# KR TITKOSÍTÓ PROGRAM

# Felhasználói leírás

***v1.3***
***2008. március 12.***

# TARTALOMJEGYZÉK

# 1 BEVEZETÉS

A Krtitok nevű kriptográfiai alkalmazás JAVA programozási nyelven íródott, amely az ügyfélkapun keresztül történő titkosított kommunikációt biztosítja, platform függetlenül.
A program kétféle működést tesz lehetővé, parancssori indítást megfelelő paraméterezettséggel vagy a krtitok.exe indítását. Az utóbbi az adott platformnak megfelelő kinézetű ablakban, a hozzá tartozó menürendszeren keresztül használható.

## 1.1 Felhasználói dokumentációra vonatkozó általános leírások

A felhasználói dokumentációban alkalmazott képernyőtervek WINDOWS XP operációs rendszerben kerültek elkészítésre. Ezen képernyőtervek megjelenése az adott operációs rendszertől függően eltérőek, de a programban elérhető menüpontok és funkciók változatlanok.

A dokumentum szerkesztése során a következő formai elemek kerültek alkalmazásra:

- <Nyomógombok> a relációs jelek között megadott szöveg nyomógombra utal. A szöveg a nyomógomb feliratát tartalmazza;
- Ablakok, és felületek neve vastagított betűkkel szedve;
- „Üzenetek”, „Opciók” és „apró képek” idézőjelek között;
- Mezőnevek vastagított betűkkel szedve;
- Menüpontokat „\” jel választja el.

# 2 ALAPFOGALMAK

Az itt felsorolásra kerülő fogalmak a krtitok programban használt kifejezések magyarázatát írják le a krtitok programra vonatkoztatva, melyek a nyomtatványkitöltő programmal előállított állományokra értelmezve kerülnek tárgyalásra.

Titkosítás: A nyomtatványkitöltő programmal előállított .xml vagy .abv kiterjesztésű állományok és a nyomtatványhoz csatolt dokumentumok nyílt adatainak, matematikai műveletekkel és kulcs felhasználásával történő, védett adattartalmú állapotának előállítása.

Kititkosítás: A védett adattartalom visszafejtése, matematikai műveletekkel és kulcs felhasználásával, melynek során előáll a nyílt adattartalom (pl.:.dat, .xml vagy .abv).

Kulcspár: Egy nyilvános kulcsból (public key) és egy magán kulcsból (private key) áll.

Nyilvános kulcs (public key): Bárki számára hozzáférhető kulcs – például egy publikus adatbázisból kikereshető -, amellyel a titkosítást végezzük.

Magán kulcs (private key): Csak a tulajdonos számára ismert kulcs, amelyet a kititkosításnál vagy másképpen visszafejtésnél használunk.

Kulcshossz: A kulcs készítés során a felhasznált bitek számát határozza meg. Az alapértelmezett kulcshossz 1024 bit, de választható 2048 bit is. Általában kevésbé veszélyeztetett a nagyobb kulcs, de tovább tarthat a titkosítás és a visszafejtés, mint egy kisebb méretű kulcs esetében.

Kulcstár típusa: Kulcspár generálásakor alapértelmezetten a PGP kulcstár támogatott.

A Krtitok program ezen kívül a következő kulcstár típusokat támogatja:

- X509 típusú kulcstár;
- Pkcs12 típusú kulcstár;
- JKS (Java Key Store) típusú kulcstár.

Kulcspár neve: Egyedi azonosítóként szolgál, amely a kulcsgenerálás során a nyilvános és magán kulcs elnevezéseiben is felhasználásra kerül.

Jelszó (magán): (A krtitok programban elvárt jelszó politika szerint a megfelelő jelszó kisbetűt, nagybetűt, számot és egyéb speciális karaktereket egyaránt tartalmaz, amelynek minimum nyolc karakter hosszúnak kell lennie.)

Kulcspár generálás: A megadott kulcshosszal, kulcstár típussal és jelszóval létrehoz egy nyilvános és egy magán kulcsot.

Titkosítandó fájl neve: A nyomtatványkitöltő program által előállított, alapértlemezett telepítés esetén a titkosítatlan könyvtárban lévő .xml vagy .abv kiterjesztésű állományok.

Meta fájl neve: Egy .mf kiterjesztésű állomány, melyet a nyomtatványkitöltő program állít elő. Ez egy boríték, melyben a címzettre vonatkozó nyilvános adatok és a címzett nyilvános kulcsa található.

Titkosítás célkönyvtára: A krtitok program által létrehozásra kerülő .kr állomány elérési útvonala.

Kulcsot védő jelszó: A kulcstárból kiválasztott kulcshoz tartozó magán kulcs kijelölésekor kéri a program, amely a visszafejtés során kerül felhasználásra.

Kititkosítás célkönyvtára: A krtitok program által létrehozásra kerülő .xml vagy .abv llomány elérési útvonala.

**Programban használt Ikonok**

| Ikon képe | Leírása |
|---|---|
|  | PGP kulcstár |
|  | Nyilvános kulcs |
|  | Magán kulcs |
|  | X509 tanúsítvány |
|  | Java kulcstár |
|  | PKCS12 típusú kulcstár |

**A program használata során előforduló fájlok és kiterjesztésük**

Kulcsok:

- Nyilvános kulcs (Public key): kulcspár neve + Pub.asc pl.:kulcsomPub.asc
- Magán kulcs (Private key): kulcspár neve + Prv.asc pl.:kulcsomPrv.asc

Titkosítatlan állományok:

- „.dat”: A nyomtatványkitöltő programban lévő nyomtatványaink mentett adatait tartalmazó állomány.
- „.abv”: A nyomtatványkitöltő program **Bevallás megjelölése elektronikus beküldésre** menüpontja által létrehozásra kerülő állomány, amely a kitöltött nyomtatvány adatait és vizuális képét hordozza bináris formátumban.
- „.xml”: Az „.abv” állománynál leírtak jellemzik, különbség, hogy csak a nyomtatvány kitöltött adatait hordozza xml formátumban.
- „.mf”: Szintén a **Bevallás megjelölése elektronikus beküldésre** menüpont hatására létrejövő boríték állomány, amely a kitöltött nyomtatványunkra vonatkozó nyílt adatokat hordoz.
- „.cst”: A nyomtatvány csatolmányait tartalmazza. A fájl xml formátumú, Bzip2-vel tömörítve.

Titkosított állomány:

- „.kr” A nyomtatványkitöltő program által létrehozott állomány, melyet a **Bevallás megjelölése elektronikus beküldésre** vagy az **XML file ellenőrzése és megjelölése beküldésre** menüpontok választása esetén jön létre.

Kititkosított állomány (visszafejtett):

- Eredeti kiterjesztés

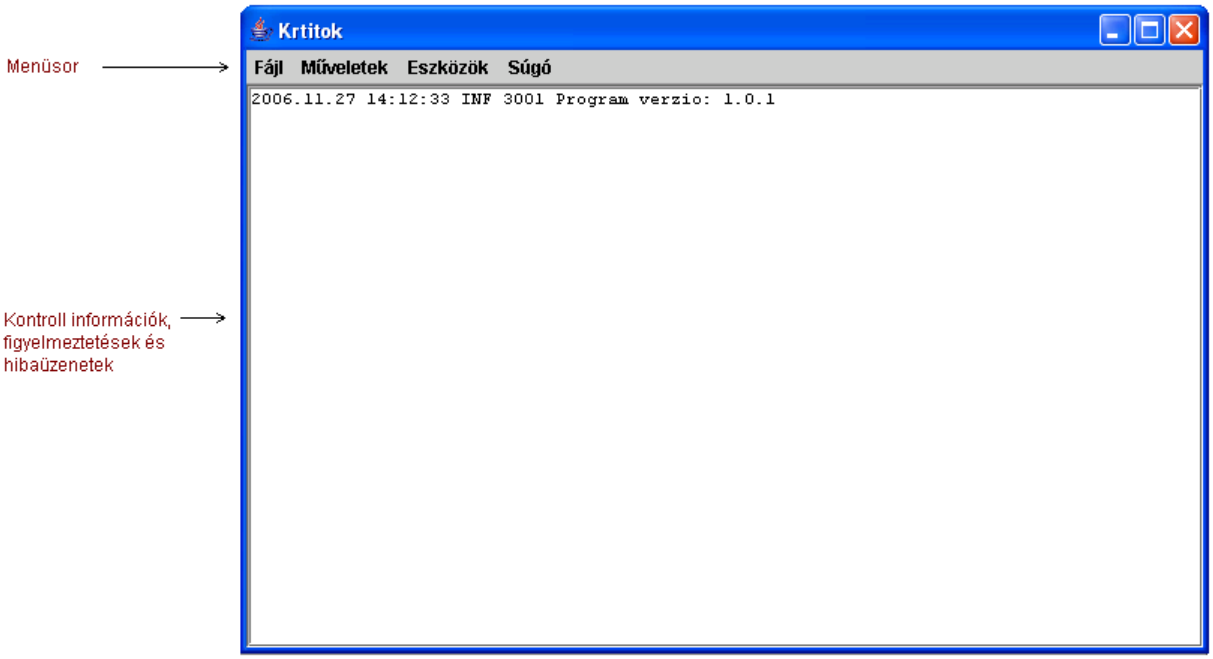
Krtitok munkaállományai:

- .krtitok.log: A Krtitok program napló állománya.
- .krtitok.ini: A Krtitok programban lévő Eszközök\Beállítások menüpontban megadható adatokat tárolja.

# 3 A KRTITOK NEVŰ PROGRAM HASZNÁLATA

## 3.1 Menüpontok

Induló képernyő



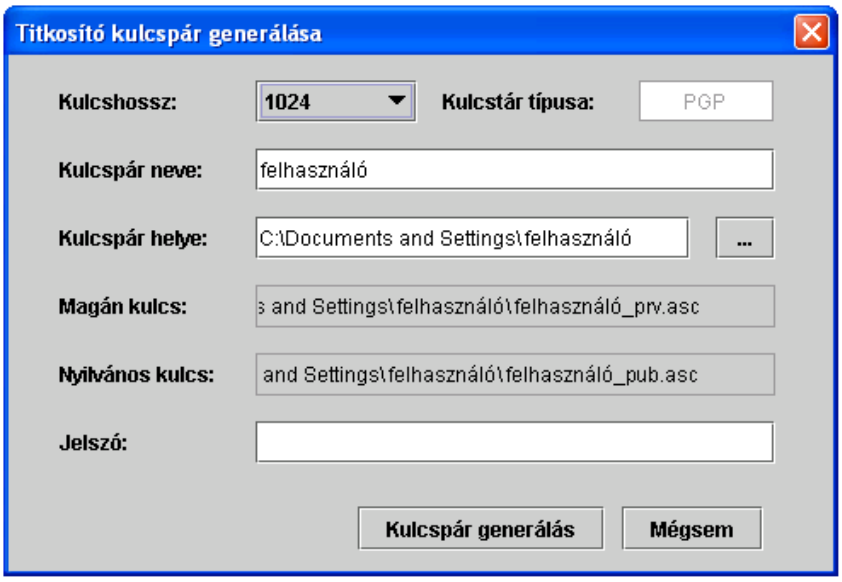

A program Windows XP operációs rendszer esetében a következő megjelenésű képernyővel indul.

A KRTITOK program közvetlenül indítható az ÁNYK -> Szerviz -> Titkosítás saját tanúsítvánnyal menüpontjából.

### *3.1.1 Műveletek*

#### 3.1.1.1 Titkosító kulcspár generálás

A menüpont lehetőséget biztosít a titkosításhoz és a kititkosításhoz (visszafejtéshez) szükséges nyilvános és magán kulcsok előállítására.




Titkosító kulcspár generálásakor a következőket kell megadnunk:

**Kulcshossz**: A program alapértelmezettként az 1024 bit-es kulcshosszt ajánlja fel. A lefelé mutató nyílra kattintva az értéklistában megjelenő 2048 bit-es érték is választható.

**Kulcstár típusa**: Nem módosítható. Alapértelmezett érték a PGP típusú kulcstár használata.

**Kulcspár neve**: Az itt megadott érték kulcs párunk egyedi azonosítója lesz, amely a nyilvános és magán kulcsunk nevében megjelenítésre kerül.

Nyilvános kulcsunk esetében a „Pub” (Public), míg magán kulcsunk esetében a „Prv” (Private) karakterekkel kerülnek kiegészítésre a kulcsnevek.

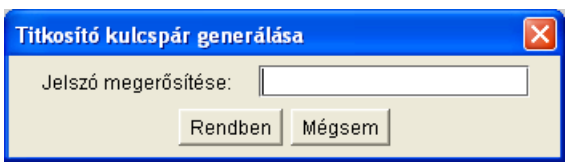
A létrehozásra kerülő nyilvános és magán kulcsok kiterjesztése „.asc”.

**Nyilvános kulcs helye**: Alapértelmezett esetben operációs rendszertől függően a bejelentkezett felhasználóhoz tartozó munkakönyvtár útvonala. Az útvonalat a <...> könyvtárválasztó gomb segítségével tetszőlegesen módosíthatjuk, de a mező kézzel nem írható.

**Magán kulcs helye**: Megegyezik a nyilvános kulcs helyével, így ugyanaz a könyvtárválasztó gomb vonatkozik rá, mint a nyilvános kulcsra.

**Jelszó (magán)**: Az itt megadásra kerülő jelszót a magán kulcsunk használatakor kéri majd a rendszer. Mások által, a saját nyilvános kulcsunkkal titkosított adatok kititkosításához (visszafejtéséhez) szükségünk lesz a saját magán kulcsunkra és a hozzá tartozó jelszóra, így a jelszó megadására és megjegyzésére fordítsunk kellő figyelmet.

A mezők megfelelő kitöltése után válasszuk a **<Kulcspár generálása>** gombot. A következő ablak kerül megjelenítésre:



Itt újra meg kell adnunk a korábban a Jelszó(magán) mezőbe írt értéket megerősítés céljából. Megfelelő jelszó megadása esetén megtörténik a kulcspár generálása, melyet sikeres esetben a következő üzenet jelez:


A létrejött állományok:

| | |
|---|---|
| felhasználó_prv.asc | felhasználó_pub.asc |

A kulcsgenerálás után az Eszközök\Beállítások menüpontban lévő következő elérési útvonalak és kulcshasználatra vonatkozó opció automatikusan beállításra kerül:

- Saját magán kulcsának helye kulcspár helye;
- Saját nyilvános kulcsának helye kulcspár helye;
- Kívánja-e a saját kulcsát a titkosításhoz automatikusan használni: igen.

#### *3.1.1.1.1 TITKOSÍTÓ KULCSPÁR GENERÁLÁSRA VONATKOZÓ FIGYELMEZTETÉSEK*

- A kulcspár neve és a jelszó megadása kötelező!

A **<Kulcspár generálás>** gombra kattintáskor még nem kerültek kitöltésre a kulcspár neve és a jelszó mezők.

- Sikertelen kulcsgenerálás! Hiba a fájl létrehozásakor!

Lehet jogosultság probléma a megadott könyvtár írásakor, vagy már ugyanazon a néven létezik nyilvános és magán kulcsunk a megadott útvonalon.

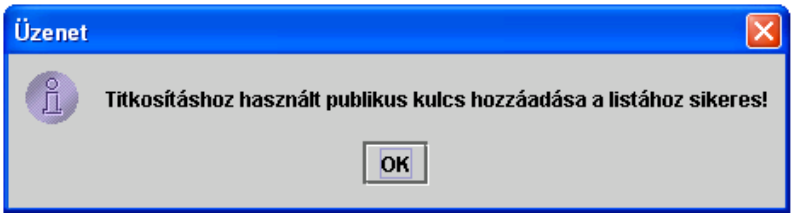
- A jelszó megerősítésekor hibásan adta meg jelszavát!

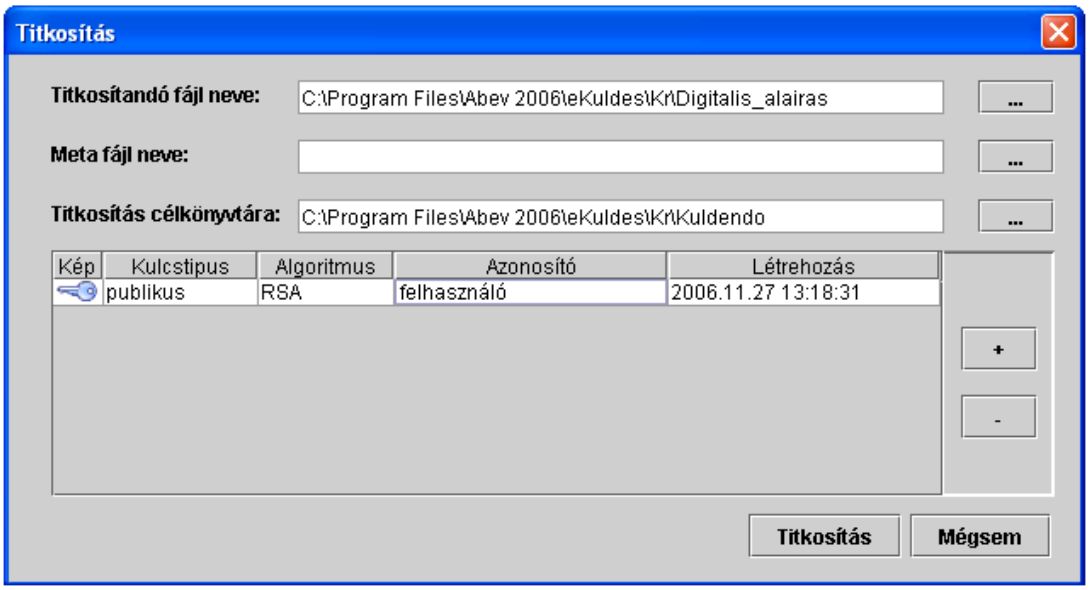
Eltérő érték került begépelésre a **Jelszó (magán)** illetve a **Jelszó megerősítése** mezőkbe.

### 3.1.1.2 Titkosítás

A menüpont lehetőséget biztosít a nyomtatványkitöltő által előállított .xml vagy .abv kiterjesztésű állományok, illetve a nyomtatványhoz csatolt dokumentumok nyílt adatainak védetté tételére.

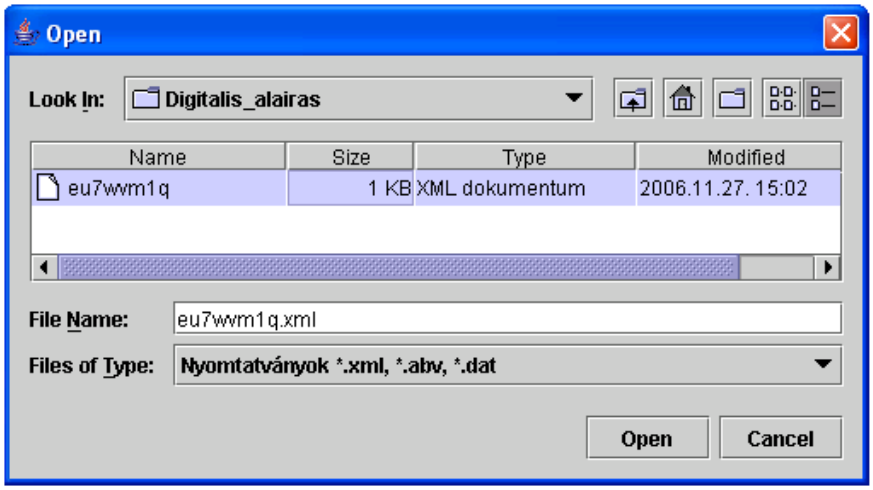
Amennyiben az Eszközök\Beállítások menüpontban jelölt a „Kívánja-e saját kulcsát a titkosításhoz automatikusan használni” opció, úgy saját kulcsunk automatikusan hozzáadásra kerül a címzettek listájához.





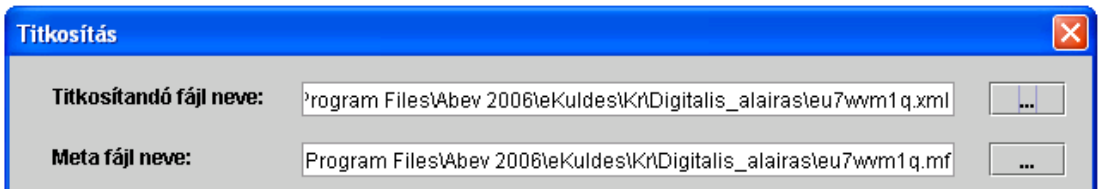

Titkosítás során a következőket kell megadnunk:

**Titkosítandó fájl neve**: Alapértelmezetten a nyomtatványkitöltő program Digitalis_alairas könyvtárát ajánlja fel. A <...> fájlválasztó gombra kattintva a következő ablak jelenik meg:




A kiválasztott fájlt az **<Open>** gomb megnyomásával érvényesíthetjük, amely a titkosítatlan fájl neve mezőbe beírásra kerül.

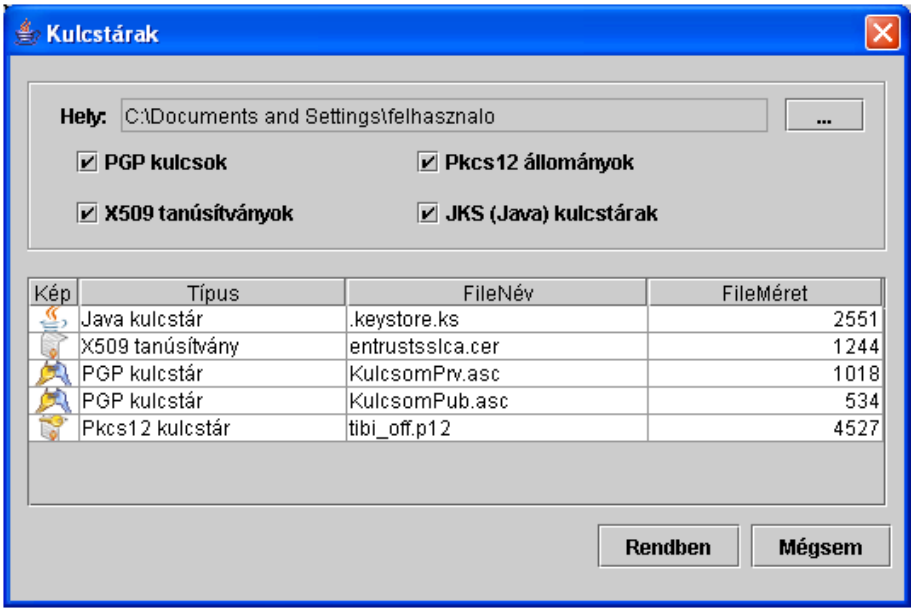
**Meta fájl neve**: Ha nyomtatványkitöltő programunk az alapértelmezett könyvtárak szerint telepített, akkor az előbb kiválasztott titkosítatlan fájl nevével megegyező nevű „.mf” kiterjesztésű állomány automatikusan beírásra kerül ebbe a mezőbe.




Egyébként a <...> fájlválasztó gombra kattintva adhatjuk meg a titkosítandó fájlhoz tartozó boritékot.

**Titkosítás célkönyvtára**: Alapértelmezetten a nyomtatványkitöltő program Kuldendo könyvtárát ajánlja fel, amit tetszőlegesen módosíthatunk a <...> fájlválasztó gombbal.

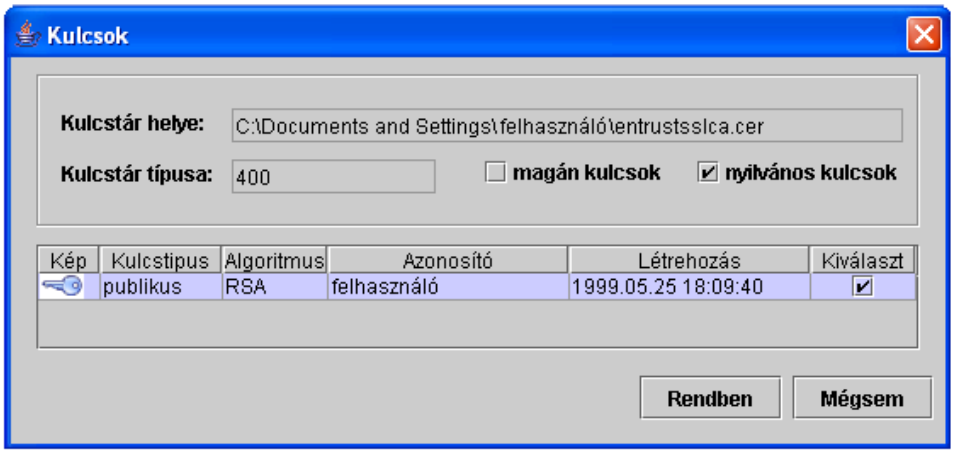
**Hozzáadás címzettek listájához** <+>: A címzettek listájához nyilvános kulcsot adhatunk, melyet a **Kulcstárak** nevű ablakon választhatunk ki.




A kiválasztás a következők szerint végezzük:

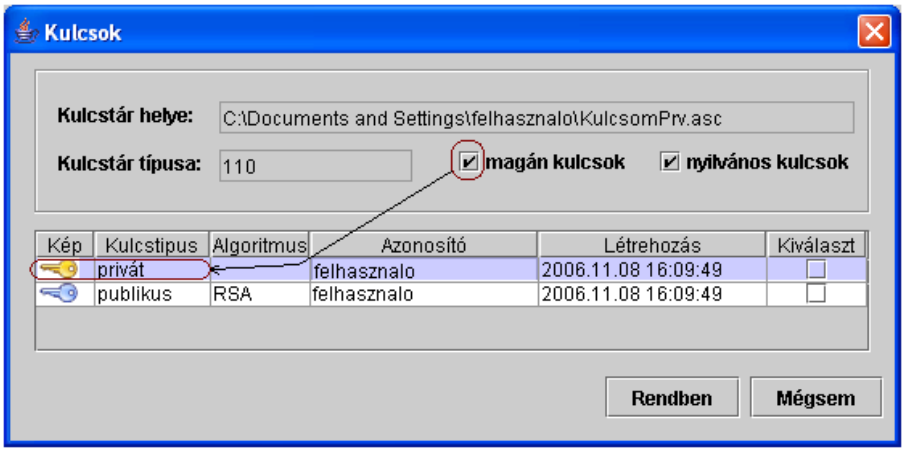
1. Jelöljük ki a listában azt az egy kulcstár típust, melynek nyilvános kulcsát a címzettek listájához kívánjuk hozzáadni.
2. Az egér bal gombjával kattintsunk duplán a kiválasztott kulcstár típuson.

A megjelenő **Kulcsok** ablakban alapértelmezetten a „nyilvános kulcsok” opció jelölt. A listában megjelenő kulcsot „” az egér bal gombjával történő dupla kattintással, vagy a „Kiválaszt” oszlopban lévő jelölőnégyzetre történő egyszeri kattintással választhatjuk ki.



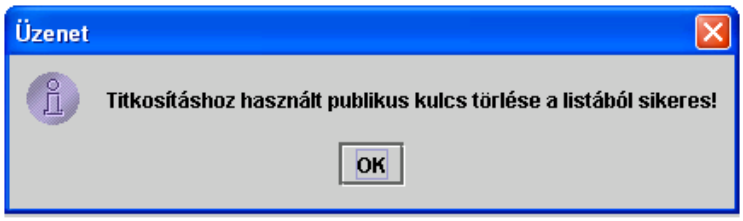

Ennek tényét a jelölőnégyzetben a pipa is „” igazolja, valamint a megjelenő **Üzenet** ablak szövege „Kulcs hozzáadása a listához sikeres!”.

Az ablakon található „magán kulcsok” opció alapértelmezetten nem jelölt, mivel itt nyilvános kulcsok hozzáadása a cél. A jelölőnégyzetre kattintva azonban lehetőségünk van meggyőződni arról, hogy kulcstárunk tartalmazza-e magán kulcsunkat is.

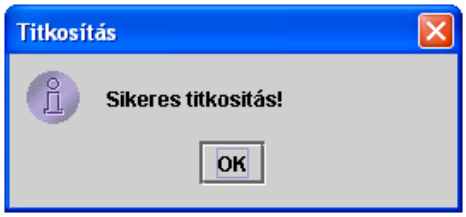



A <Rendben> gomb a kiválasztott kulcsot hozzáadja a címzettek listájához. A <Mégsem> gombot választva a program a **Kulcsok** ablak meghívása előtti állapothoz tér vissza.

**Törlés címzettek listájából** <-> : A címzettek listájából törli a kiválasztott nyilvános kulcsot.




A mezők megfelelő kitöltése után válasszuk a **<Titkosítás>** gombot, amely után, sikeres esetben a következő ablak kerül megjelenítésre:



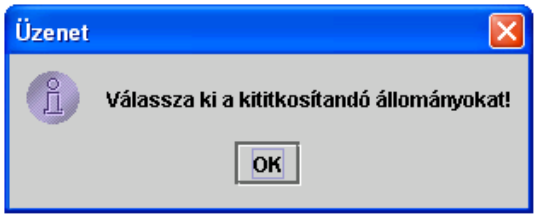

A létrejött állomány:

| Titkosítandó fájl neve.kr |
|---|

### 3.1.1.3 Kititkosítás

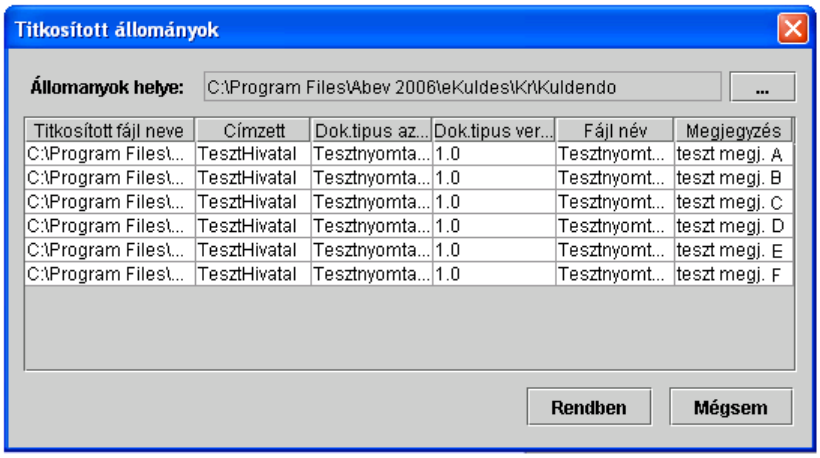
A menüpont lehetőséget biztosít a titkosított állományok visszafejtésére. Titkosítás során a következőket kell megadnunk:

**Kititkosítandó állományok**: A Műveletek\Kititkosítás menüpont meghívása után a következő üzenet kerül megjelenítésre:




Az <Ok> gombra kattintás után a nyomtatványkitöltő program Kuldendo könyvtárában lévő „.kr” kiterjesztésű állományok kerülnek megjelenítésre a **Titkosított állományok** nevű

ablakban. Az útvonalat a <...> könyvtárválasztó gomb segítségével tetszőlegesen módosíthatjuk, de a mező kézzel nem írható.

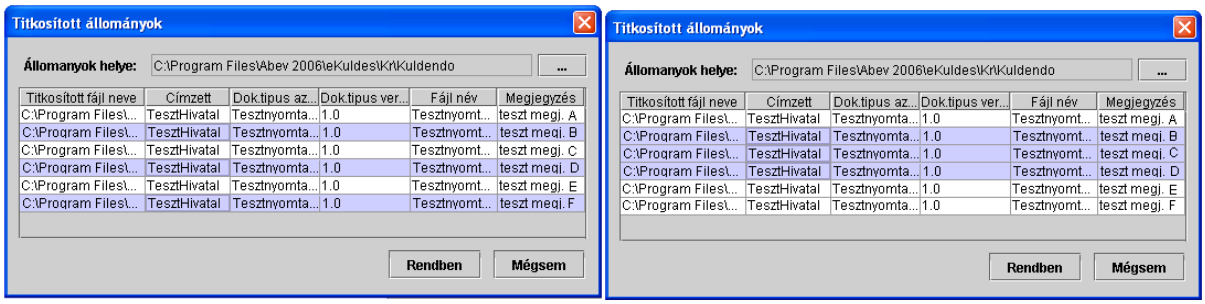



Több állomány együttes kijelölése:

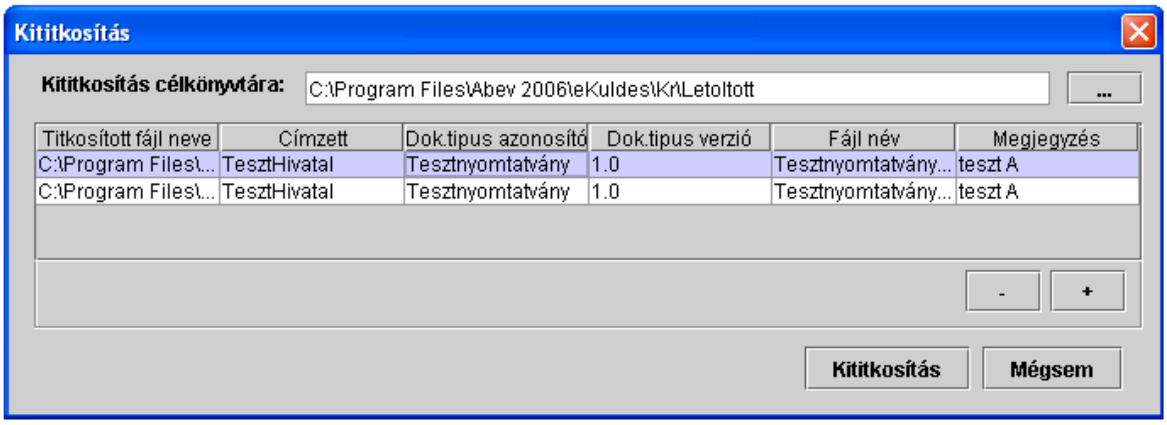
A <CTRL> gomb folyamatos nyomva tartása mellett az egér bal gombjával egyesével tudjuk egymás után kijelölni a kititkosítandó állományokat.

A <SHIFT> gomb folyamatos nyomva tartása mellett az egér bal gombjával egyszerre több állományt jelölhetünk ki

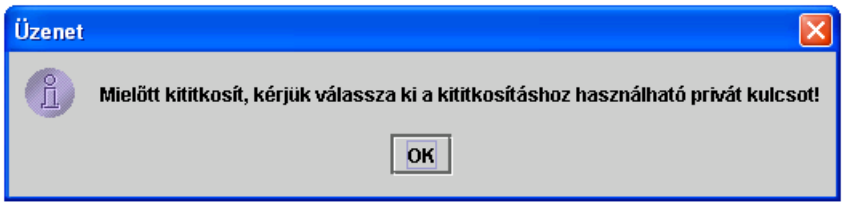
Példa a <CTRL> és <SHIFT> gombbal történő kijelölésekre.



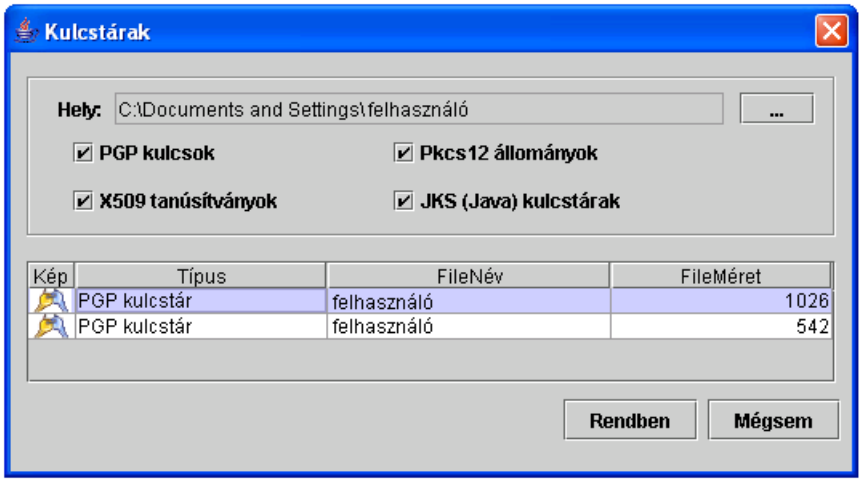

**Kititkosítás célkönyvtára**: Alapértelmezetten a nyomtatványkitöltő program Letoltott könyvtárát ajánlja fel. Útvonalat a <...> könyvtárválasztó gombbal módosíthatjuk.



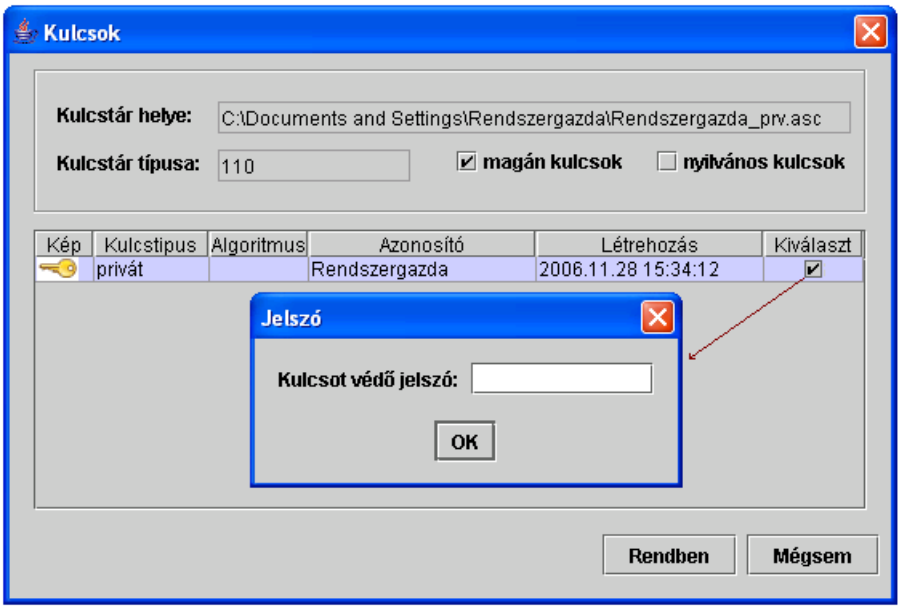

A **Kititkosítandó állományok** és a **Kititkosítás célkönyvtárának** megadása után válasszuk a **<**Kititkosítás**>** gombot, amely után egy **Üzenet** ablak kerül megjelenítésre:



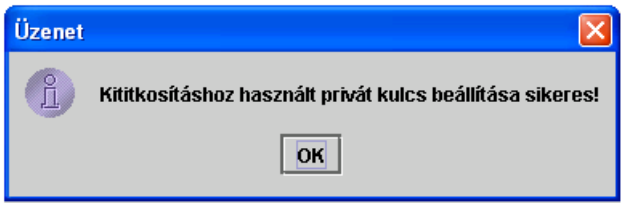

Az <Ok> gombra kattintva megjelenik a **Kulcstárak** nevű ablak, ahol az egér bal gombjával történő dupla kattintással választhatjuk ki a kívánt kulcstárat, melyből privát kulcsunkat adhatjuk meg.



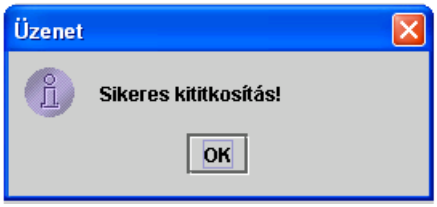

A kulcstár kiválasztása után a **Kulcsok** nevű ablakban alapértelmezetten a „magán kulcsok” opció jelölt, mivel itt a magán kulcs kiválasztása a cél.




A listában lévő magán kulcson duplán, vagy a „Kiválaszt” oszlopon egyszer kattintva az egér bal gombjával, megjelenik a **Jelszó** bekérő ablak. Itt kell megadnunk a magán kulcsunkhoz tartozó jelszót. Megfelelő jelszó megadása esetén a jelölőnégyzetben a pipa lesz látható, majd egy **Üzenet** ablak jelenik meg:



Ezek után megtörténik a kititkosítás, amely sikeres esetben a következő üzenetet adja:




A létrejött állomány:

- a kititkosított állomány eredeti néven,
- amennyiben a titkosított állomány csatolt dokumentumokat is tartalmaz, a titkosítatlan csatolmányok a kititkosítás célkönyvtárán belül, a **kititkosítandó fájl neve_csatolmányok** könyvtárba kerülnek mentésre.

## *3.1.2 Eszközök*

### 3.1.2.1 Beállítások

A menüpont lehetőséget biztosít saját magánkulcsunk elérési útvonalának és használatának módosítására, valamint tetszőleges könyvtárak elérési útvonalának megadására.