

INFORMATIKAI BIZTONSÁG ALAPJAI

3. előadás

Göcs László

főiskolai tanársegéd

Neumann János Egyetem GAMF Műszaki és Informatikai Kar

Informatika Tanszék

Felhasználók azonosítása



A hagyományos azonosítás alapjai

- **Személy, objektumleírás**

Az azonosítani kívánt elem adatait feljegyzik

Hiba: hiányos információ, a felismerést személy végzi

- **Aláírás vizsgálat**

Eltárolt aláírást a pillanatnyival hasonlítanak össze

Hiba: könnyen hamisítható, összehasonlítás nem megbízható

- **Kulcs vagy kulcsszó használata**

Az objektum vagy személy rendelkezik egy olyan tárggyal, kulccsal, vagy jelszóval, amit ismer az azonosító fél

Hiba: a technológia széles körben ismert, hamisítható

Elektronikus azonosító rendszerek

- A hagyományos azonosítást használják, de az emberi azonosításnál megbízhatóbbak

Hiba: a berendezés is elromolhat, és a berendezést is ember kezeli

Megfelelő humán háttér biztosítása

- Megfelelő oktatás
- Egyszerű kezelhetőség biztosítása
- Segítséget nyújtó rendszerek
- Külső felügyelő

Megfelelő technikai háttér biztosítása

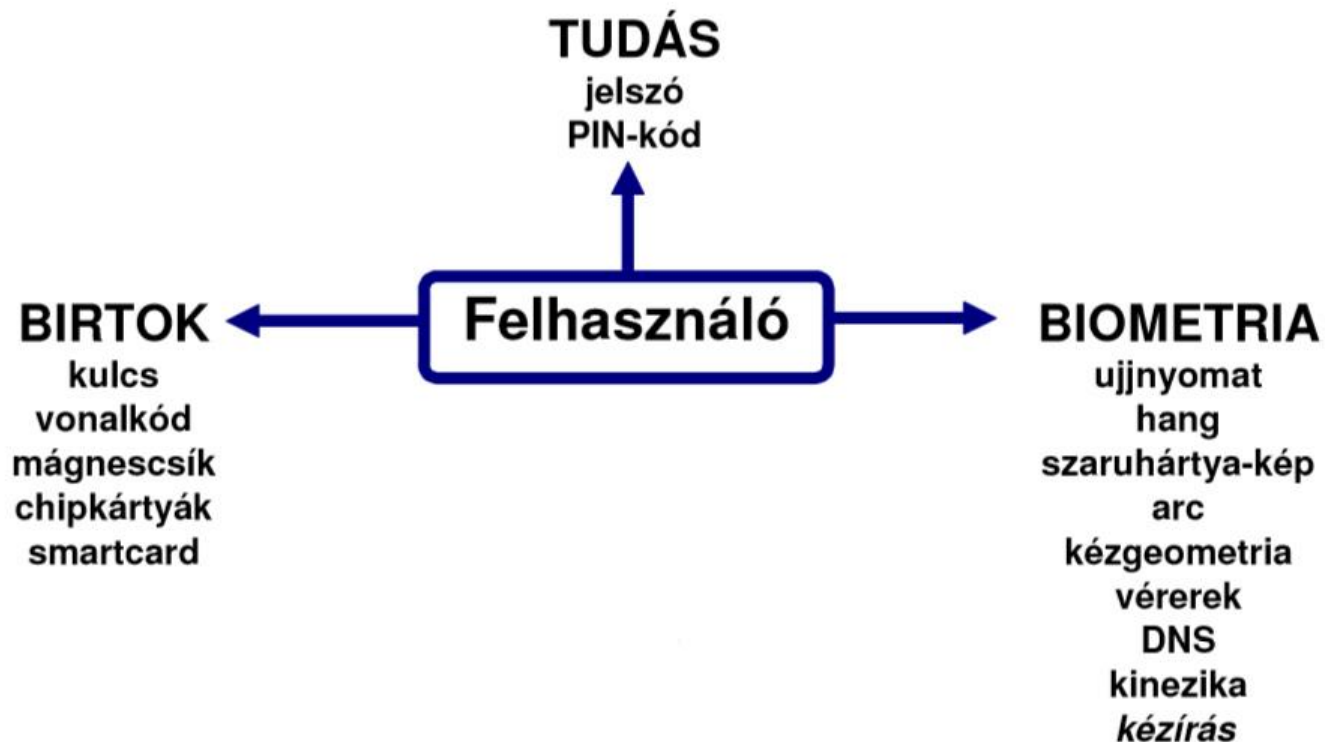
- A feladat által megkívánt rendszer biztosítása
(igényfelmérés, ár-megbízhatóság, körülmények)
- Igénybevételnek megfelelő rendszer
(felmerülő fizikai, kémiai igénybevétel)
- A rendszer megkívánt kiépítése
(teljes, használható, hozzáférhető, igény szerint kihasználható)

Felhasználó azonosítás

Egy személyt több jellemzője alapján is lehet azonosítani!

- Mit tud?
- Mi van nála?
- Fizikai-biológiai értelemben kicsoda?

A felhasználó-azonosítás alapmódszerei:



Tudás

- Használata egyszerű
- Olcsó
- Észrevétlenül másolható és tulajdonítható el
(*nincs visszajelzés ha más birtokába került*)
- Erős védelem megjegyezhetősége nehéz

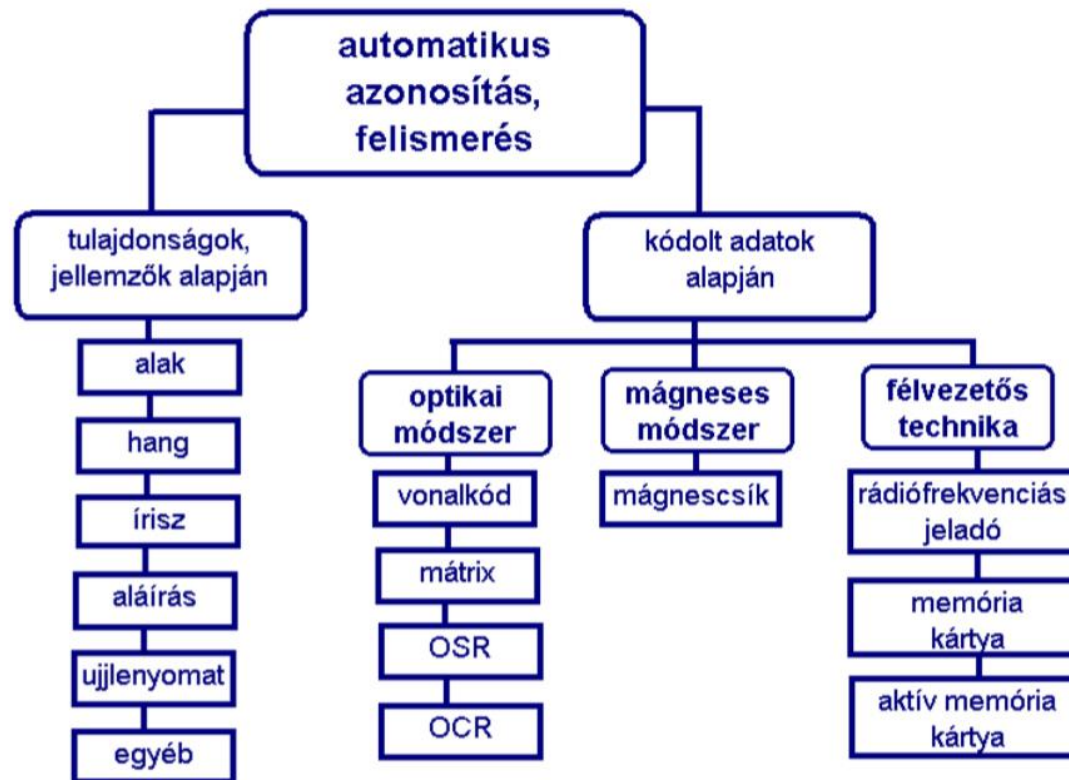
Birtok

- Egyszerű használat.
- Olcsótól a drágáig.
- Eltulajdonítható *(érzékelhető, letiltható)*
- Másolás elleni védelem fontossága! *(titokban ne lehessen másolni, mert nincs visszajelzés)*
 - Másolás szempontjából:
 - Passzív, csak olvasható (vonalkód)
 - Aktív, írható/olvasható (mágneskártyák, chipkártyák, telefonkártyák)
 - Intelligens, kriptográfiai műveletek (másolásvédelem)

Biometria

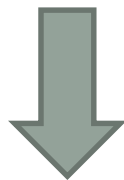
- Néhol nehézkes az alkalmazása de megbízható
- Egyszerű megoldások nem biztonságosak, kizárhatóak.
- A komoly megvalósítások drágák.
- Jogi, adatvédelmi problémák (*biometrikus adatok tárolása*)
- Egészségügyi problémák

Technikai megvalósítás:



Jelszó alapú azonosítás

A személyt azonosító titkos információ (jelszó) titokban tartása lehetetlen



gyenge védelem

(kifigyelhető, megszerezhető)

Jelszavak

- Felhasználók által kitalált
- Számítógép által generált
- PIN-kódok
- Kérdés és válasz kódok
- Kombinációs jelszavak
- Jelmondatok
- Jelmondat alapú betűszavak
- Algoritmikus jelszavak

Azonosítási technikák

Eszközök azonosítása

Vonalkódos rendszerek

A vonalkód **vékony és vastag** vonalakból áll. A vonalkód olvasó fotóérzékelővel a kódot elektromos jellé változtatja olvasás közben, és méri a **relatív szélességét** a vonalaknak és a **helyeket** a vonalak közt.

Így fordítja az olvasó a vonalkódokat írásjelekre, és küldi a számítógéphez vagy kézi terminálhoz.



Vékony-Vastag-Vékony-Vékony-Vastag-Vékony-Vastag-Vékony-Vékony

010010100

(Code 39 Start/Stop írásjel)

Vonalkódos rendszerek

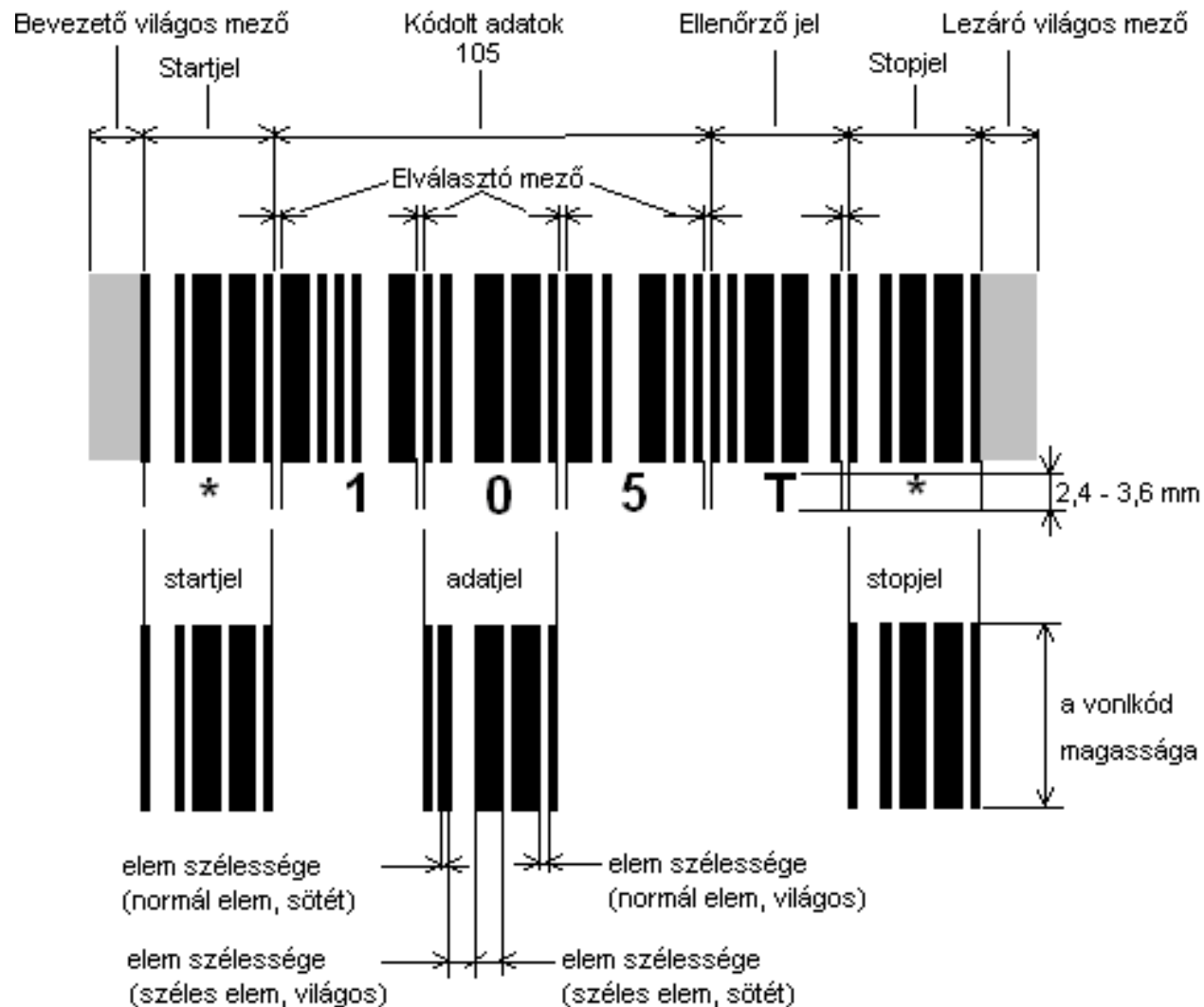
Minden vonalkód egy különleges **Start és egy Stop** jellel rendelkezik. Így tudja az olvasó felismerni, ha előre vagy visszafelé olvasta a vonalsorozatot.

Továbbá, egyes vonalkódoknak **checksum jele** is van közvetlen a Stop jel előtt. A checksum nyomtatás közben van kiszámítva, a vonalkód karakterek alapján.

A vonalkód olvasó **ugyanezt a számítást végrehajtja**, és hozzá hasonlítja az eredményt a checksumhoz.

Ha a két szám nem egyezik, az olvasó **hibát feltételez**, és újból próbálkozik.

Vonalkódos rendszerek



EAN-13 -t világszerte használják kiskereskedelemben. A jel 13 karaktert kódol: az első két vagy három vonal az **országkód** mely jelezi. Az országkódot folytatja 9 vagy 10 **adat** jegyszám, és egy **checkszum**. Két vagy öt jegyszámú kiegészítő vonalkód hozzáadható. Így elérhető a 14 vagy 17 jegyszámú vonalkód.

Modulo 10 kalkuláció a checkszum:

Add össze a páros számú számjegyeket: 2, 4, 6, stb.

Az eredményt 3 -al beszorozni.

Add össze a páratlan számú számjegyeket: 1, 3, 5, stb.

Add össze a 2. és 3. végeredményét.

A check karakter a legkisebb szám mely a 4. lépéshez adható, hogy a 10 többszöröse legyen az eredmény.

Például: Legyen a vonalkód adata = 001234567890

$$0 + 2 + 4 + 6 + 8 + 0 = 20$$

$$20 * 3 = 60$$

$$0 + 1 + 3 + 5 + 7 + 9 = 25$$

$$60 + 25 = 85$$

$$85 + X = 90 \text{ (10 többszöröse legyen az eredmény), tehát } X = 5 \text{ (checkszum)}$$



EAN-8 az EAN-13 kód rövidített változata. Az első két vagy három vonal az országcód, 4 of 5 adat számjegy (az országcód hosszúságán függő), és a checksum. Igaz, hogy lehetséges plusz 2 vagy 5 számjegyes hosszabbítást tenni a kódhoz, az EAN-8 kód fő célja minél kisebb helyet foglaljon el.



A **UPC-A 12** számjegyű kódot tartalmaz. Az első számjegy a számolórendszert azonosítja.

A következő 5 számjegyű kód a gyártót azonosítja.

A ezután levő 5 számjegy a tárgyat azonosítja, és ezt a számot a gyártó adja meg.

Az utolsó számjegy a checksum.



UPC-E az UPC-A variációja, amelyet a 0-s számú rendszerre használható. UPC-E kódok nagyon kicsi helyen elférnek mivel a 0 -t kiszűrik.



Interleaved 2 of 5 számokból álló vonalkód, melyet főleg áruraktárakban, és ipari műhelyekben használnak. Az adatnak páros számú számjegyből kell állnia.

A karakterek 5 elemből állnak, 5 vonal, vagy 5 space. Két elem az ötből vastag, valamint három vékony. Szomszédos karakterek összefésültek, tehát alternálódik a space és vonal egyik karaktertől a következőig.



Codabar a számokat (0-9), hat jelt (-:.\$/+), és a start/stop karaktereket (A, B, C, D, E, *, N, vagy T) kódol. A start/stop karakterek párokban vannak, és nem szerepelhetnek többször a vonalkódban.

Codabar-t könyvtárak, csomagkiszállító szolgálatok, véradó központok, és más adatfeldolgozó alkalmazók használják. Nincs előírt checksum, viszont egyes iparágak kifejlesztették a saját checksum standardekét.



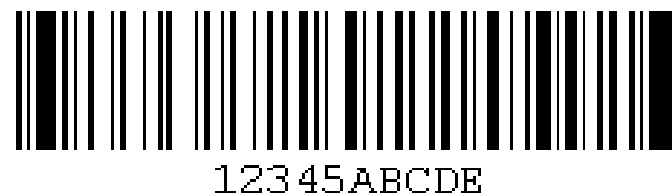
A Code 39 teljes karakter sorozata 0-9, A-Z (csak nagy betűk), és a space, mínusz (-), plusz (+), pont (.), dollár (\$), slash (/), és százalék (%).

A start/stop karakter a kód elején és végén található, és a vonalkódnak nincs maximum hosszassága, viszont 25 -nél több karakter terheli kapacitását.

Minden egyes karakter 9 elemből áll: 5 vonal, és 4 üres hely. Egy karakter 3 vastag, és 6 vékony elemből áll.



Code 93 egy kisebb fajtája a Code 39-nek. Ugyanazokat a karaktereket használja, mint a Code 39, de karakterenként csupán 9 vonalkód elemet használ a 15 helyett. A Modulus 43 checksum nem kötelező, úgy, mint a Code 39 esetében.



Code 128 kitűnően tömörít numerikus és alfanumerikus adatoknak.

Előnyösebb, mint a Code 39, mivel karakterválasztéka bővebb, és tömörebb.

A Code 128-nak teljes karakter sorozata 0-9, A-Z (nagy és kis betűk), és az összes standard ASCII jelek és kontrol kódokból áll.

A kódok három alegységre vannak választva: A, B és C.

- Az A alegység a standard ASCII jeleket, számokat, nagybetűket és kontrol kódokat tartalmazza;
- A B alegység standard ASCII jeleket, számokat, nagybetűket és kisbetűket foglalja össze; és a
- C alegység két számot tömörít egy karakterbe.

Ráadásul, mindegyik alegység tartalmaz kontrol karaktereket, ami engedi a váltást egyik alegységtől a másikig egy vonalkódban. Végül, három külön start kód létezik, mely jelezi, hogy melyik alegységet használja.



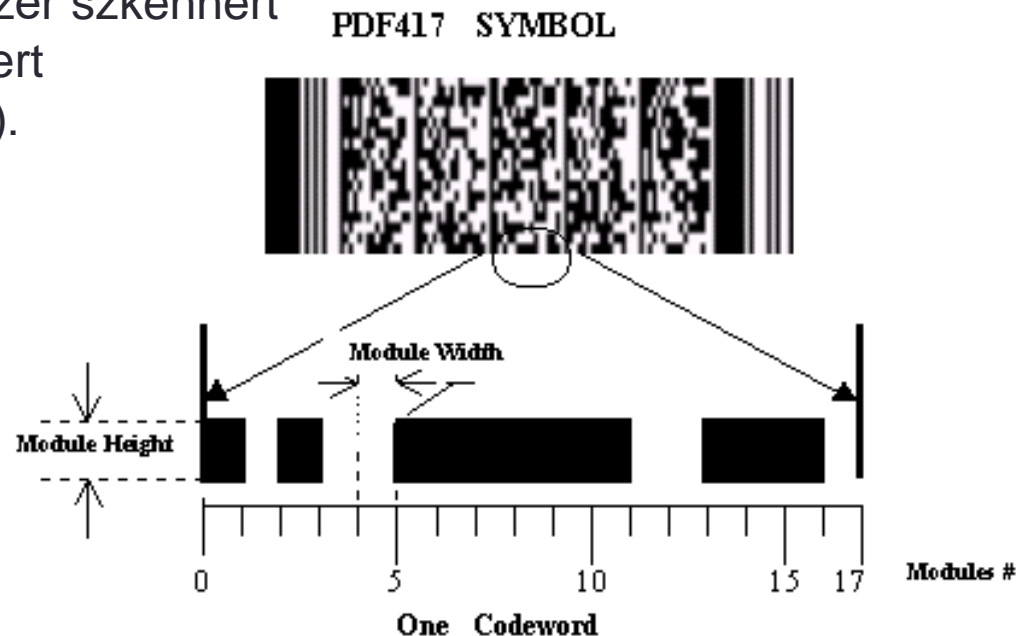
ABCxyz#\$%15z

PDF-417 2-dimeziós vonalkód, ami 1 800 nyomtatható ASCII karaktert, vagy 1 100 bináris karaktert tud tárolni.

A jel négyszögletű, a hosszassága növekedhet az adat mennyiségétől függően. Többszörös PDF-417 jelekre is lehet szétválasztani az adatokat, melyek összefűzhetőek, tehát nincs határa a PDF-417 csoport tartalom képességének.

A PDF-417 hasznos eljárás, főleg mikor az adatok a termékkel utaznak, például mikor az adatbázis nem elérhető. A PDF-417-at általában veszélyes anyagok megjelöléséhez, ujjlenyomatok és fényképek kódolásához főleg jogosítványokon, és műszaki cikkek részletezésére használják.

PDF-417 jelei kétdimenziós szkennert igényelnek;
vagy egy standard CCD-t vagy lézer szkennert
és egy speciális dekódoló-szoftvert
(a wand olvasó nem fog működni).



A **DataMatrix** egy két-dimenziós vonalkód, ami 1 - től 2 000 karaktert tud tárolni. A négyzet - alakú jel lehet 0.001 arasz nagyságútól 14 arasz is. A kód denzitása példájaként, 500 számos kód, mindössze egy arasz nagyságú DataMatrix. A felül látható DataMatrix, 20 ASCII karakter kódja.

Termékek és sorozat számok kódolhatóak DataMatrix-al.

A DataMatrix olvasásához csupán a két-dimenziós vonalkód olvasó használható, ami lézer, és CCD kamera technológiát igényel, tehát a lineáris vonalkód olvasók nem alkalmasak. DataMatrix jelek nyomtatásához a termál transzfer vonalkód nyomtató használható.



IR vonalkód

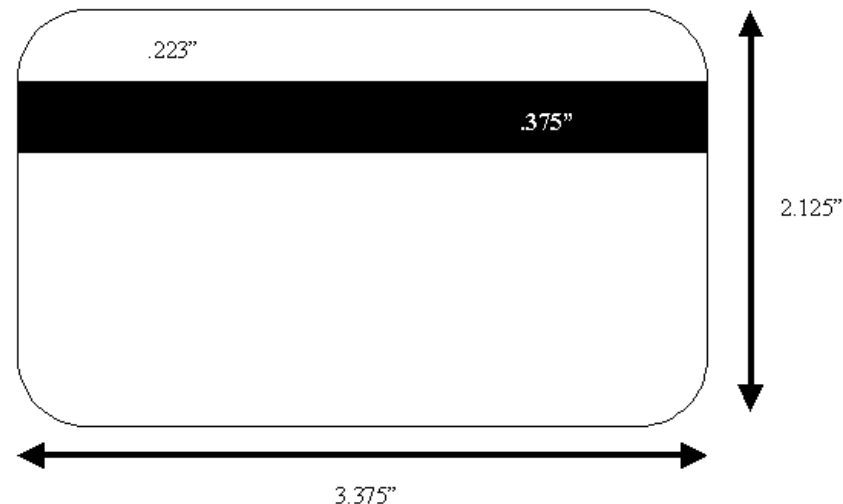
A kód nem látható, mert olyan réteggel vonják be, ami a fénynek csak az infra részét engedi át.

Használatához infra megvilágítás és olvasás szükséges.

Felhasználók beléptetése

Mágneskártya

A mágnescsík tartalma nem más, mint **mágneses mezők váltakozása**, amely lényegében minden olyan tulajdonsággal rendelkezik, amivel a hagyományos vonalkódok, csak éppen a kiolvasáshoz az egyszerű optikai leolvasás helyett **elektromágneses eljárás** szükséges.



Mágneskártya

A kártya működése egy nagyon egyszerű fizikai jelenségen alakul, miszerint ha egy mágneses mező és egy vezető relatív **mozog**, akkor a mező **feszültséget indukál a vezetőben**.

Ezt kihasználva a csíkon mágneses területeket alakítanak ki, amelyek így lehúzáskor az olvasóban feszültséget indukálnak és így olvassák ki a rajta lévő tartalmat.



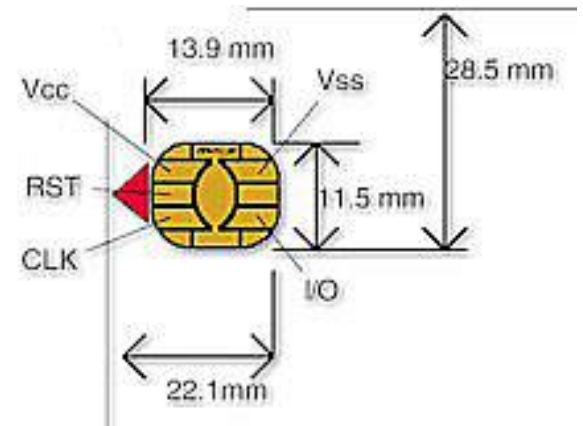
Chipkártya

A chipkártyák, vagy más néven intelligens kártyák nem hasonlíthatók technológiailag a mágneskártyákhoz. Mondhatni, hogy szinte **csak az alakjuk egyezik** meg, minden más tulajdonságuk teljesen eltérő.

A hordozó nem más, mint egy **műanyagból készített lap**.



Az általánosan használt chipek mérete 10-20 mm² és jellemző vastagsága kevesebb, mint 0,2 mm. Ezekkel a paraméterekkel biztosítani lehet, hogy a kártya a használat során fellépő hajlítási igénybevételnek ellenáll az elektronika sérülése nélkül.



Chipkártya

- **memóriakártyák:** azok a fajta kártyák, amelyek CPU-t nem tartalmaznak, de leg-alább 100 byte memóriakapacitással rendelkeznek. Tipikus példája a telefonkártya.
- **intelligens kártyák:** ezekre a kártyákra integrálnak egy mikrokontrollert, ami szempontunkból CPU-t, ami képes különböző műveletek végrehajtására, tehát lényegében egy programozható eszközzel állunk szemben. Ennek 3 fontos fajtája van, melyek különböző további részekre bonthatók:
 - **Érintkezéssel (contact) kártyák:** a legelterjedtebb fajta. A kártyakezelő eszközzel fizikailag is érintkezik a működése során.
 - **Érintkezésmentes (contactless) kártyák:** rádiós kapcsolattal kommunikál a kezelőegységgel
 - **Hibrid és kombi kártyák:** Az előző 2 fajta keresztezése, bizonyos esetekben 2 különböző chippel.

Biometriai azonosítás

Biometria

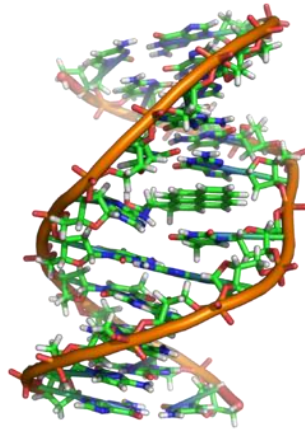
A biometria olyan testi, illetve viselkedésbeli **jellemvonások összessége**, melyek mérése alkalmas arra, hogy egy adott személyt **egyértelműen azonosítani** lehessen.

Minden egyes ember saját, **egyedi-egyszeri-megismételhetetlen** jellemezőkkel rendelkezik.

Biometria

A biometrikus azonosítás legfőbb előnye, hogy **magát az embert azonosítja**.

Mivel a biometrikus mérés az **adott személyre** egyedileg jellemző jegyeket azonosítja, gyakorlatilag kizárható a tévedés lehetősége.



Kézírás

A handwritten word "Signature" in a cursive script, written in black ink on a white background.

- Nem tiszta biometria azonosítás
- A kézírás nem igényel komolyabb olvasó berendezést
- Nem csak az írásképet, hanem a vonalvezetés dinamizmusát is ellenőrizni kell
- Hatékony azonosításhoz:
 - Betűk alakja, mérete, dőlése, kötése
 - Ékezetek formája, dőlése, betűhöz viszonyított helyzete
 - Tollemelés stb.
- Nem megbízható, mert a fizikailag és lelki állapot befolyásolhatja.

Ujjnyomat



- **Optikai**, melyek az ujjnyomat fodorszál-szerkezetét a látványa alapján rögzítik: általában látható/nem látható tartományba eső hullámhosszúságú fénnel megvilágítják, az ujjat, és "lefényképezik". Ezek az olvasók a bőr legfelső, egyben legsérülékenyebb felületét látják csak. Érzékenyek a **bőr szennyezettségére, a bőr minőségére** (száraz, repedezett, nedves, kopott).

Ujjnyomat



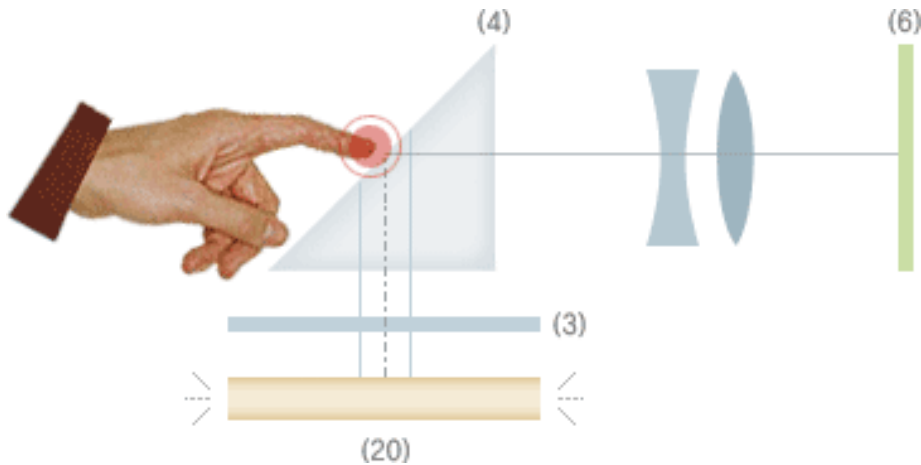
- A **kapacitív** és a **nyomásérzékelős** elven működő eszközök eltérő jeleket érzékelnek a bőrredők dombos vagy völgyes részein.

Ujjnyomat



- Az **ultrahangos** és a **rádiófrekvenciás** szenzorok az újra bocsátott és visszavert hang illetve rádiófrekvenciás jelek különbségei alapján térképezik fel a bőr redőzöttségét.

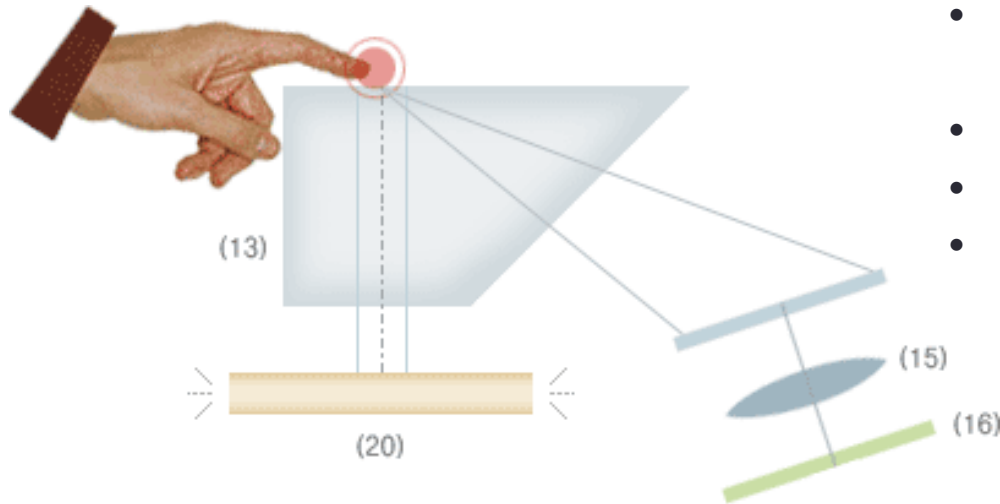
Abszorpciós elven működő optikai olvasók. A képalkotáshoz egy prizmát használnak.



- derékszögű háromszög prizma (4)
- fényforrás (20)
- diffúziós lemez (3)
- lencse-csoport és a képérzékelő (6)

A teljes **fényvisszaverődés megszűnik**, amennyiben az üvegfelülettel érintkezik a bőrfelület, a "hegygerinc". Itt elnyelődik a fény, mert kilép a prizmából. A fodorszálak fekete vonalként jelennek meg a lencserendszer utáni képalkotó felületen, általában CCD elemen.

Ennél a másik kialakításnál mintha **inverz képet** készítenénk: a völgy lesz sötét, és a heggyerinc világos: csak az ujjról visszaverődött fény jut el a CCD elemhez.

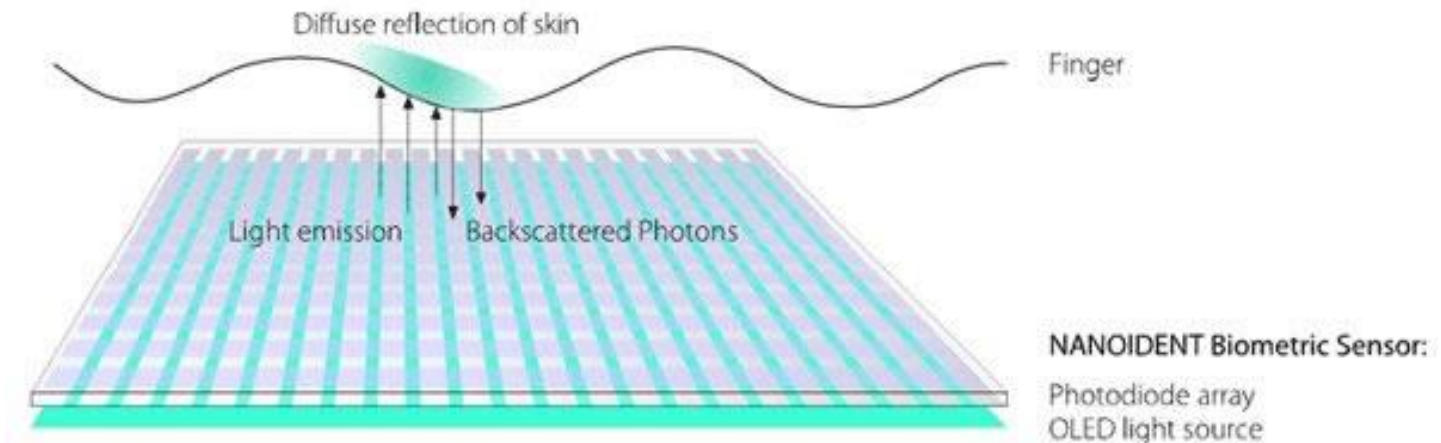


- négyszögletes-háromszög prizma (13)
- fényforrás (20)
- lencse csoport (15)
- képérzékelő (16)

Ez a kialakítás jobb, kontrasztosabb képet ad, de drágább. (Az elsőnél a teljes CCD felületre jutó összfény mennyiséget "csökkentjük", amikor az ujj érintkezik a felülettel, az utóbbinál a CCD-re csakis az ujjfelületről visszaverődött fény kerül.)

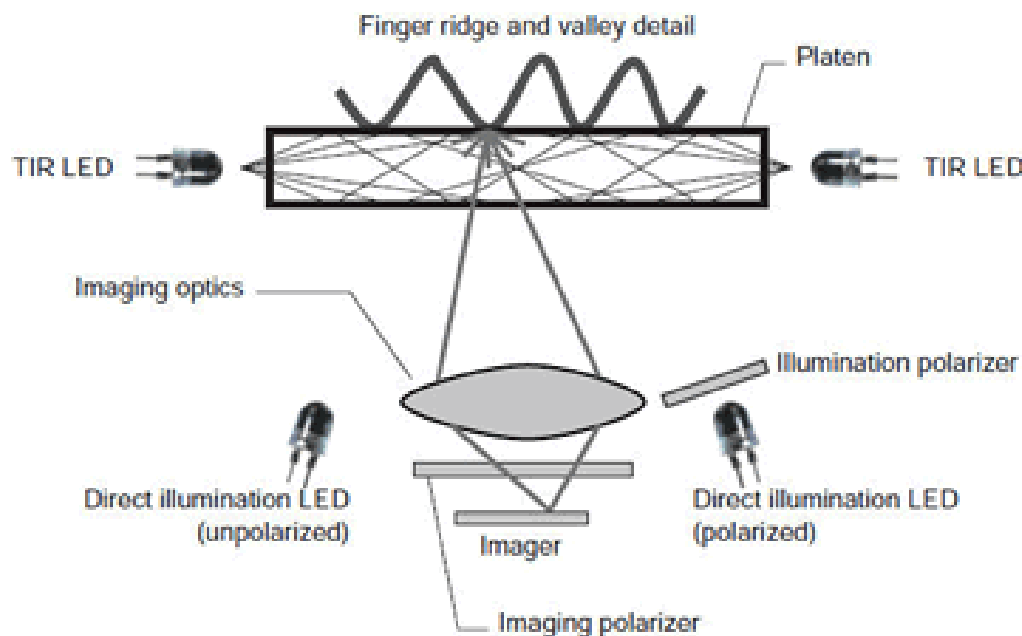
Touchless optikai olvasó

Vannak olyan optikai olvasók, melyeknél kihagyják a prizmát. Ezek közvetlenül, érintés nélkül fényképezik az ujjat. Használatánál figyelni kell az ujj-kamera távolságra.



InfraLED-ekkel világítják meg a speciális "touch" lapot két szélről, valamint szemből polarizált fénnel is.

Több képet készítenek, melyből egy MSI módszerrel szerkesztenek össze egy képet.

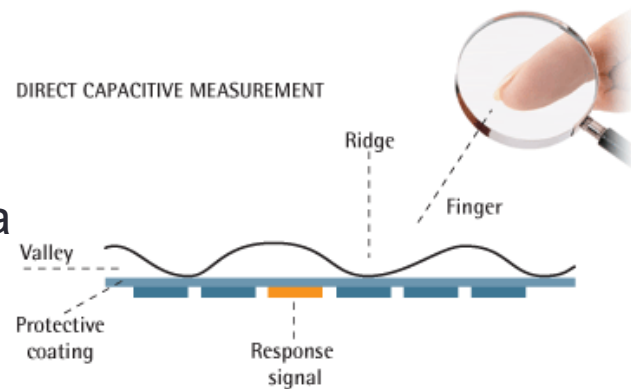


Kapacitív olvasók

A kapacitív olvasók a touch felület és a bőr közötti **elektrosztatikus kapacitást** mérik, és alakítják azt át képpé.

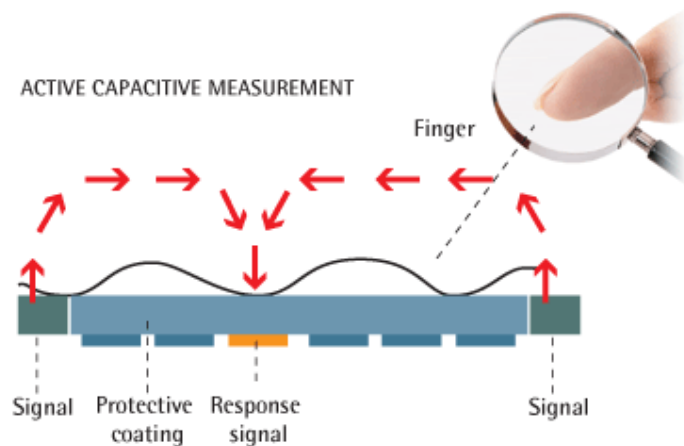
Passzív kapacitív olvasók

A bőr és a touch felület közötti kapacitást méri: mászt mér a völgyeknél, mert itt a bőr és a felület távolsága nagyobb, és mászt mér a hegygerincen.



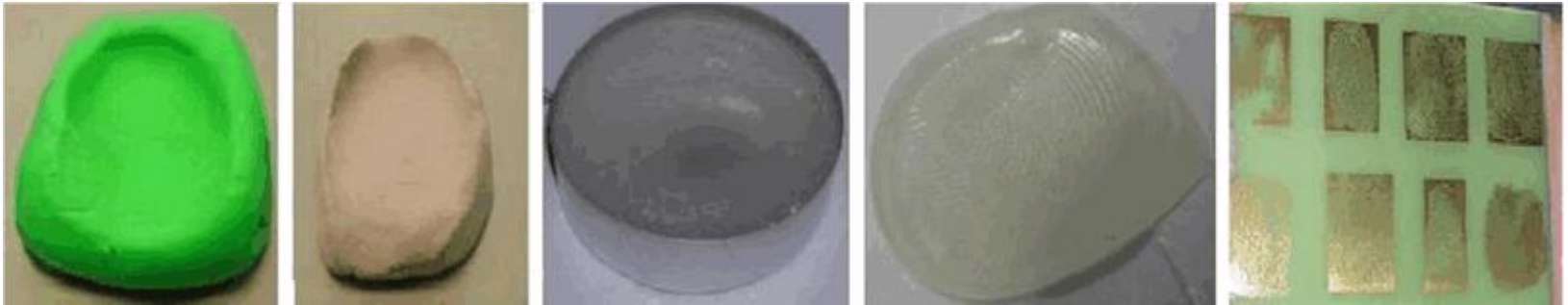
Aktív kapacitív olvasók

A kapacitás mérés előtt "töltést" kap az ujj is.



Ujjnyomat hamisítás

Mára a legtöbb olvasó érzékeli, hogyha "hamis ujjal" próbálják becsapni. (De vannak technológiára épülő olvasók, melyek eleve csak "élő" ujjról képesek felvételt készíteni.)



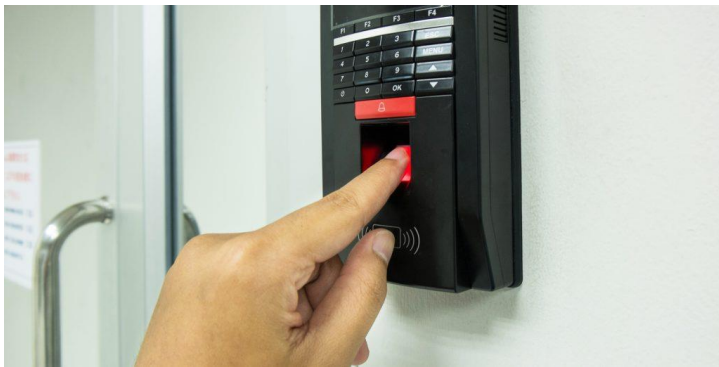
Ujjnyomat hamisítás

Az ellenőrzési módszerek a legkülönbözőbbek:

- érzékelik az "élő bőr" elektromos vezetőképességét,
- vér oxigén szintjét mérik
- pulzust mérik
- vizsgálják a véráramlást
- vagy a hamis ujjkészítéshez általában hasznát vegyszer szagát érzékelik
- az élő és a hamis ujjról alkotott képek között különbséget tudnak tenni az alkalmazott képalkotási technológia miatt

Alkalmazás

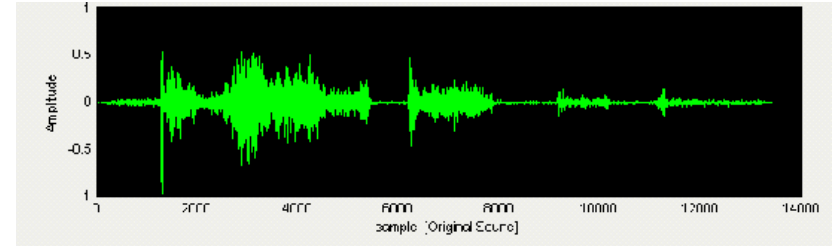
- Okmányok
- Telefon
- Beléptetés objektumba
- Azonosítás (bűnüldözés)



Hang azonosítás

- Az azonosítandó személy egy-egy rövid tárolt hangmintáját hasonlítják össze az éppen elmondott szöveggel.
- A beszédstílus jellemzői alapján történik az azonosítás több hangminta alapján.
- Hangminták összehasonlítására elektronikák az időtartományból frekvenciatartományba konvertálnak.

Hang azonosítás



Speaker recognition

Magának a hangnak az azonosítása szolgál, mely a beszélőre egyedileg jellemző.

A beszélő mindig ugyanazt mondja (szövegfüggő azonosítás), vagy szöveg független (bármit mondhat) azonosítás.

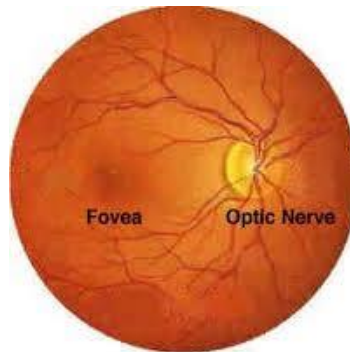
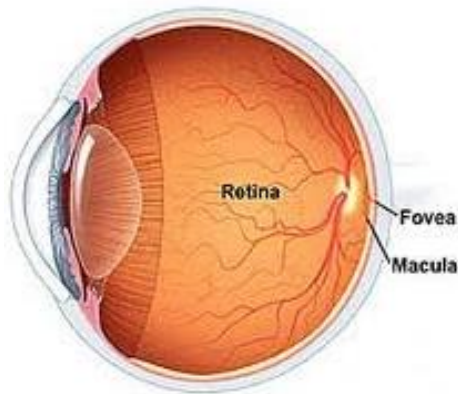
Speech recognition

A beszédnek az azonosítása/felismerése szolgál.

A speaker és speech recognition szinte adja magát a **multimódusos biometriára** (a kettő együttes alkalmazása).

Retina azonosítás

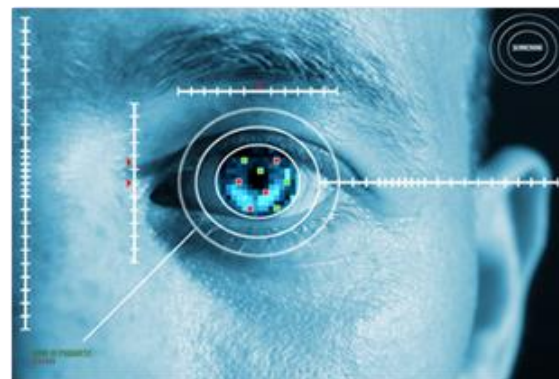
- Az emberi szem hátsó falán található vérerek mintázatán alapul.
- Nagy pontosságú.
- A felhasználók számára sokszor kellemetlen a mintavétel.
- Felléphetnek fertőzésveszélyek, cukorbetegség esetén az érhalózat sérülhet.



Írisz azonosítás



- A feldolgozás a zajszűréssel kezdődik.
(Zavarok: szempilla, szemhéj, pupilla, tükröződések)
- Utána történik meg az irisz struktúra felismerése, majd az Irisz kód előállítása.
- Az irisz kód egy polárkoordináta-rendszerben leírt sajátosságok sorozata, melyet a pupillától kifelé haladva körkörösén vesznek fel.
- Az irisz kód 256 byte hosszú (Dr. John Daugmann 1998 - 400 különböző tulajdonságot azonosított be)
- A minta idővel nem változik.



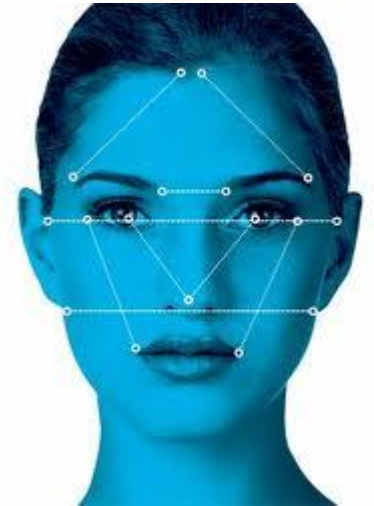
Arc felismerés

- Az azonosítást nehezíti a képminőség (megvilágítás) és az arckifejezés.
- Az arc **nem tartós** biometria jellemző, öregszik, betegségekre is érzékeny, és a nézőponttól erősen függ a geometriája.
- Jó azonosítási módszer: nem igényel együttműködést, nagy adatbázis áll rendelkezésre, messziről is, térfigyelő kamerákkal alkalmazható, eszközei olcsók, társadalmi elfogadottsága jó.



Arc felismerés elemzési módszerei

- **PCA**, (Principal Components Analysis), mely alapvetően a **frontális arckép** elemzését jelenti. (Önmagában legfeljebb 1/1000 a szelektivitása.)
- **LDA** (Linear Discriminant Analysis), **minta** osztályok és alosztályok létrehozásával és az azokba történő besorolással is vizsgál.
- **EBGM** (Elastic Bunch Graph Matching) a lineáris karakterisztika vizsgálat által nem megválaszolt **problémákra** próbál megoldást adni, mint pl. megvilágítás, pozíció (nem szemből), vagy arckifejezés). Lényegében a három dimenziós vizsgálatot jelenti.



Kéz geometria

- A kéz körvonalának geometriáját hasonlítja össze az előre felvett mintával. A felvételt olcsó, tömegcikknek számító CCD kamerával készíti.
- A tenyér felülete elég nagy, így viszonylag sok mérhető sajátosságot lehet találni rajta.



Kéz geometria

Az összehasonlításban a sok hasonló analóg sajátosság vesz részt:

- ujjak hossza,
- az ujj-izületek távolsága,
- az ujjak vastagsága,
- a tenyérszélességi adatai, hossza.
- Az adatok kevés byteon tárolhatók, így kicsi a template, és gyors az összehasonlítás.



Véredény azonosítás

- **Infra fény** megvilágított testrészek véredényeinek geometriai struktúráját elemzi, azonosítja. Előnyösen a kézen, a tenyéren és az ujjon.
- A véredények geometriai struktúrájának jellemzői **állandóak és egyediek**.
- Hamisításuk szinte **lehetetlen**, mert változtatni rajta nem lehet.
- Az azonosításhoz szükséges képet **csak eleve élő szervezet** ad (a képalkotáshoz kell a véráramlás is az erekben).
- Az infraledes fényforrás fénye behatol a kézfej bőrébe, és másképp verődik vissza az erekről és másképp a többi testszövetről.



Biometriai összehasonlítás

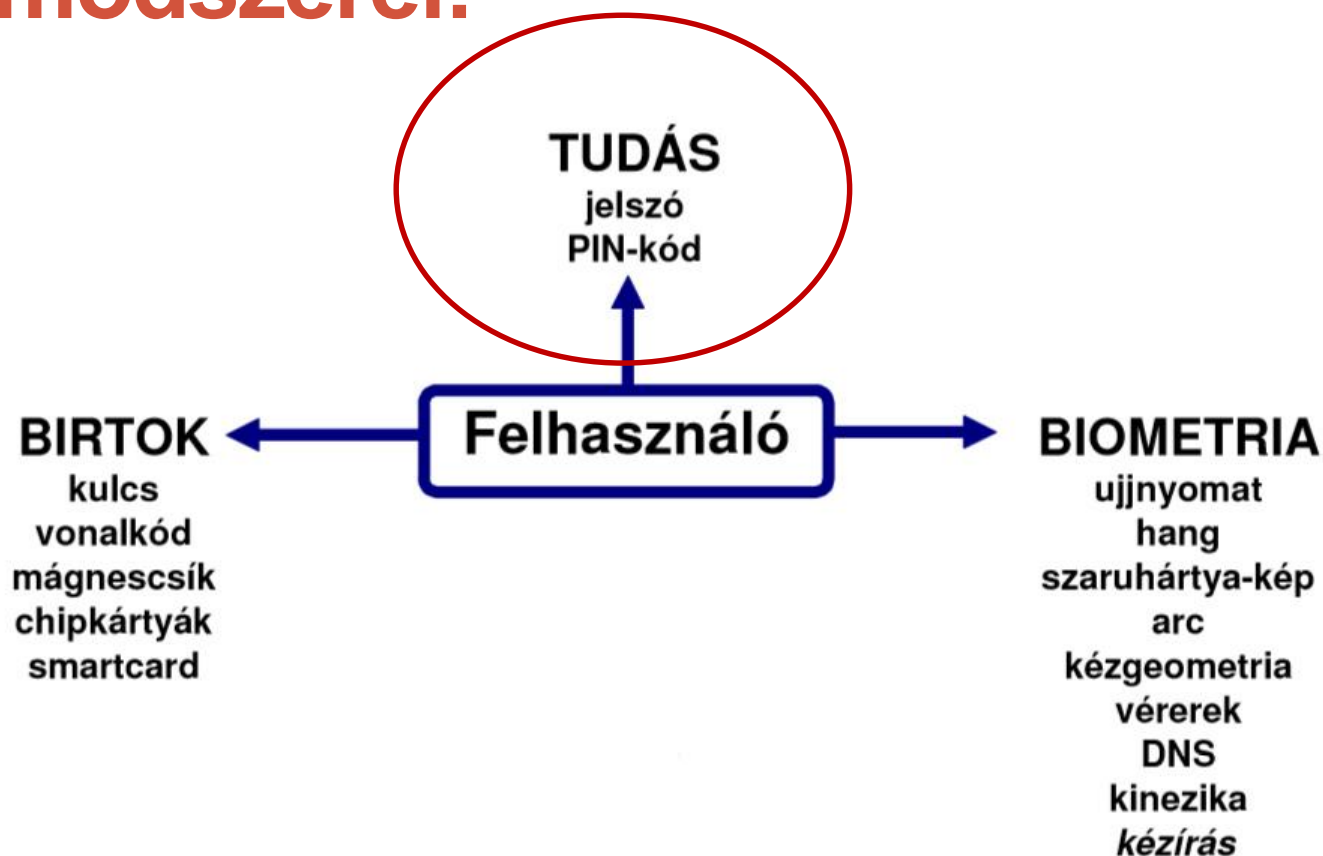
Hasonlítsuk össze néhány biometrikus rendszer FAR mutatóját (hány helyes azonosításra jut egy téves):

Arcfelismerés	2000:1
Hangazonosítás	500:1
Ujjlenyomat azonosítás	1 000 000:1
Íriszvizsgálat	10 000 000:1
Retinaazonosítás	10 000 000:1

Jelszavak szerepe, fontossága



A felhasználó-azonosítás alapmódszerei:



Tudás

- Használata egyszerű
- Olcsó
- Észrevétlenül másolható és tulajdonítható el
(*nincs visszajelzés ha más birtokába került*)
- Erős védelem megjegyezhetősége nehéz

A jelszó minőségek meghatározói

Hosszúság

minden egyes hozzáadott karakter növeli a jelszó értékét; 8 vagy annál több karakter minimum szükséges egy erős jelszóhoz, de 14 vagy annál több lenne az ideális.

Komplexitás

minél többféle karaktert alkalmazunk, annál nehezebb kitalálni a jelszót, használjuk a teljes billentyűzetet.

Könnyű észben tartani, nehéz kitalálni

úgy a legkönnyebb egy jelszót kezelni tartani, ha leírjuk valahová; habár ezt egyáltalán nem javasolt, de ha mégis így járnánk el, akkor rejtjük el biztonságos helyre!



Leggyakoribb jelszavak

- **123456** – Ez a leggyakrabban használt jelszó. És igen, létezik olyan, aki fontos adatok hozzáféréséhez használja ezt a jelszót.
- **jelszó** – A kreativitás csúcsa, amikor valaki ezt a szót választja jelszóként.
- **Fradi, fradi, fradi** – Gyakori, hogy valaki a kedvenc csapatát vagy játékosát választja jelszó gyanánt. Ezt sem túl nehéz kitalálni, ha valaki egy kicsit is ismeri az illetőt.
- **Petike** – Amikor a jelszó az illető keresztnevének becézése. Még durvább, ha még csak nem is becézi, hanem egyenesen beírja a nevét.
- **0740174156** – A ismerősöm telefonszáma, vagy saját szám.

Leggyakoribb jelszavak

- **asdf** – mindenki más kipróbálja
- **alma** – Vagy angolban a **monkey**. Mindenki kedvenc szavai, divatszavak bizonyos körökben.
- **ábécé** – Sorban az ábécé betűi. Ez sem egy nehéz rejtvény.
- **19820906** – Bármennyire is tudják, hogy ez nem egy jó ötlet, fantáziahiány miatt mégis rengetegen választják a születési dátumukat jelszó gyanánt.
- **szerelmünk neve** – Elsőre lehet, hogy jó ötletnek tűnik, de ezt az információt a neten keresgélve még egy ezer idegen is megszerezheti.

- Here are the worst passwords of 2017:
- 1. 123456 (rank unchanged since 2016 list)
- 2. password (unchanged)
- 3. 12345678 (up 1)
- 4. qwerty (up 2)
- 5. 12345 (down 2)
- 6. 123456789 (new)
- 7. letmein (new)
- 8. 1234567 (unchanged)
- 9. football (down 4)
- 10. iloveyou (new)
- 11. admin (up 4)
- 12. welcome (unchanged)
- 13. monkey (new)
- 14. login (down 3)
- 15. abc123 (down 1)
- 16. starwars (new)
- 17. 123123 (new)
- 18. dragon (up 1)
- 19. passw0rd (down 1)
- 20. master (up 1)
- 21. hello (new)
- 22. freedom (new)
- 23. whatever (new)
- 24. qazwsx (new)
- 25. trustno1 (new)

Hogyan védj a jelszavadat?

- **Ne mond el és ne add oda másnak!** Tartsd a jelszavaidat távol a családotól, barátaitól és a gyerekeidtól, akik esetleg továbbadhatnák másnak. Légy elővigyázatos a jelszó- emlékeztető kérdésekkel: ne válassz olyan kérdést, amely mások által is kitalálható.
- **Vigyázz a leírt vagy mentett jelszavakra!** Ne őrizz jelszavakat fájlokban a számítógépeden, ugyanis itt keresik először. Ne tedd a jelszavadat a pénztárcádba, se a billentyűzet alá.
- **Sose írd meg a jelszavadat e-mailben, és ne válaszolj a jelszavadat elkérő levelekre!** Ha valaki e-mailben kéri el a jelszavadat, akkor szinte bizonyosan valamilyen átverésre, csalásra kell gondolni. Ez érvényes az általad megbízhatónak tartott cégekre/személyekre is, ugyanis a csalók könnyen álcázhatják magukat más valakinek.

Hogyan védj a jelszavadat?

- **Ne írd be a jelszavadat olyan számítógépen, amelyet nem ismersz!** Minden olyan számítógép, amely internetkávézókban, laborokban, osztott rendszereken, konferenciákon, reptereken stb. található nem tekinthető biztonságosnak, mert nem tudhatjuk, milyen szoftverek rögzítik minden billentyűleütésünket. Ne használjuk ezeket a számítógépeket internetes utalásra, e-mailezésre, vagy bármi olyan művelethez, ahol fontos adatokhoz férünk hozzá.
- **Használj több mint egy jelszót!** Legyen különböző jelszavad a különböző webes szolgáltatásokhoz. Gondolj bele, ha az egyik szolgáltatónál kitudódna a jelszavad, akkor azzal mindenhová beléphetnének.

Az erős jelszavak:

- *legalább* **hét karakterből** állnak.
- kis- és nagybetűket, számokat és a második és a hatodik karakter között egy szimbólumot tartalmaznak.
- **véletlenszerű** karaktersorozatnak tűnnek.
- nem tartalmaznak **ismétlődő** karaktereket.

Az erős jelszavak:

- nem tartalmaznak **egymás után következő** karaktereket, például 1234, abcd vagy qwerty.
- nem tartalmaznak mintákat, témákat vagy (valamilyen nyelven) **felismerhető** teljes szavakat.
- nem tartalmaznak hasonló betűket **helyettesítő** számokat vagy szimbólumokat, például \$ jelet az S betű helyett, vagy az 1 számot az l karakter helyett, mivel ezek segítik a jelszó kitalálását.
- nem tartalmazhatják az internetre vagy egy hálózatba történő belépéshez használt felhasználói nevének egyetlen részletét sem.

Jelszó használat

Mobil eszközök

- **PIN kód**

Egy négy számjegyből álló kód 10 ezer lehetőséget rejt, azonban a felhasználók 15%-a ebből csupán 10-et használ (1234, 2222, 0000, 1991...).

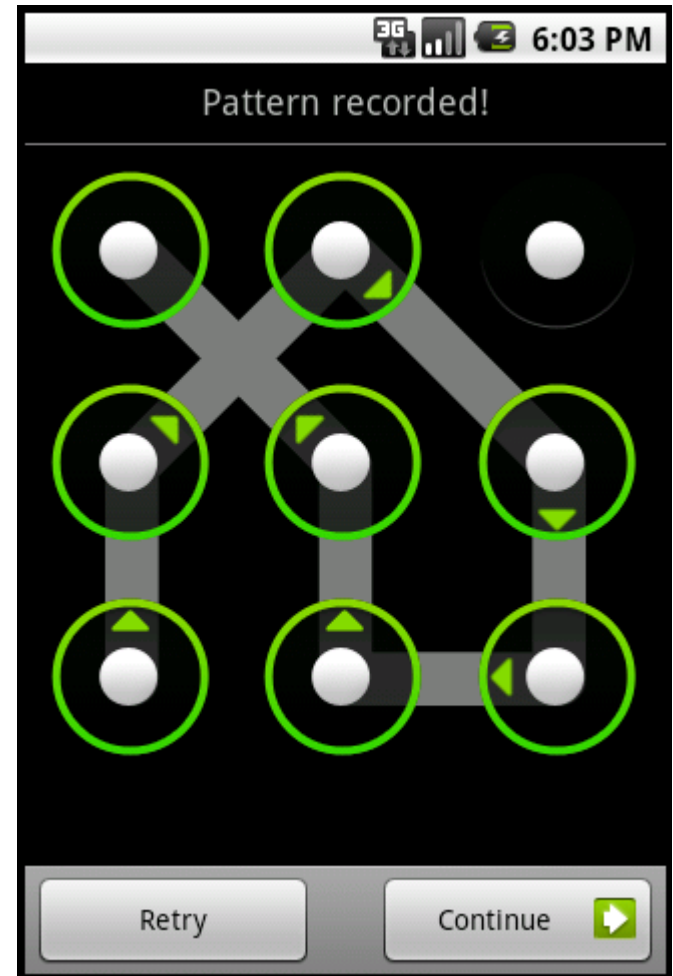


Mobil eszközök

- **Android belépési minta**

9 pont elhelyezve egy négyzetesen, egy megadott útvonalat kell bejárni az újjunkkal.

Hátrány: Az újaink nyomot hagyhatnak és könnyen megfejthető a kód



BIOS

A **BIOS** az angol **Basic Input/Output System** kifejezés rövidítése, ami magyarul alapvető bemeneti/kimeneti rendszert jelent, és a számítógép szoftveres és hardveres része közötti interfész megvalósítására szolgál.



- Hardverek ellenőrzése (POST – Power-On Self Test)
- Hardverek vezérlőinek betöltése
- Rendszerkonfiguráció
- Az operációs rendszer merevlemezről, floppyról, SCSI egységről, USB-ről, hálózati kártyáról vagy egyéb tárolóról való elindítása
- BIOS interfész biztosítása az operációs rendszer számára

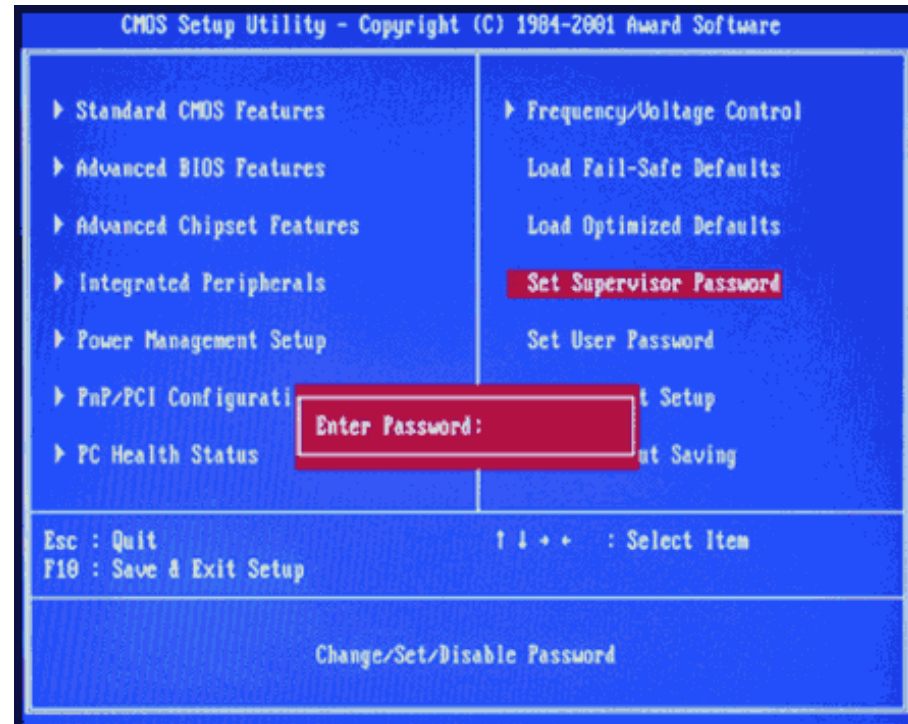
BIOS jelszó

User password

A beállításokhoz fér hozzá

Supervisor password

A beállításokhoz vagy épp a bootoláshoz ad jelszót



BIOS jelszó

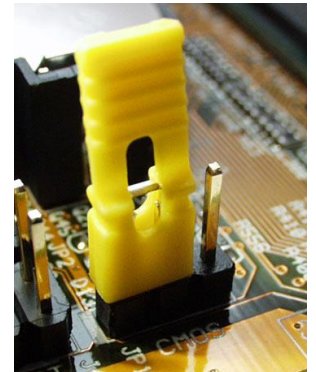
A boot-olás előtt kér
jelszót



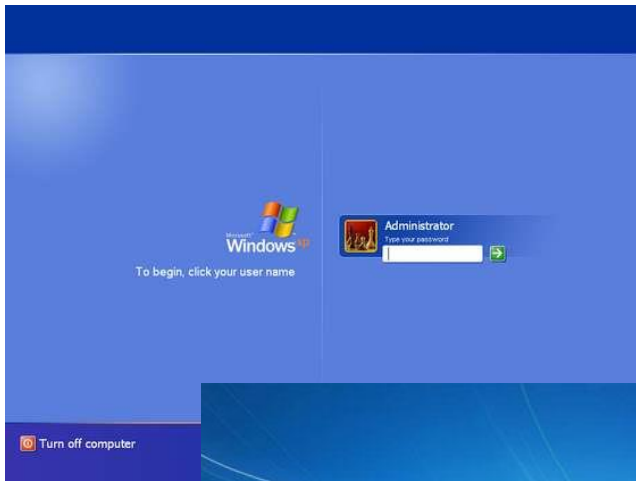
BIOS jelszó

A jelszó „kiütése” egy ismert egyszerű hardveres művelettel megoldható.

Ezért fontos a **számítógépek házainak biztonságos lezárása!!!!**

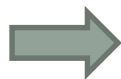


Operációs rendszer belépési jelszava



Operációs rendszer belépési jelszava

Vezérlőpult



Felhasználói fiókok és családbiztonság

Fióktípus módosítása

Családbiztonság beállítása bármely felhasználóhoz



A fiókhoz tartozó név módosítása

A jelszó módosítása

Családbiztonság beállítása

Fióktípus módosítása

Fiók törlése

Másik fiók kezelése



Göcs László - GAMF

Helyi fiók

Jelszóvédett

Fontos, hogy a **VENDÉG** Fiók tiltva legyen

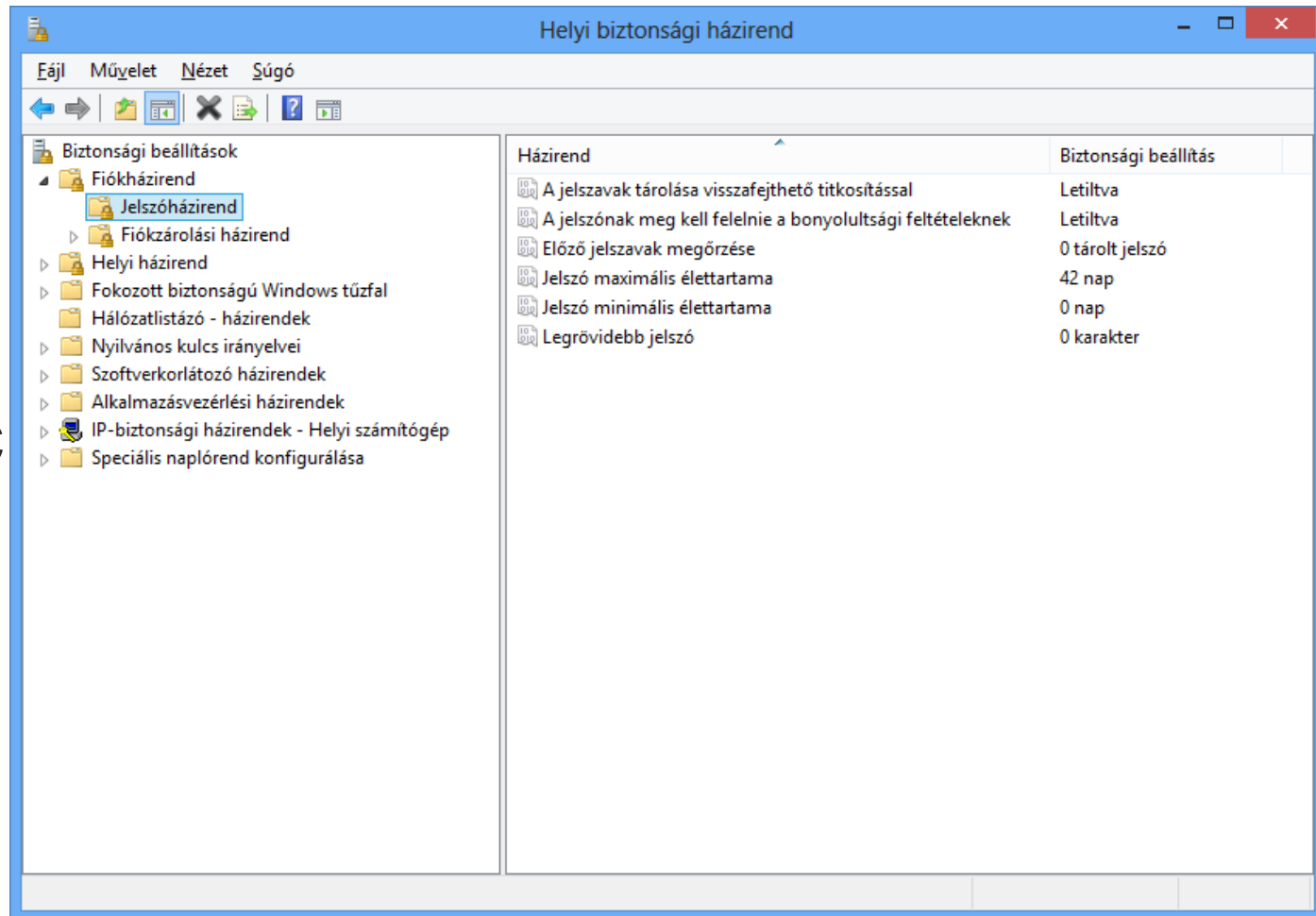


Vendég

Vendégfiók letiltva

Helyi biztonsági házirend beállítása

secpol.msc



Jelszó Bonyolultsági feltételek

- **Legrövidebb jelszó:** 1..14 (0-nem kell jelszó)

Meghatározza, hogy a felhasználói fiókokhoz tartozó jelszavaknak legalább hány karakterből kell állniuk.

- **Minimális élettartam:** 1..999 (0-azonnal változtatható)

Ez a biztonsági beállítás azt az időtartamot adja meg (napokban), ameddig egy jelszót kötelező használni, mielőtt a felhasználó megváltoztathatná azt.

Jelszó Bonyolultsági feltételek

- **A jelszónak meg kell felelnie a bonyolultsági feltételeknek**
 - Nem tartalmazhatják a felhasználói fiók nevét vagy a felhasználó teljes nevének két egymás utáni karaktert meghaladó részletét
 - Legalább hat karakter hosszúságúnak kell lenniük
 - Tartalmazniuk kell az alábbi négy kategória közül legalább háromnak az elemeit:
 - Angol nagybetűs karakterek (A-tól Z-ig)
 - Angol kisbetűs karakterek (a-tól z-ig)
 - Az alapvető 10 számjegy (0-tól 9-ig)
 - Nem betű jellegű karakterek (például !, \$, #, %)

A bonyolultsági feltételeknek a jelszavak létrehozásakor vagy módosításakor kell érvényesülniük.

Jelszó Bonyolultsági feltételek

- **Maximális élettartam:** 1..42 (0-soha nem jár le)

Ez a biztonsági beállítás azt az időtartamot határozza meg (napokban), ameddig egy jelszó használható, mielőtt a rendszer felszólítaná a felhasználót a megváltoztatására

- **Előző jelszavak megőrzése:** 0..24 (alapért.:1)

Ez a biztonsági beállítás meghatározza, hogy hány új egyedi jelszó hozzárendelése szükséges egy felhasználói fiókhoz egy régi jelszó újrafelhasználása előtt. Az értéknek 0 és 24 jelszó között kell lennie.

www.strongpasswordgenerator.com

Strong Password Generator

Strong Password Generator

Password length: ▼

☒ Punctuation (!, ", £, \$, %, and so on)

Generate strong password

Your new password:

6enB]3?3F1

Remember your new password as:

6 echo november BRAVO] 3 ? 3 FOXTROT 1

Ste

Minőség

Hidege

www.passwordmeter.com

Test Your Password		Minimum Requirements			
Password:	<input type="password"/>	<ul style="list-style-type: none">• Minimum 8 characters in length• Contains 3/4 of the following items:<ul style="list-style-type: none">- Uppercase Letters- Lowercase Letters- Numbers- Symbols			
Hide:	<input checked="" type="checkbox"/>				
Score:	<div><div></div>0%</div>				
Complexity:	Too Short				

Additions		Type	Rate	Count	Bonus
✗	Number of Characters	Flat	$+(n*4)$	<input type="text" value="0"/>	0
✗	Uppercase Letters	Cond/Incr	$+((len-n)*2)$	<input type="text" value="0"/>	0
✗	Lowercase Letters	Cond/Incr	$+((len-n)*2)$	<input type="text" value="0"/>	0
✗	Numbers	Cond	$+(n*4)$	<input type="text" value="0"/>	0
✗	Symbols	Flat	$+(n*6)$	<input type="text" value="0"/>	0
✗	Middle Numbers or Symbols	Flat	$+(n*2)$	<input type="text" value="0"/>	0
✗	Requirements	Flat	$+(n*2)$	<input type="text" value="0"/>	0

Deductions		Type	Rate	Count	Bonus
✓	Letters Only	Flat	$-n$	<input type="text" value="0"/>	0
✓	Numbers Only	Flat	$-n$	<input type="text" value="0"/>	0
✓	Repeat Characters (Case Insensitive)	Comp	-	<input type="text" value="0"/>	0
✓	Consecutive Uppercase Letters	Flat	$-(n*2)$	<input type="text" value="0"/>	0
✓	Consecutive Lowercase Letters	Flat	$-(n*2)$	<input type="text" value="0"/>	0
✓	Consecutive Numbers	Flat	$-(n*2)$	<input type="text" value="0"/>	0
✓	Sequential Letters (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
✓	Sequential Numbers (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0
✓	Sequential Symbols (3+)	Flat	$-(n*3)$	<input type="text" value="0"/>	0

Legend	
⚡	Exceptional: Exceeds minimum standards. Additional bonuses are applied.
✓	Sufficient: Meets minimum standards. Additional bonuses are applied.
⚠	Warning: Advisory against employing bad practices. Overall score is reduced.
✗	Failure: Does not meet the minimum standards. Overall score is reduced.

Jelszó tárolás

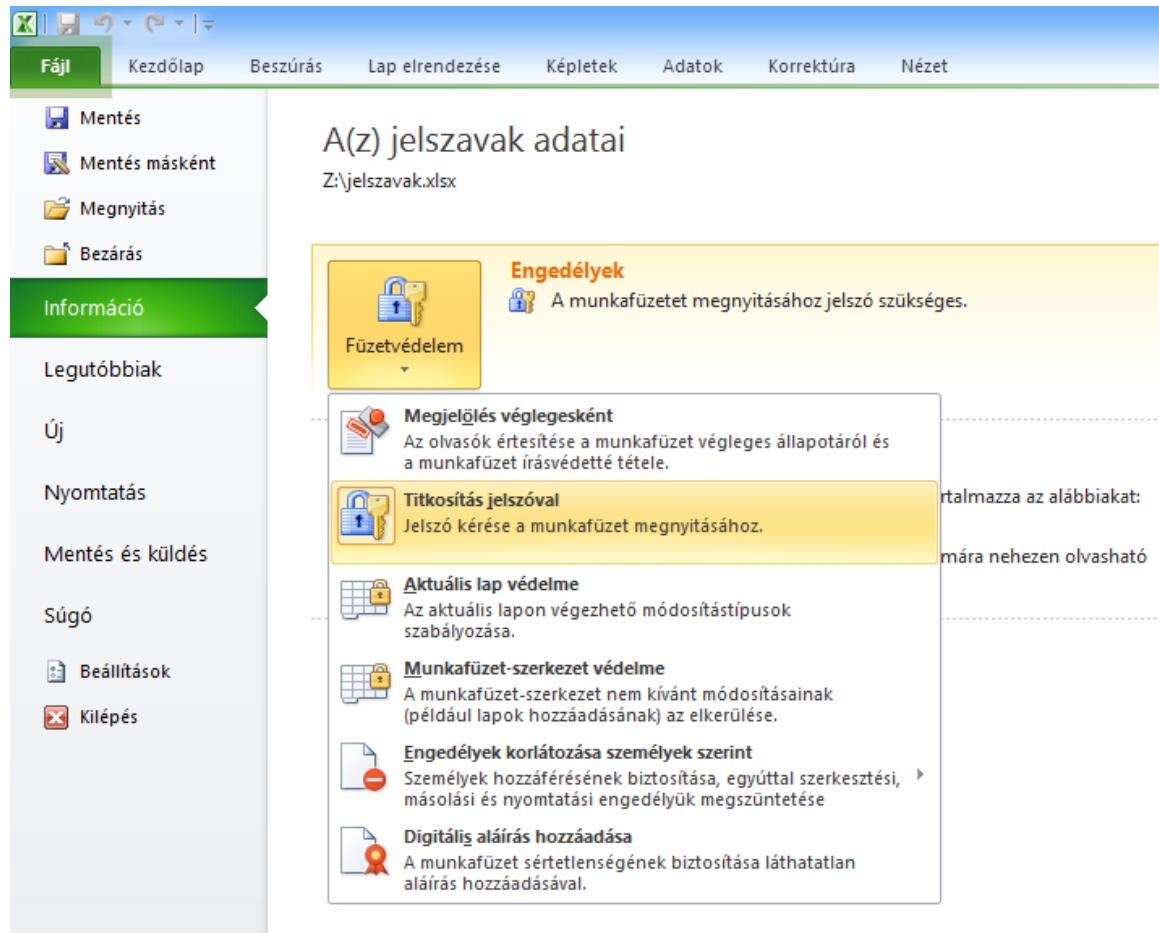
- **Fejben tárolva**

Elfelejtődik, vagy ha túl bonyolult akkor nehéz megjegyezni. Több jelszónál még több probléma.

- **Fájlban tárolva (pl XLS)**

Jelszavas védelem a fájl megnyitására!

Fájl jelszavazás



Jelszótörő módszerek

- **Brute Force** (nyers erő)

Módszeresen az összes lehetséges jelkombinációt kipróbálja.

- Csak akkor, ha minden más eljárás eredménytelen
- Nagy teljesítményű gépet igényel
- A jelszó hosszától, illetve a használt jelektől függően nagyon sok időre van szükség
- A végeredmény sem biztos



Jelszótörő módszerek

- **Szótár alapú**

A legtöbb felhasználó a hétköznapi nyelvezetből, magánéletéből használja a szavakat, vagy szótöredékeket.

- Lényegesen kevesebb időt igényel
- Nem vezet mindig eredményre



Jelszótörés jogi háttere

Törvénytelen, ha valaki megpróbál engedély nélkül jelszófeltörő program segítségével olyan állományok tartalmához jutni, amelyekhez nincs jogosultsága.

10 karakter kombinációjából alkotott jelszó – 0123456789

Innen látható mennyire rossz ötlet csak számokat használni a jelszóban.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	100	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	1000	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
4	10 000	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
5	100 000	10 mp	azonnal	azonnal	azonnal	azonnal	azonnal
6	1 millió	1½ perc	10 mp	azonnal	azonnal	azonnal	azonnal
7	10 millió	17 perc	1½ perc	1½ perc	azonnal	azonnal	azonnal
8	100 millió	2¾ óra	17 perc	1½ perc	10 mp	azonnal	azonnal
9	1 milliárd	28 óra	2¾ óra	17 perc	1½ perc	10 mp	azonnal

26 karakter kombinációjából alkotott jelszó –

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

Most pedig lássuk, mennyire nehéz kitalálni egy olyan jelszót, amelyben csak az angol ábécé kis- vagy nagybetűit találhatók.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	676	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	17 576	2 mp	azonnal	azonnal	azonnal	azonnal	azonnal
4	456 976	46 mp	5 mp	azonnal	azonnal	azonnal	azonnal
5	11,8 millió	20 perc	2 perc	12 mp	azonnal	azonnal	azonnal
6	308,9 millió	8½ óra	51½ perc	5 perc	30 mp	3 mp	azonnal
7	8 billió	9 nap	22 óra	2¼ óra	13 perc	1¼ perc	8 mp
8	200 billió	242 nap	24 nap	2½ nap	348 perc	35 perc	3½ perc
9	5,4 trillió	17 év	21 hónap	63 nap	6¼ nap	15 óra	1½ óra
10	141 trillió	447 év	45 év	4½ év	163 nap	16 nap	39¼ óra
12	95 quadrillió	302 603 év	30 260 év	3026 év	302 év	30 év	3 év
15	1,6 sextillió	53 trillió év	532 millió év	53 millió év	5 millió év	531 855 év	53 185 év
20	19,9 octillió	63 quadrillió év	6,3 quadrillió év	631 trillió év	63,1 trillió év	6,3 trillió év	631 billió év

36 karakter kombinációjából alkotott jelszó –

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789

A teljes angol ábécé (csak kis vagy csak nagybetűk) és a számok együttes használatával az eredmény csak egy picit jobb.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	1 296	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	46 656	4 mp	azonnal	azonnal	azonnal	azonnal	azonnal
4	1,6 millió	2½ perc	16 mp	1½ mp	azonnal	azonnal	azonnal
5	60,4 millió	1½ óra	10 perc	1 perc	azonnal	azonnal	azonnal

52 karakter kombinációjából alkotott jelszó –

AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz

Most nézzük mi történik, ha vegyítjük a kis és nagybetűket.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombináció	A típus	B típus	C típus	D típus	E típus	F típus
2	2704	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	140 608	14 mp	2 mp	azonnal	azonnal	azonnal	azonnal
4	7,3 millió	12½ perc	1¼ perc	8 mp	azonnal	azonnal	azonnal
5	380 millió	10½ óra	1 óra	6 perc	38 mp	4 mp	azonnal
6	19 billió	23 nap	2¼ nap	5½ óra	33 perc	3¼ perc	19 mp
7	1 trillió	3¼ év	119 nap	12 nap	28½ óra	3 óra	7 perc
8	53 trillió	169½ év	17 év	1½ év	62 nap	6 nap	15 óra
9	2,7 quadrillió	8815 év	881 év	88 év	9 év	322 nap	32 nap

96 karakter kombinációjából alkotott jelszó – !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~
0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz

Kis- és nagybetűk, számok, valamint néhány gyakori szimbólum használata a jelszóban.

Jelszó		A feltöréshez használt számítógép típusa					
Hossz	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
2	9 216	azonnal	azonnal	azonnal	azonnal	azonnal	azonnal
3	884 736	88½ mp	9 mp	azonnal	azonnal	azonnal	azonnal
4	85 millió	2¼ óra	14 perc	1½ perc	8½ mp	azonnal	azonnal
5	8 billió	9½ nap	22½ óra	2¼ óra	13½ perc	1¼ perc	8 mp
6	782 billió	2½ év	90 nap	9 nap	22 óra	2 óra	13 perc
7	75 trillió	238 év	24 év	2½ év	87 nap	8½ nap	20 óra
8	7,2 quadrillió	22 875 év	2287 év	229 év	23 év	2¼ év	83½ nap

Példák

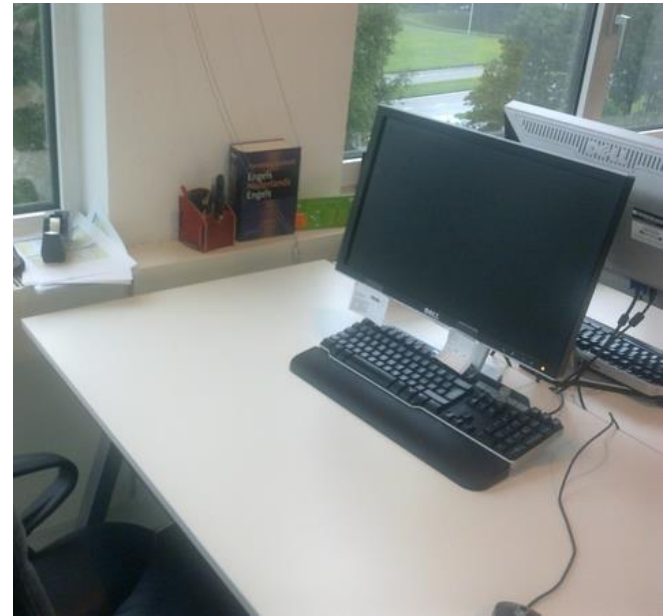
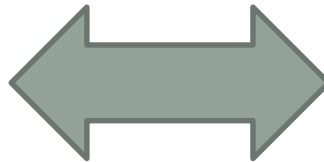
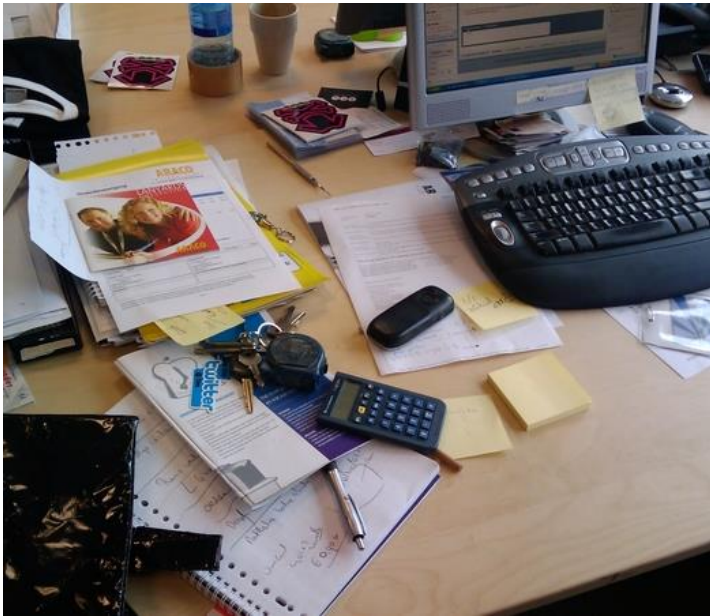
Most pedig lássunk néhány konkrét példát jelszavakra!

Jelszó		A feltöréshez használt számítógép típusa					
Jelszó	Kombinációk	A típus	B típus	C típus	D típus	E típus	F típus
Iacika	308,9 millió	8½ óra	51½ perc	5 perc	30 mp	3 mp	azonnal
P3terke	3,5 trillió	11 év	1 év	41 nap	4 nap	10 óra	58 perc
B33r&Mug	7,2 quadrillió	22 875 év	2287 év	229 év	23 év	2¼ év	83½ nap

A tesztekben használt számítógép-típusok jellemzői

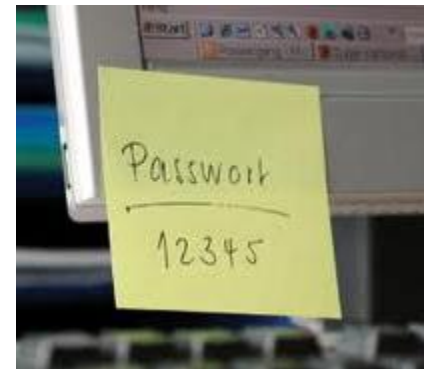
- **A típus** (10 000 jelszó/mp) – Tipikusan egy Microsoft Office jelszó feltörésére használható Pentium 100-as gép.
- **B típus** (100 000 jelszó/mp) – Tipikusan egy Windows Password Cache (.pwl) jelszó feltörésére használható Pentium 100-as gép.
- **C típus** (1 000 000 jelszó/mp) – Tipikusan egy ZIP vagy ARJ jelszó feltörésére használható Pentium 100-as gép.
- **D típus** (10 000 000 jelszó/mp) – Gyors PC, duplamagos processzorral.
- **E típus** (100 000 000 jelszó/mp) – Munkaállomás vagy több PC együttműködve.
- **F típus** (1 000 000 000 jelszó/mp) – Tipikus közepes vagy nagyméretű elosztott számítógép, szuperszámítógép.

Clean Desk Policy (CDP) - Tiszta Asztal Politika



Clean Desk Policy (CDP) - Tiszta Asztal Politika

- **Belépési azonosító és jelszó**
 - Papíralapon (Post-It, regisztrációs lap kinyomtatva)
 - Hardverre írva (monitor, billentyűzet)
- **Személyes információk**
 - Amiből a jelszavak megfejthetők, kitalálhatóak
- **Otthoni/Céges dokumentumok, leírások**
- **Mobiltelefon**



Erős jelszó példa

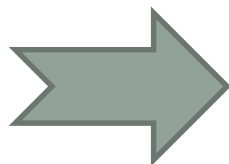
- **Találj ki egy mondatot, amit könnyen észben tudsz tartani!**
Például: *A kisfiam Péter ma pontosan két éves.*
- **Alakítsd a mondatot jelszóvá!**
Használd minden szó első betűjét, hogy egy betűsorozatot gyárts: *akpmpke*
- **Bonyolítsd a szöveget egy kis fantáziával!**
Vegyítsd a kis- és nagybetűket, használj számokat a betűk helyett. Például: *AkPmp2e*
- **Vonj be speciális karaktereket!**
Használd olyan szimbólumokat, amelyek hasonlítanak bizonyos betűkhöz: *Ak#P?mp%2e!*
- **Tartsd titokban a jelszavadat!**

KeePass



Ingyenes, nyílt forráskódú jelszó menedzselő program.
Minden jelszót 1 adatbázisban lehet tárolni mesterkulcs segítségével.

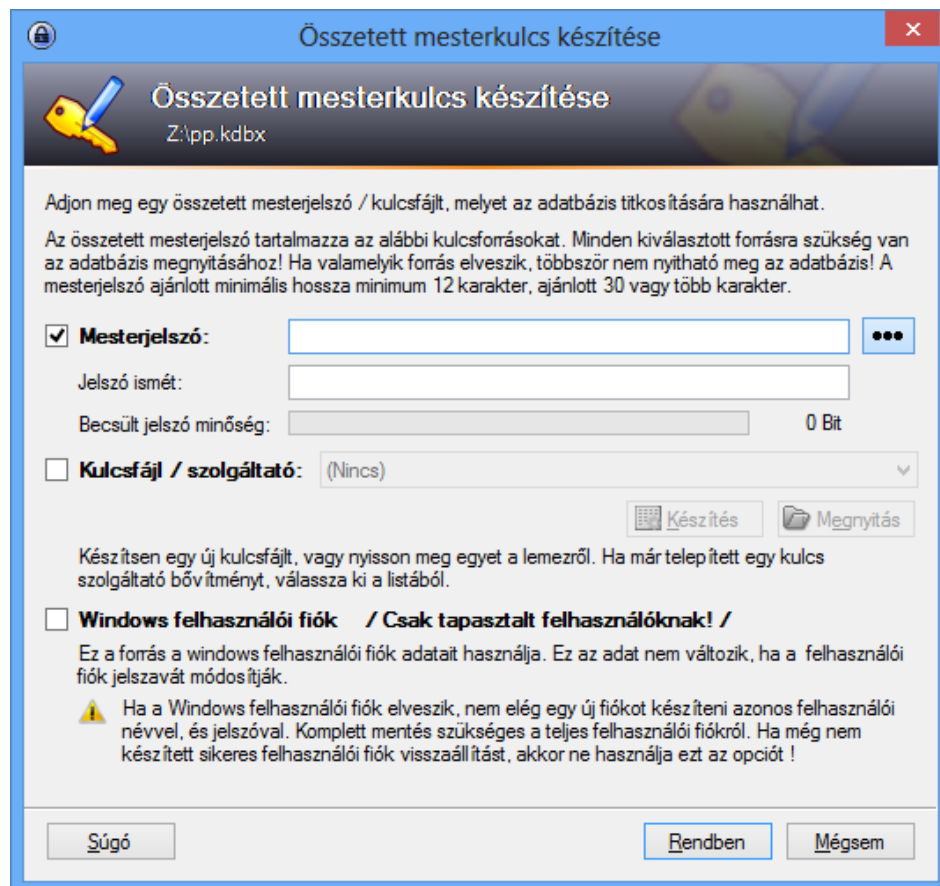
1 db Mesterkulcs



- Felhasználói jelszavak
- Email account-ok
- Windows hálózati belépések
- Webes jelszavak

KeePass

Új adatbázis létrehozáshoz
egy **mesterkulcs**
szükséges



The screenshot shows the 'Összetett mesterkulcs készítése' (Composite Master Key Creation) dialog box in KeePass. The title bar includes a lock icon and the text 'Összetett mesterkulcs készítése'. The main header area features a key icon and the title 'Összetett mesterkulcs készítése' with the file name 'Z:\pp.kdbx' below it.

The main text area contains the following instructions:

Adjon meg egy összetett mesterjelszó / kulcsfájlt, melyet az adatbázis titkosítására használhat.

Az összetett mesterjelszó tartalmazza az alábbi kulcsforrásokat. Minden kiválasztott forrásra szükség van az adatbázis megnyitásához! Ha valamelyik forrás elveszik, többször nem nyitható meg az adatbázis! A mesterjelszó ajánlott minimális hossza minimum 12 karakter, ajánlott 30 vagy több karakter.

The dialog has two main sections for selecting sources:

- Mesterjelszó:** This section is checked. It includes a text input field, a 'Jelszó ismét:' (Repeat password) field, and a 'Becsült jelszó minőség:' (Estimated password quality) field showing '0 Bit'. There is a three-dot menu icon to the right of the first input field.
- Kulcsfájl / szolgáltató:** This section is unchecked. It includes a dropdown menu currently showing '(Nincs)' (None).

Below these sections are two buttons: 'Készítés' (Create) and 'Megnyitás' (Open).

Below the buttons, there is a note: 'Készítsen egy új kulcsfájlt, vagy nyisson meg egyet a lemezeiről. Ha már telepített egy kulcs szolgáltató bővítményt, válassza ki a listából.'

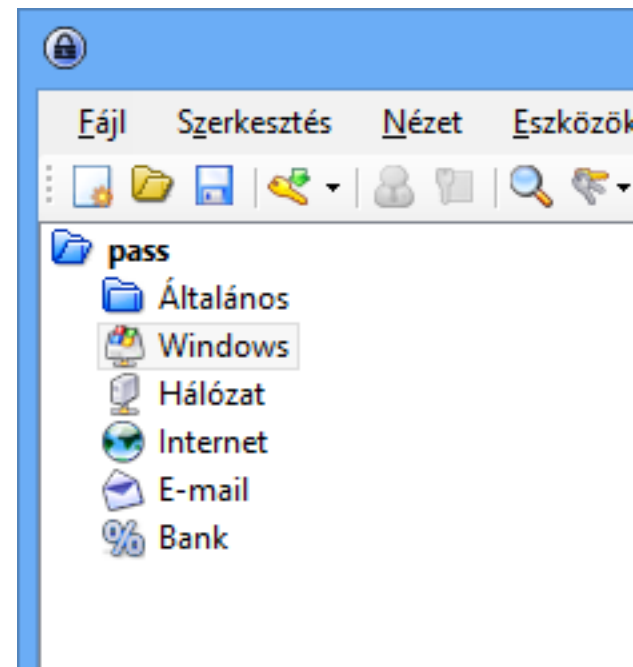
At the bottom, there is a section for 'Windows felhasználói fiók / Csak tapasztalt felhasználóknak!' (Windows user account / Only for experienced users!). It is unchecked. The text below it says: 'Ez a forrás a windows felhasználói fiók adatait használja. Ez az adat nem változik, ha a felhasználói fiók jelszavát módosítják.'

Below this is a warning icon and text: 'Ha a Windows felhasználói fiók elveszik, nem elég egy új fiókot készíteni azonos felhasználói névvel, és jelszóval. Komplet mentés szükséges a teljes felhasználói fiókról. Ha még nem készített sikeres felhasználói fiók visszaállítást, akkor ne használja ezt az opciót!'

The bottom of the dialog has three buttons: 'Súgó' (Help), 'Rendben' (OK), and 'Mégsem' (Cancel).

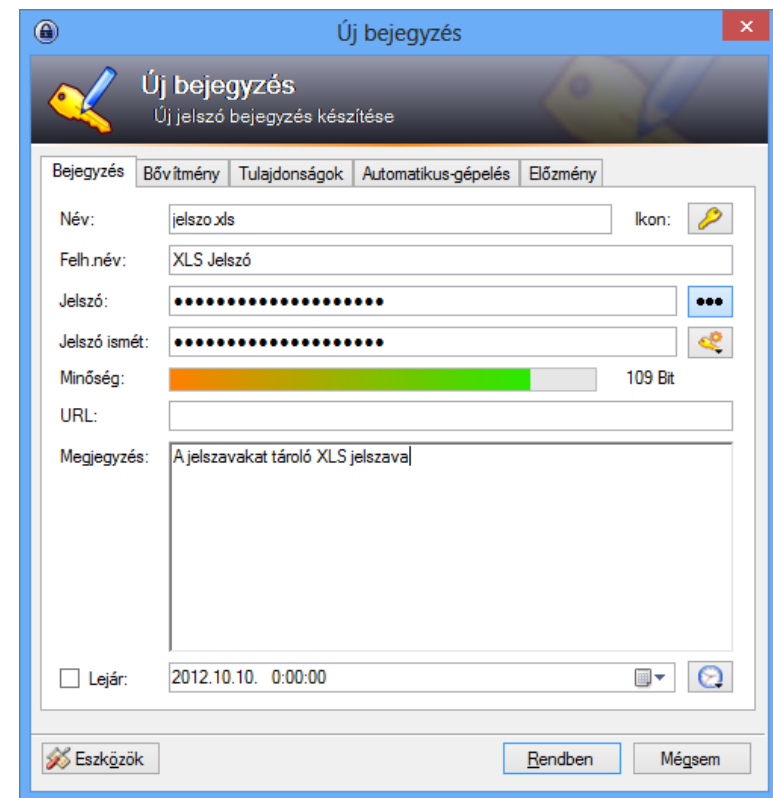
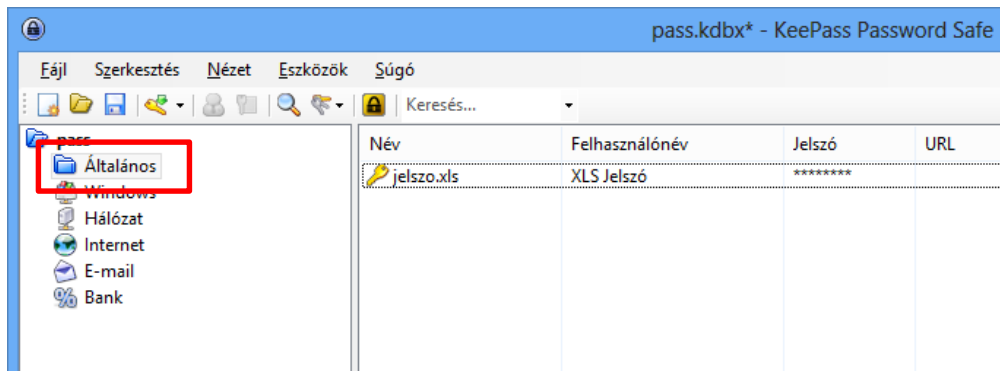
KeePass

Különböző témakörökhöz lehet jelszavakat rendelni.



KeePass

Új bejegyzés létrehozása (Általános)



KeePass

Új bejegyzés létrehozása (Windows)

