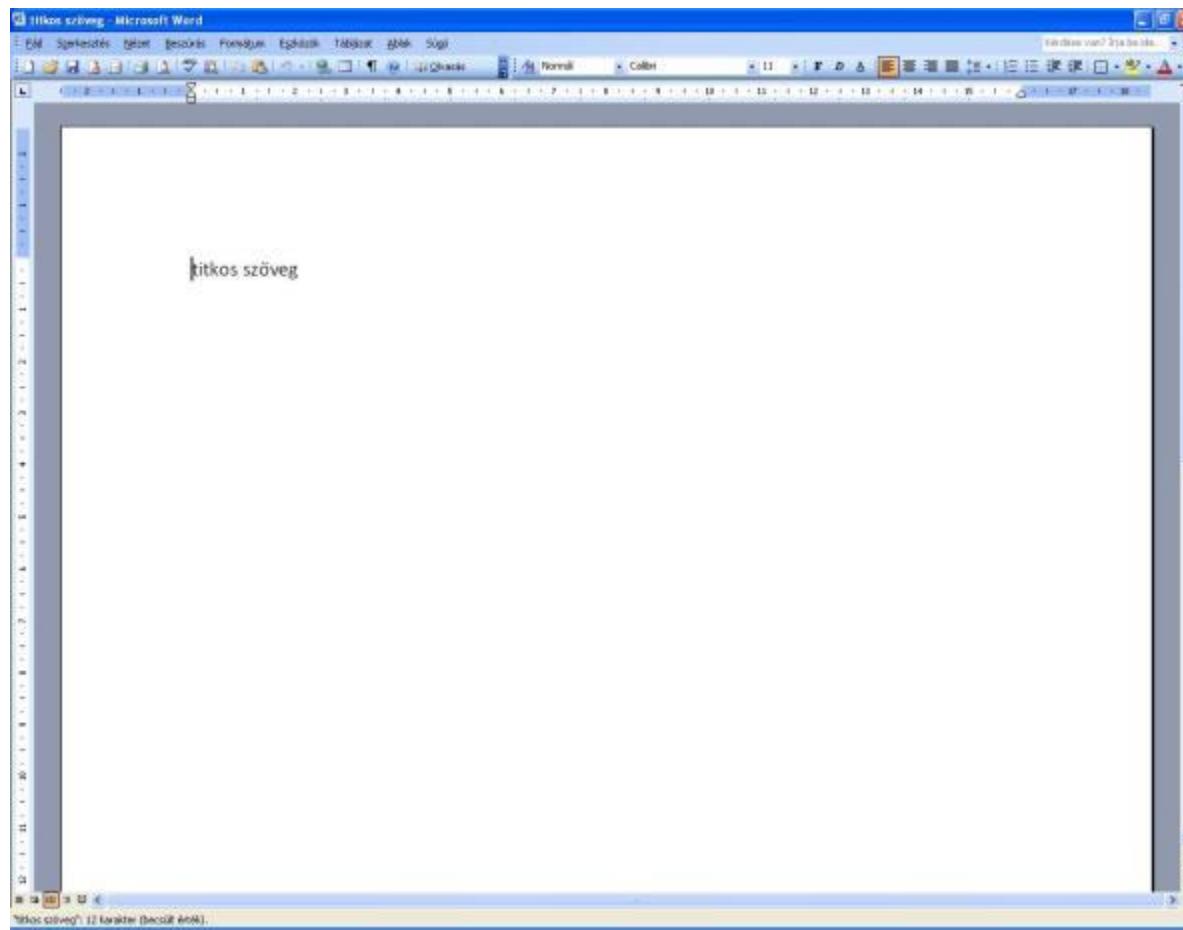
Tanúsítványok - aktuális felhasználó

Személyes

- Tanúsítványok
- Megbízható legfelső szintű hitele
- Vállalati szintű megbízhatóság
- Közbenső szintű hitelesítésszolg.
- Active Directory - felhasználók
- Megbízható gyártók
- Nem megbízható tanúsítványok
- Külső Fő hitelesítésszolgáltatók
- Megbízható személyek
- Más személyek

Tulajdonos	Kiállító	Lejárat dátuma	Kívánt célok	Rövi...	Állapot
Göcs László - GAMF	Göcs László - G...	2112.10.13.	Fájrendszer titkosítása	<Nincs...	

A tárolóban (Személyes) 1 tanúsítvány van.



Az emberi tényező az IT biztonságban



Az ember szerepe az IT biztonságban

Az információbiztonság sokszor
elfelejtett tényezője az ember, vagyis a

- vállalat munkatársai,
- partnereinek alkalmazottjai,
- beszállítói,
- ügyfelei,
- egyéb látogatói.

Az ember szerepe az IT biztonságban

A védendő értékre **közvetlen hatással van**, hiszen a vállalat alkalmazottjai

- kezelik a számítógépeket,
- futtatják a programokat és
- dolgoznak a cég adataival.

Az ember szerepe az IT biztonságban

Az informatikai jellegű meghibásodások, károk oka majdnem 60%-ban valamilyen **emberi mulasztás** következménye.

Gyakori veszélyforrás az **emberi hanyagság**, a munkatársak figyelmetlensége.

A felhasználók nincsenek tisztában azzal, hogy az őrizetlenül hagyott vagy **nem megfelelően kezelt** hardver eszközök, adathordozók mekkora veszélyt is jelenthetnek információbiztonsági szempontból.

Az ember szerepe az IT biztonságban

- Számítógép
 - Távollétéükben jelszó nélküli adathozzáférés
 - Laptop eltulajdonítása, szervizbe adása
- Hordozható adattárolók elvesztése
 - Pendrive, memóriakártya
 - Mobiltelefon
 - CD/DVD lemez
- Eszközök leselejtezése, adatok megsemmisítése
 - Szoftveres törlés
 - Hardveres megsemmisítés

Kihasználható emberi tulajdonság

- **Segítőkészség**

Az emberek legtöbbje **szívesen segít** az arra rászorulón, különösen ha az egy munkatársnak tűnik.

- **Hiszékenység, naivság**

A munkatársak segítenek egy támadónak, mert naivan elhiszik, hogy **tényleg bajban van**, de nyugodt szívvel rendelkezésre bocsátanak bizalmas információkat olyan illetéktelen személyeknek, akik valódi munkatársnak tűnnek, holott lehet, csak ismerik az adott területen használt szakzsargont.

Kihasználható emberi tulajdonság

- **Befolyásolhatóság**

Meggyőzés, megvesztegetés, vagy akár megfélemlítés is. A munkatársak befolyásolhatóságának sikerességéhez több tényező is hozzájárulhat, ezért minden célszerű figyelmet fordítani a kiszemelt alkalmazott **munkahelyi körülményeire, életszínvonalára.**

- **Bosszúállás**

A támadók legtöbbje **belülről**, a cég munkatársai közül, vagy legalábbis a segítségükkel kerül ki. Ha az alkalmazott már különösen **negatív érzéseket** táplál munkahelye iránt, vagy esetleg éppen önként távozik vagy elbocsátják, akkor a befolyásolhatóságon túl felmerülhet a bosszúállás lehetősége is.

„Az amatőrök a rendszereket hackelik, a profik az embereket.”

Social Engineering



Pszichológiai manipuláció

Amikor egy **jogosultsággal rendelkező** felhasználó **jogosulatlan** személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít a rendszerbe történő belépéstre a másik személy **megtévesztő viselkedése** miatt.

Informatikai rendszerek biztonsága ellen indított támadások.

Social Engineering

Az emberi természet két aspektusát igyekeznek kihasználni:

- a legtöbb ember **segítőkész** és igyekszik segíteni azoknak, akik segítséget kérnek.
- az emberek általában **konfliktuskerülők**.

Social Engineering

Ha egy hacker be kíván törni egy informatikai rendszerbe, vagy egy programot akar feltörni, hibából fakadó **sebezhetőségeket** kell keresnie (pl. forráskód).

Ha az efféle hibáktól mentes az adott szoftver, más utakon kell elindulnia.

További információkat kell szereznie a rendszerrel kapcsolatban.

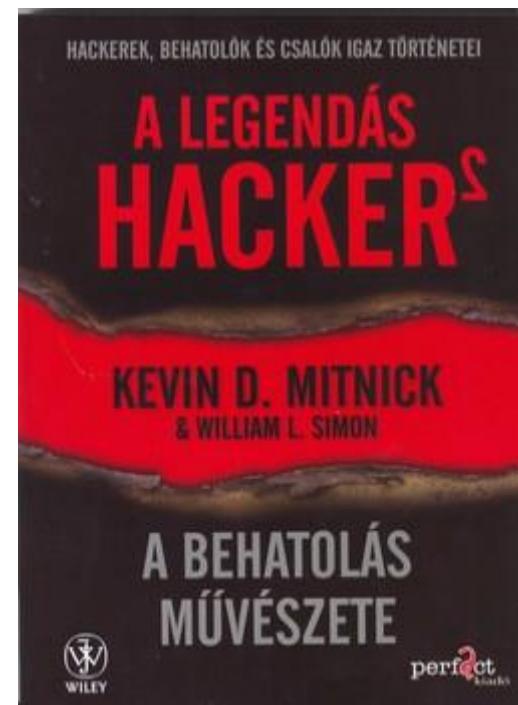
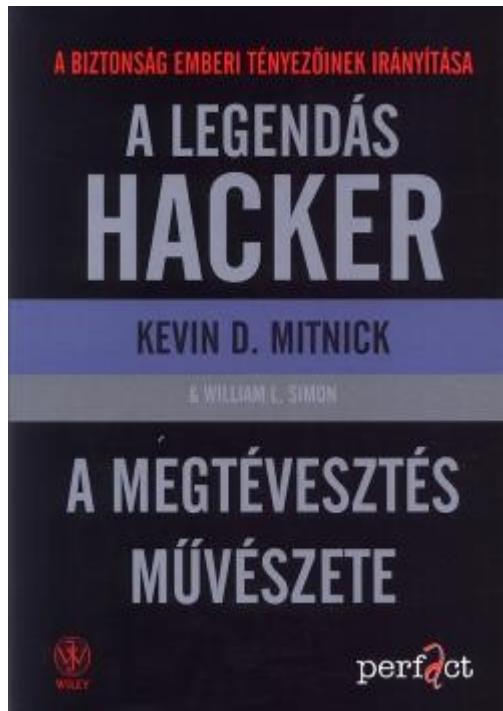
A biztonsági rendszerek mindenkor leggyengébb láncszemére, magára az **emberi tényezőre** összpontosít.

Egy social engineernek tudnia kell

- álcázni magát,
- hamis identitással mutatkozni,
- raffinált technikákkal sarokba szorítani a kiszemelt áldozatot **információszerzés** szempontjából,
- egyszóval tudnia kell hazudni.

Social Engineering

Kevin David Mitnick



Social Engineering

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”

(Kevin D. Mitnick – A megtévesztés művészete, borító)

Humán alapú social engineering

- **Segítség kérése**
 - HelpDesk átverése
 - Új alkalmazott megszemélyesítése
 - HelpDesk kér segítséget
 - Piggybacing – más jogosultságának a használata (open wifi)
- **Segítség nyújtása**
 - hibát generál, majd az illetékeseket megelőzve tűnik fel a megoldást jelentő
 - szakember szerepében.

Humán alapú social engineering

- **Valamit valamiért**
 - A social engineer azt próbálja elérni, hogy az áldozat tegyen meg neki valamilyen szívességet, jellemzően mondjon meg neki valamilyen felhasználható információt egy későbbi támadáshoz.
- **Fontos ember megszemélyesítése**
 - A támadó a főnököt megszemélyesítve garantáltan megkap minden kért információt.
- **Felhatalmazás**
 - Ha a támadó a főnököt nem tudja megszemélyesíteni, mert például a kiszemelt kolléga ismeri valamennyire.

Humán alapú social engineering

- **Reverse Social Engineering**

- a social engineer olyan kérdéseket tettet fel magának, amelyekben benne vannak a számára szükséges információk.

- **Dumpster Diving – kukaátvizsgálás**

- Szemetesbe kerülhetnek a monitorról leszedett jelszavas címkék, másrészt az alkalmazott olyan személyes adatai, amelyek segítséget nyújthatnak az illető személyazonosságának felvételéhez.

Humán alapú social engineering

- **Shoulder Surfing – „váll szörf”**
 - valamilyen módon az áldozat közelébe kell férkőzni, ami történhet konkrét céllal, úgy hogy nem kell semmi hazugságot kitalálni (például ügyfélként) vagy valamilyen más social engineering módszerrel kombinálva.valaki mást megszemélyesítve.
- **Tailgating – szoros követés**
 - támadó úgy tesz, mintha egy vendég- vagy munkás csoport tagja lenne, majd hozzájuk csapódva egyszerűen besurran az épületbe és ott szabadon járkálva kutathat az információk után.

Számítógép alapú social engineering

- **Ál weboldalak**
 - Regisztráció ellenében kínálunk valamilyen ingyenes tartalmat, vagy sorsolunk ki valamilyen nyereményt. A felhasználók legtöbbje ugyanis több helyen is ugyanazt a karakterszorozatot használja, vagy valamilyen nagyon hasonlatosat.
- **Phishing – adathalászat**
 - Hamis e-mailek és weboldalak

1. figyelem felkeltés, megtévesztés

2. Az adatlopás felülete – egy álweboldal

The screenshot shows a login form for a fake Facebook page. The header reads 'facebook Regisztráció'. The main title is 'Facebook-belépés'. A red box highlights a message: 'Ki lettéi léptetve, kérjük jelentkezz be újra! Az általad megtekintett hivatkozás nem biztonságos ezért rendszerünk automatikusan kiléptetett. Elfelejtette a jelszavadat? Új jelszó igénylése.' Below this is an input field for 'E-mail vagy telefon:' and a password field for 'Jelszó:'. There is a checkbox for 'Bejelentkezve maradok'. At the bottom are buttons for 'Bejelentkezés' and 'Regisztráció a Facebookra!', and a link for 'Elfelejtette a jelszavadat?'. The footer includes language links: Magyar, English (US), Deutsch, Français (France), Italiano, Русский, Español, Română, Português (Brasil), and Arabic (...).

Regisztráció Bejelentkezés Messenger Facebook Lite Mobil Ismerősök keresése Névjegyek Emberek Oldalak Helyek
Játékok Helyek Rólunk Hirdetés létrehozása Oldal létrehozása Fejlesztő Álláslehetőség Adatvédelem Súlik AdChoices
Feltételek Helyek Sugó

Facebook © 2015
Magyar

Számítógép alapú social engineering

- **Phishing – adathalászat**

- Smishing - pénzintézetnél az utalás elengedhetetlen feltétele az SMS-ben érkező jelszó begépelése.
- Hamis bannerek, reklámok

- **Pharming**

Nem a felhasználót, hanem a DNS-szerverek sebezhetőségeit és a böngészőprogramok befoltozatlan biztonsági réseit kihasználva az adott weboldal tényleges címét módosítják az alábbi módszerek valamelyikével.

BIZTONSÁGOS BÖNGÉSZÉS

- HTTPS:// böngészés



Kétfaktoros autentikáció

1. Azonosító + Jelszó

OTPdirekt belépés 

Azonosító

Számla **117** Számlaszám

Jelszó

Tranzakcionkénti azonosítás
 Azonosító, számlaszám megjegyzés

Belépés →

2. SMS

Kérjük, adja meg az alábbi adatokat!

SMS-ben kapott azonosító

Tovább

Google

Bejelentkezés

Tovább a Gmailre

E-mail-cím vagy telefonszám

Nem tudja az e-mail-címét?

További lehetőségek **KÖVETKEZŐ**

Enter the verification code sent to your phone number ending in **65**.

Enter code: **Verify**

Trust this computer
We won't ask you for a code again when we recognize one of your trusted computers. [Learn more](#)



Elektronikus levelezés veszélyei

- Kéretlen levelek, reklámok
- Megtévesztő információk
- Adatkérés -> adatlopás
- Veszélyes mellékletek (vírus, kémprogram)

Kéretlen levél /spam/ - Kéretlen levél minden olyan elektronikus levél, amelyet a címzett nem kért. Leggyakoribb előfordulási formája a kéretlen reklám. Az ilyen küldemény gyakran még kéretlen betolakodót (vírust) is hordoz. A levél feladója, tárgya és szövege olyan gyakran változik, hogy ezen **levelek szűrése, egyszerű minta alapján nem lehetséges.**

Beugrató levél /hoax/ - Hamis levélriasztás, mely az emberek jóhiszeműségére építve, hatalmas levélforgalmat generál, ezzel a **levelező rendszereket lassíthat, vagy béníthat meg.** Kártékony programot nem tartalmaz, ha tartalmaz, akkor már vírusnak /malware/ hívják.

Támadás jelei, formái

- A feladó neve, és maga az email cím valódisága
 - Komoly megrendelés -> telefon
- Hivatalos levél nem jön @gmail.com, @freemail.hu stb címről
- Mellékletek

Megtévesztő feladó, veszélyes melléklet

Kijelölés Témák Üzenetek: 1 - 5 / 5

Attached: 9B1016A5BC22D3

Feladó gocs.laszlo@gamf.kefo.hu +
Címzett gocs.laszlo@gamf.kefo.hu +
Dátum 2016-07-15 12:42

ZIP 9B1016A5BC22D3.zip

Adathalászat

 **Dear Account User**

Feladó Admin 

Címzett Recipients 

Dátum 2016-07-14 13:15

Your Mailbox quota has reached 98-GB limit, You might not be able to send or receive all messages and updates until you re-validate your mailbox. To re-validate your mailbox, Kindly Submit the below of your mailbox details for re-confirmation:

{user-name :
{Password :
{Confirm Password :

Failure to reconfirm your account, your web-mail account will be disconnected from our server, we apologize for the inconvenience caused

Best Service
Web-mail Team

Magyar változatban (Telekom logo)

We've Disabled Your Account Access □ Spam x



Apple Support <no-reply@server2.sashianceit.com>

clíenzeti saját magam ▾



Miért van ez ez üzenet a Spam mappában? Az üzenet hasonló a spamszűrőink által korábban észlelt üzenetekhez. További információ



angol ▾

> magyar ▾

Üzenet lefordítása

Update Your Information Within 48 Hours.

Dear Customer,

We have changed our policy terms, so we need from you to confirm your ID Apple and accept our new terms. **Policy Update**. To learn more about what's been changed, simply [Log in](#) to your ID Apple and click on policy updates under the notifications section.

[Update Your ID Apple](#)

Sincerely,
Apple Support



<http://rossignol.kiev.ua/skin/test.php>

Veszélyes melléklet

- **Keylogger**

- minden billentyűzet leütést rögzít, továbbít emailre
- Kategóriákba szedi (böngésző, gépelés, programok indítása...)
- Már nem csak **exe** fájtként hanem **jpg** fájlban is terjed



Számítógép alapú social engineering

- **Keyloggerek**

Olyan billentyűzetnaplózó programok, amelyek a felhasználó által begépelt karaktereket naplózzák, majd elküldik a támadónak.

- Szoftveres
- Hardveres



2012. évi C törvény XLIII. Fejezet

422. § (1) ...

d) elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon **tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti**, bűntett miatt **három évig** terjedő szabadságvesztéssel büntetendő.

424. § (1)...

a) **jelszót** vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, **megszerez**, vagy forgalomba hoz

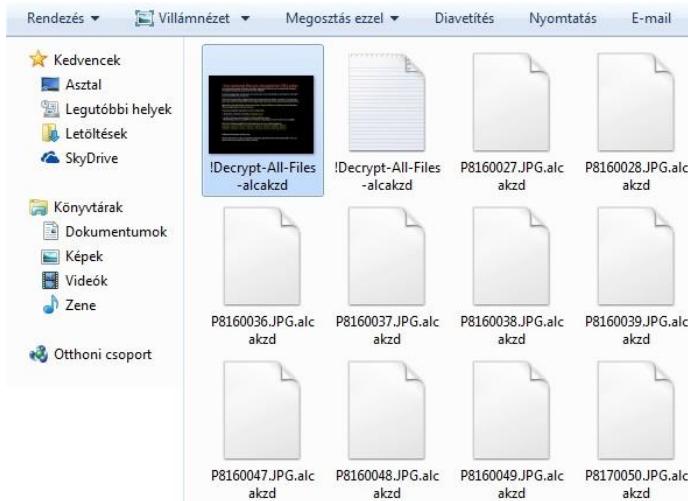
...

vétség miatt **két évig** terjedő szabadságvesztéssel büntetendő.

Fájlok ellen irányuló támadás

- Helyi számítógépen: Vírus által törlődnek vagy kódolva lesznek
- Felhő alapú tárolásnál: adathalászat következtében -> hozzáférés
- Elhagyott adathordozó

CryptoLocker támadás



		Fajlmappa	
Asztal	tételek	2015.02.05. 19:13	
Legutóbbi helyek	e_tortma_14maj_ut.PDF.alcakzd	2014.07.10. 6:33	ALCAKZD fájl
Letöltések	feladat sor 1 jav kulcs.PDF.alcakzd	2014.07.10. 6:27	ALCAKZD fájl
SkyDrive	feladatsor 1.PDF.alcakzd	2014.07.10. 6:26	ALCAKZD fájl
Könyvtárak	feladatsor 2 javító kulcs.PDF.alcakzd	2014.07.10. 6:36	ALCAKZD fájl
Dokumentumok	feladatsor 2.PDF.alcakzd	2014.07.10. 6:33	ALCAKZD fájl
	tortenelem_vk.PDF.alcakzd	2014.07.10. 6:23	ALCAKZD fájl
			177 KB

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Otherwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open <http://fizxfsi3cad3kn7v.onion.cab> or <http://fizxfsi3cad3kn7v.tor2web.org> in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1. Download Tor Browser from <http://torproject.org>
2. In the Tor Browser open the <http://fizxfsi3cad3kn7v.onion/>. Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable.

Copy and paste the following public key in the input form on server. Avoid missprints.
JG4ZBMAJ-R72YVDJ-WIDYVXP-MLN4TDTI-KETQJ6-H2WYKWC-KSQHQME-ANEATA5
MNMQFEN-CB4XK6M-25HCF24-E3ADUIK-5BW7JUK-4TUNYDH-J2WLTAQ-RHS3O14
SVQWCKN-5RB6PWQ-C2H5O27-VXL5RN3-IC5QLH2-OO2ZDVX-DTEKOEW-NSPCK4S

Follow the instructions on the server.

<https://www.youtube.com/watch?v=Gz2kmmsMpMI>

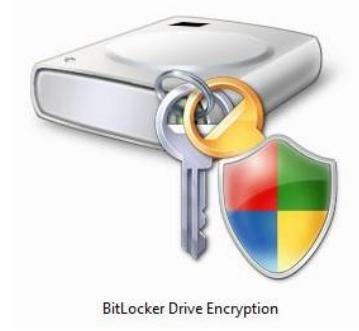
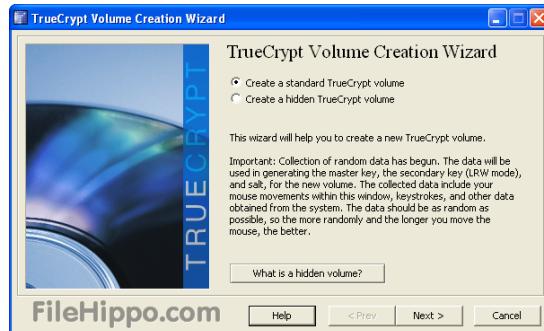
ADATMENTÉS KÜLSŐ TÁROLÓRA!

- Fontos adatainkat, munkáinkat időközönként mentsük külső adathordozóra, amit csak az adatmentéskor csatlakoztassunk a géünkhez.



TITKOSÍTÁS

- Az adathordozót, partíciót, teljes merevlemezt titkosítani.



Számítógép alapú social engineering

- **Pharming**

- Szerver alapú DNS Poisioning
 - DNS szerver támadás – a letárolt URL mellé saját IP
- Cross-Site Scripting (XSS)
 - Idegen parancsok végrehajtása – valód weblap kódjába való betörés

- **Trójai programok**

- Letöltő oldalakról
- Email mellékeletek
- Road Apple (direkt elveszít egy adathordozót)

Támadások felépítése

- Információ szerzés
- Kapcsolat kiépítése
- Kapcsolat kihasználása
- Támadás végrehajtása

Védekezés

- **Sebezhetőségek feltérképezése**

Alkalmazott megoldások, eljárások időnkénti ellenőrzése, felülvizsgálata, hogy ezáltal fény derüljön az újonnan keletkezett vagy eddig figyelmen kívül hagyott sebezhetőségekre.

- **Audit, felülvizsgálat**

A vállalat fizikai védelmének, az informatikai eszközök és adathordozók kezelésének, a hozzáférés-védelemnek valamint a vállalati kultúra és a felhasználók képzésének vizsgálata is

Védekezés

- **Penetration teszt**

Behatolási teszt. A behatolási teszteket információbiztonsági cégek szakértői hajtják végre, és munkájuk során csak olyan módszereket alkalmaznak, amelyeket a megrendelő kér, illetve engedélyez.

- **Audit, felülvizsgálat**

A vállalat fizikai védelmének, az informatikai eszközök és adathordozók kezelésének, a hozzáférés-védelemnek valamint a vállalati kultúra és a felhasználók képzésének vizsgálata is

Az informatikával kapcsolatos törvények



Technikai fejlődés

számítástechnikai bűnözés

Szervezett bűnözés: határon átnyúló bűnelkövetések

Nagy sebességű adatáramlás, kommunikáció, ellenőrizetlen
pénzmozgások pénzmosás

- a számítógép már **nem csak az elkövetés eszköze**, hanem egyre inkább maga a számítástechnikai rendszer, illetőleg **a benne tárolt adatok válnak a visszaélések célpontjaivá**.
- A bűncselekmények tárgya is az így megszerzett **információ** lesz.

Történelmi áttekintés

- Már a 70-es években is felmerült, hogy a **számítástechnikai szerzői jogról** is rendelkezni kellene.
- Az első tényállások **a szerzői jogok újra kiépülő büntetőjogi védelmével** voltak összefüggésben.
- Az **informatikai bűncselekmények** a magyar büntető anyagi jogban a számítástechnikai eszközök elterjedésével párhuzamosan az **1990-es évek közepén** jelentek meg.

Informatikai biztonsági károk

- 1997-ben a kár **91,5 millió forintra**
- 1999-re a kár **1,66 milliárd forintra** nőtt.
- 2000-ben a kár **1,04 milliárd** forintos kárt regisztráltak.

a felderítetlen és a nyilvánosságra nem hozott ügyekkel
együtt a teljes összeg akár az **évi 4-5 milliárd** forintot is
elérheti

2012. évi C törvény

XLIII. (43) fejezet

TILTOTT ADATSZERZÉS ÉS AZ INFORMÁCIÓS
RENDSZER ELLENI BŰNCSELEKMÉNYEK

Tiltott adatszerzés

422. § (1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

- a) más lakását, egyéb helyiséget vagy az azokhoz tartozó bekerített helyet titokban átkutatja,
 - b) más lakásában, egyéb helyiségenben vagy az azokhoz tartozó bekerített helyen történteket technikai eszköz alkalmazásával megfigyeli vagy rögzíti,
 - c) más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,
 - d) elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti,
- bűntett miatt **három évig** terjedő szabadságvesztéssel büntetendő.

Tiltott adatszerzés

(2) Az (1) bekezdés szerint büntetendő, aki fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából az (1) bekezdésben meghatározottakon kívül információt gyűjt.

(3) Az (1) bekezdés szerint büntetendő, aki az (1)-(2) bekezdésben meghatározott módon megismert személyes adatot, magántitkot, gazdasági titkot vagy üzleti titkot továbbít vagy felhasznál.

(4) A büntetés **egy évtől öt évig** terjedő szabadságvesztés, ha az (1)-(3) bekezdésben meghatározott tiltott adatszerzést

- a) hivatalos eljárás színlelésével,
- b) üzletszerűen,
- c) bűnszövetségen vagy
- d) jelentős érdeksérelmet okozva követik el.

Információs rendszer vagy adat megsértése

423. § (1) Aki

- a) információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad,
- b) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
- c) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,
vétség miatt **két évig** terjedő szabadságvesztéssel büntetendő.

Információs rendszer vagy adat megsértése

- (2) A büntetés bűntett miatt **egy évtől öt évig** terjedő szabadságvesztés, ha az (1) bekezdés b)-c) pontjában meghatározott bűncselekmény jelentős számú információs rendszert érint.
- (3) A büntetés **két évtől nyolc évig** terjedő szabadságvesztés, ha a bűncselekményt közérdekű üzem ellen követik el.
- (4) E § alkalmazásában adat: információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

Információs rendszer védelmét biztosító technikai intézkedés kijátszása

424. § (1) Aki a 375. vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő

a) jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve

b) jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétség miatt **két évig terjedő** szabadságvesztéssel büntetendő.

Információs rendszer védelmét biztosító technikai intézkedés kijátszása

(2) Nem büntethető az (1) bekezdés a) pontjában meghatározott bűncselekmény elkövetője, ha - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

(3) E § alkalmazásában jelszó: az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító.

2012. évi C. törvény

a Büntető Törvénykönyvről

Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése

385§

(1) Aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait **vagyoni hátrányt okozva megsérte**, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a szerzői jogról szóló törvény szerint a **magáncélú másolásra** tekintettel a szerzőt, illetve a kapcsolódó jogi jogosultat megillető üreshordozó díj, illetve reprográfiai díj megfizetését elmulasztja.

(reprográfiára szolgáló készülékek: fénymásoló gépek, multifunkcionális berendezések és nyomtatók)

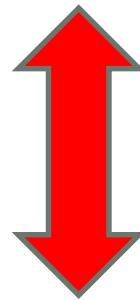
(3) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a szerzői vagy szerzői joghoz kapcsolódó jogok megsértését **nagyobb vagyoni hátrányt** okozva követik el.

(4) Ha a szerzői vagy szerzői joghoz kapcsolódó jogok megsértését

- a) **jelentős** vagyoni hátrányt okozva követik el, a büntetés bűntett miatt
egy évtől öt évig,
- b) **különösen nagy** vagyoni hátrányt okozva követik el, a büntetés **két évtől nyolc évig**,
- c) **különösen jelentős** vagyoni hátrányt okozva követik el, a büntetés
öt évtől tíz évig
terjedő szabadságvesztés.

(5) Nem valósítja meg az (1) bekezdés szerinti bűncselekményt, aki másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait többszörözéssel vagy lehívásra történő hozzáférhetővé téTELLEL sérti meg, feltéve, hogy a **cselekmény jövedelemszerzés célját közvetve sem szolgálja**.

„jövedelemszerzés célját közvetve sem szolgálja”



„lehet közvetett jövedelmet szerezni egyszerű felhasználóként is, hiszen a jog azt is jövedelemként értékeli, ha nem fizettem meg valamely egyébként megfizetendő díjat.”

„...magáncélra, tehát a jövedelemszerzést közvetve sem szolgáló letöltésekkel kapcsolatban felmerülő károkkal szembeni szerzői igényeket a **polgári jog területére szorította.”**



Védelmet biztosító műszaki intézkedés kijátszása

386 §

(1) Aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedést haszonszerzés végett megkerüli, vétség miatt két évig terjedő szabadságvesztéssel büntetendő.

(2) Az (1) bekezdés szerint büntetendő, aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedés megkerülése céljából

a) az ehhez szükséges eszközt, terméket, számítástechnikai programot, berendezést vagy felszerelést készít, előállít, átad, hozzáférhetővé tesz, vagy forgalomba hoz,

b) az ehhez szükséges vagy ezt könnyítő gazdasági, műszaki vagy szervezési ismeretet másnak a rendelkezésére bocsátja.

- (3) A büntetés bűntett miatt **három évig** terjedő szabadságvesztés, ha a **műszaki intézkedés kijátszását üzletszerűen követik el.**
- (4) Nem büntethető a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedés megkerüléséhez szükséges eszköz, termék, berendezés, felszerelés készítése vagy előállítása miatt az, aki mielőtt tevékenysége a hatóság tudomására jutott volna, azt a **hatóság előtt felfedi**, és az elkészített, illetve az előállított dolgot a **hatóságnak átadja**, és lehetővé teszi a készítésben vagy az előállításban részt vevő **más személy kilétének megállapítását**.

Az ITIL módszertan



A 80-as években új jelenséget figyelhetünk meg, a vállalatok, intézmények kezdenek **függő helyzetbe kerülni** az információtechnológiai rendszerektől, illetve az azok által biztosított szolgáltatásoktól.

A felmerült problémára adott egyik válasz angol kormányzati kezdeményezésre és támogatással született.

A **CCTA** (Central Computer and Telecommunication Agency - Központi Számítástechnikai és Távközlési Ügynökség) támogatásával elindítottak egy programot, amely egy egységes szerkezetben próbálta meg dokumentálni a jó és sikeres gyakorlatot (best practice).

Ez a dokumentáció sorozat, az IT Infrastructure Library (**ITIL**), azzal a céllal gyűjtötte össze és írta le a bevált **gyakorlati tapasztalatokat**, hogy azokat felhasználva a kormányzati területen **javítsák az informatikai infrastruktúra működtetését**.

A módszertan létrehozásának első lépése a kiválasztott **területek, folyamatok leírása** volt, ez tekinthető az **ITIL első változatának**.

A dokumentált és ajánlott gyakorlatnak létrehozták az **oktatási és vizsgáztatási rendszerét** is, melynek akkreditálásáért az ISEB (Information Systems Examination Board) lett a felelős.

Egy dokumentált módszertan, amely az összegyűjtött jó és bevált gyakorlaton alapul, **úgy működik, mint egy modell.**

Egy modell megalkotásakor a kezelhetőség érdekében **elhanyagolásokat, egyszerűsítéseket** kell végezni, amelyeket a tervezés végén figyelembe kell venni.

Az első fórum, az **IT Service Management Forum** Nagy-Britanniában jött létre 1991-ben. A Fórum tagjai rendszeres szemináriumokon és konferenciákon tették közzé az ITIL alkalmazása során szerzett tapasztalataikat. A Fórum független, csak a felhasználók által irányított szervezet, amely a gyakorlati tapasztalatok cseréje mellett az ITIL elterjedésének támogatását is célul tűzte ki

Egyre több országban alakultak helyi Fórumok, ezek összefogására létrejött az **IT Service Management Forum International**, amely a nemzeti fórumokon keresztül egyrészt segítette az ITIL terjedését, másrészt ügyelt arra, hogy az egységes maradjon.

A második nemzeti fórum Hollandiában alakult ki, ahol az EXIN informatikai oktató és vizsgaközpont lett a módszertan hivatalos gázdája

ITIL Magyarországon

Az ITIL dokumentáció először az **MTA KFKI** könyvtárában, majd a **MATÁV** informatika üzemeltetés szervezeténél jelent meg, mint szakkönyv gyűjtemény.

Később a Miniszterelnöki Hivatal támogatásával, - amely a CCTA-val jó kapcsolatokat épített ki, - az **MTA Információtechnológiai Alapítvány** munkatársainak közreműködésével 1996-ban az **Informatikai Tárcaközi Bizottság** kormányzati ajánlásként elfogadta.

Informatikai szolgáltatásmenedzsment

Az informatikai szolgáltatásmenedzsment egymással együttműködő folyamatok együttese, amelynek feladata, hogy az ügyféllel megállapodott szolgáltatási szinteken biztosítsa az informatikaszolgáltatás minőségét.

Az ITIL módszertan leírja és definiálja a kulcsfolyamatokat és egy keretet az informatikaszolgáltatás irányítására.

A szolgáltatásmenedzsment három fő célkitűzése:

- Az informatika szolgáltatását hozzá kell rendelni a jelen és jövő üzleti igényeihez és felhasználóihoz.
- Javítani kell a nyújtott informatikaszolgáltatás minőségét.
- Csökkenteni kell a szolgáltatások hosszú távú költségét

A szolgáltatásmenedzsmenthez tartozó témakörök

Szolgáltatásbiztosítás

- Szolgáltatási szint menedzsment
- Rendelkezésre állás menedzsment
- Informatikaszolgáltatás-folytonosság menedzsment
Kapacitásmenedzsment
- Informatikaszolgáltatás pénzügyi irányítása

A szolgáltatásmenedzsmenthez tartozó témakörök

Szolgáltatástámogatás

- Ügyfélszolgálat
- Incidensmenedzsment
- Problémamenedzsment
- Változáskezelés
- Konfigurációkezelés
- Kiadáskezelés

Szolgáltatásbiztosítás

Szolgáltatási szint menedzsment

A szolgáltatási szint menedzsment az a folyamat, amely a szolgáltatási megállapodásban (SLA) dokumentált célokkal az ügyfélnek nyújtott szolgáltatások szintjeit meghatározza, egyezteti, meg- állapodik róluk, majd implementálja, figyeli, folyamatosan értékeli és menedzseli azokat.

Rendelkezésre állás menedzsmentje

Ez az informatikaszolgáltatás tervezési, implementálási és irányítási folyamataiból áll a rendszerek elérhetőségének magas szintjét biztosítandó, hogy kielégíthetőek legyenek a szervezet üzleti igényei.

Az informatikaszolgáltatás folytonosságának menedzsmentje

Az informatikaszolgáltatás-folytonosság kifejezést abban az értelemben használjuk, mint az üzletmenet-folytonosság tervezésének az informatikára vonatkozó részét. Tartalmazza a katasztrófa elhárítás és az informatika előre nem látható helyreállítási tevékenységeit. Ezek a folyamatok határozzák meg a kockázatokat és a katasztrófákkal szembeni sérülékenységet, és megfelelő intézkedéseket foganatosítanak az üzletmenet folytonosságának biztosítására.

Kapacitásmenedzsment

Ez biztosítja, hogy a szervezet mindenkor megfelelő informatikai kapacitással rendelkezzen, ugyanakkor minimális legyen a túlterhelés, illetve az alacsony kihasználtság. A nem kielégítő kapacitás rendszerint teljesítményproblémákat okoz, míg a fölösleges megdrágítja a szolgáltatás költségeit. A fő területei az üzleti, a szolgáltatási és infrastruktúra kapacitáskezelés.

Az informatikaszolgáltatás pénzügyi irányítása

Minden olyan pénzügyi szemponttal foglalkozik, amely az informatikaszolgáltatás biztosításával és támogatásával kapcsolatos. Sok szervezet megpróbál egyensúlyt teremteni a költségek és költségterhelések (számlázások) között.

Szolgáltatástámogatás

Ügyfélszolgálat

Az ügyfélszolgálat célja, hogy egyetlen központi kapcsolati pontot biztosítson az ügyfél és az informatikai szolgáltatásmenedzsment között, kezelje az incidenseket és az igényeket, és kapcsolatot biztosítson a többi folyamathoz: a változás-, probléma-, konfiguráció-, kiadás-, szolgáltatási szint és az informatikaszolgáltatás-folytonosság menedzsmenthez.

Incidensmenedzsment

Az incidensmenedzsment elsődleges célja zavar esetén a normál szolgáltatási feltételek visszaállítása, amilyen gyorsan az lehetséges, minimalizálva a üzleti tevékenységre gyakorolt káros hatását, így biztosítva a szolgáltatás minőségének lehetséges legjobb színvonalát.

Problémamenedzsment

A problémamenedzsment célja az informatikai infrastruktúrán belüli hibák által okozott incidensek és problémák üzleti tevékenységre gyakorolt káros hatásának a minimalizálása, és az ezekhez a hibákhoz tartozó incidensek ismételt előfordulásának a megakadályozása.

Változáskezelés

A változás az a folyamat, amikor az egyik definiált állapotból a másik definiált állapotba mozdulunk el.

A változáskezelés célja, hogy minden változás gyors és hatékony kezelésére szabványos módszerek és eljárások használatát biztosítsa annak érdekében, hogy a változással összefüggő incidensek szolgáltatás minőségre gyakorolt hatását minimalizálja, és következésképpen javítsa a szervezet napi működését.

Konfigurációkezelés

A konfigurációkezelés annak a folyamatnak a neve, amely magában foglalja minden informatikai komponens azonosítását, rögzítését és jelentését, beleértve azok verzióját, alkotó részeit és kapcsolatait.

A konfigurációs elemekre (CI) vonatkozó információkat a konfigurációkezelő adatbázisban (CMDB) tárolja, amelyet a szolgáltatásmenedzsment minden folyamata használ.

Kiadáskezelés

A kiadás az informatikaszolgáltatás jóváhagyott változásainak halmazát írja le.

A kiadáskezelés végzi a hardver és szoftver ütemezését, tervezését, építését, konfigurálását és tesztelését, hogy a kiadás komponensek egy készletét hozza létre a működő környezet számára. Tevékenységei ugyancsak lefedik egy kiadás több ügyfél és több helyszín számára történő tervezését, előkészítését és ütemezését.

A magas színvonalú informatikaszolgáltatás iránti igény okai:

- A szervezetek egyre nagyobb mértében válnak függővé az informatikaszolgáltatástól
- A hibák észlelhetőségének magasabb foka
- A felhasználói igények pontosodása, konkrétabbá válása
- Az infrastruktúra komplexitásának (bonyolultságának) növekedése
- Az informatikaszolgáltatás költségterhei
- Az ügyfelekért folytatott verseny

Az ITIL dokumentációs rendszere

Strategy (Portfolio)

Portfolio Strategy

Financial Management

Service Portfolio Management

Release management

Design (Product Management)

Capacity Management

Availability Management

Security Management

Continuity Management

Demand Management

Service Catalogue Management

Transition (Development)

Transition Planning & Support

Service Assets & Configuration Management

Change Management

Service Validation & Testing

Knowledge Management

Deployment Management

Evaluation

Operation (Support)

Service Desk

Incident Management

Event management

Request Fulfilment

Problem Management

Access Management

Application Management

IT Operation Management

Technical Management

Continual Improvement (Quality)

The 7- Step Improvement Process

Quality Management System

Business Questions For CSI

ROI For CSI

Service Management

Service Reporting

Szolgáltatásstratégia (Service **Strategy**)

A folyamat azonosítja azokat a (piaci) lehetőségeket, amelyeket új szolgáltatások bevezetésével ki lehetne aknázni. Az eredmény egy stratégiai dokumentum, amely felvázolja az új szolgáltatás tervezésének, megvalósításának, üzembe helyezésének és folyamatosan javuló minőségben történő nyújtásának folyamatát.

A szolgáltatás bevezetése új képességekkel ruházza fel a szolgáltató céget (szervezetet), ezáltal értéknövelő szerepet tölt be. A kötet legfontosabb fejezetei a *Szolgáltatás-portfólió kezelése* és *Pénzügyi menedzsmentje*.

Szolgáltatástervezés (Service **Design**)

A folyamat eredményeként projekt-terv készül az előző lépésekben keletkezett stratégia által felvázolt szolgáltatás konkrét megvalósítására.

A terv részletezi az új szolgáltatás bevezetésének minden vonatkozását, a bevezetéshez és üzemeltetéshez szükséges támogató folyamatokkal együtt.

A kötet legfontosabb fejezetei az *Üzemeltetés és üzembitel biztosítása*, *Kapacitástervezés* valamint az *Informatikai- és üzembiztonság*.

Szolgáltatáslétesítés és változtatás (***Service Transition***)

A megtervezett szolgáltatás létesítéséhez és a környezet módosításához szükséges folyamatok leírása.

Fontos fejezetek a Változás- és verziókezelés, Konfigurációmenedzsment és Dokumentációkezelés.

Szolgáltatásüzemeltetés (***Service Operation***)

Az előzővel szorosan összefüggő kötet tárgyalja a szolgáltatás folyamatos és hibamentes üzemeltetéséhez szükséges folyamatokat és szervezési kérdéseket.

A folyamatok garantálják a szolgáltatási megállapodásokban (SLA, *Service level agreement*) vállalt szolgáltatásminőséget.

Legfontosabb fejezetek a *Hiba-* és *igény-* és *incidenskezelés*.

Állandó szolgáltatásfejlesztés (*Continual Service Improvement*)

c. kötet tárgyalja a szolgáltatás folyamatosan javuló minőségben nyújtásának feltételeit.

Kiemelt fejezetek a *Szolgáltatási szint mérése, riportolása (jelentése) és menedzsmentje* c. fejezetek.

ISO 27001

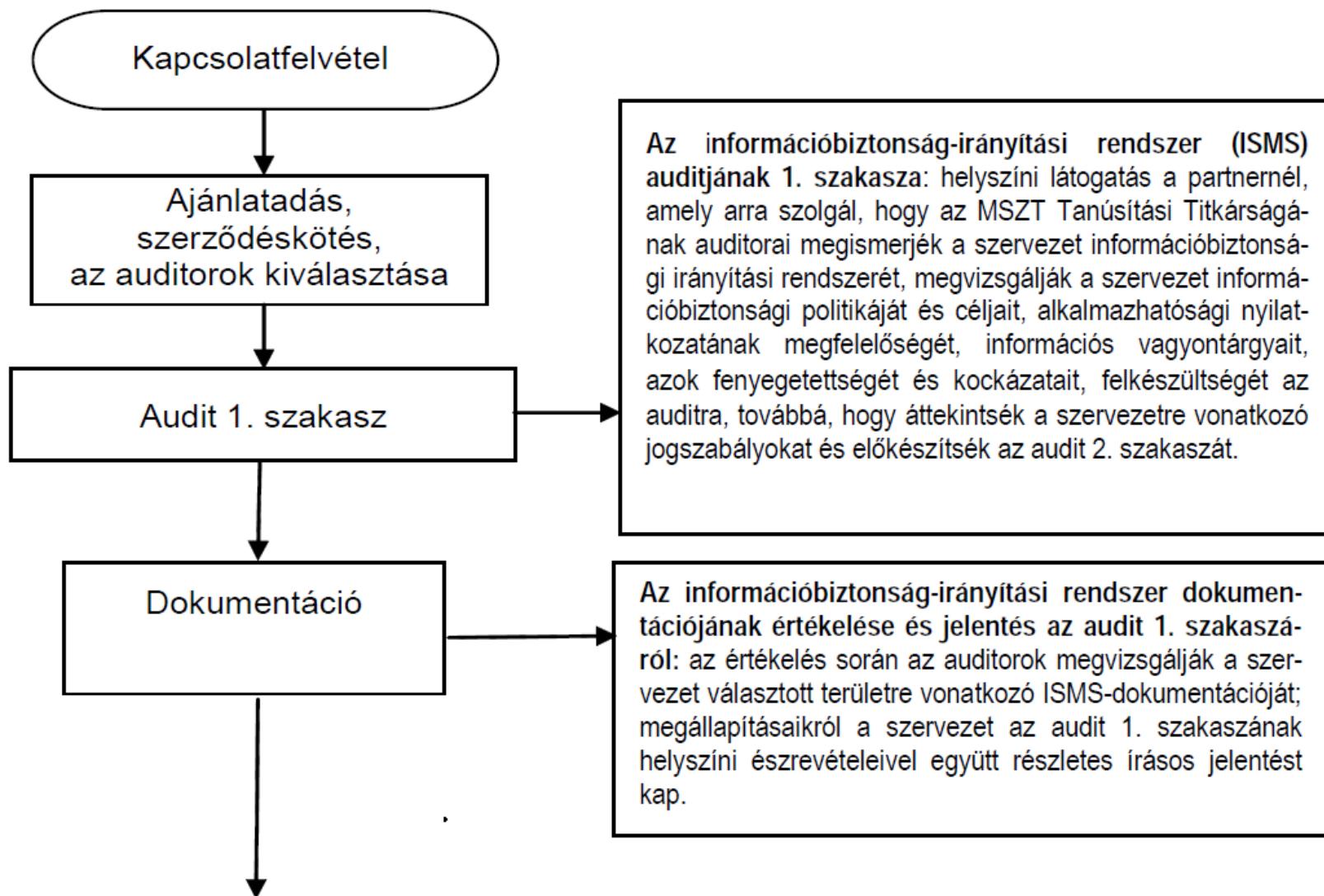


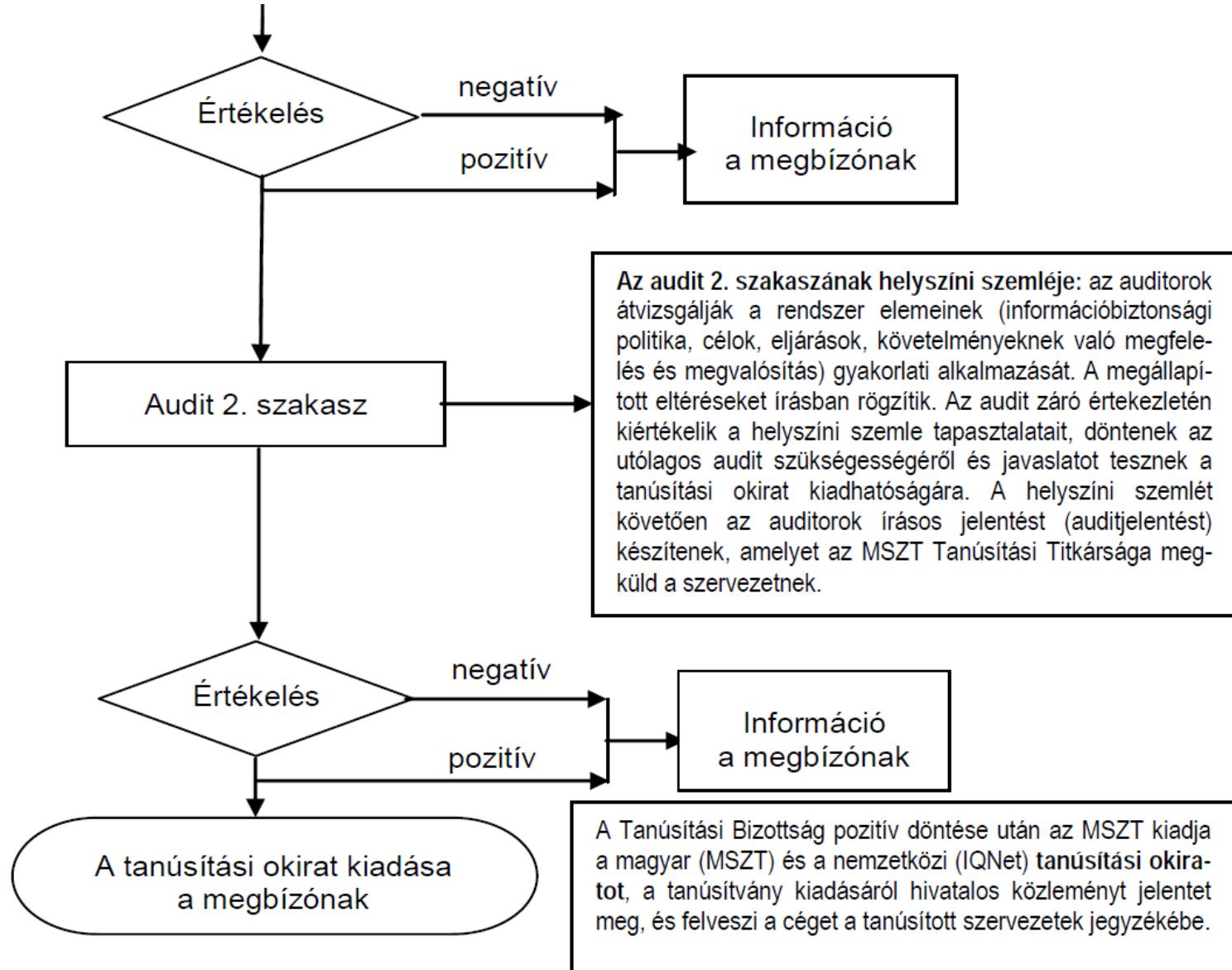
ISO

Nemzetközi Szabványosítási Szervezet (**O**rganization for International **S**tandardization).

A **27000**-es szám a nemzetközi szabványosítás területén egy speciális témakörnek van fenntartva, ez pedig az **információbiztonság** és annak menedzselése.

A Magyar Szabványügyi Testület MSZ ISO/IEC 27001:2014 szabvány szerinti tanúsítási eljárásának lépései





Magyar Szabványügyi Testület • Tanúsítási Titkárság

✉: H-1450 Budapest 9. Pf. 24. • 1082 Budapest, Horváth Mihály tér 1. • ☎ : (361) 456-6928 • Fax: (361) 456-6940
E-mail: cert@mszt.hu