

**Milyen a jó  
jelszó?**



## Milyen gyorsan lehet feltörni egy jelszót?

Az alábbi táblázatokban látható, hogy kb. mennyi idő szükséges egy számítógépnek vagy egy több számítógépből álló szuperszámítógépnek, hogy a különböző erősségű jelszavakat kitalálja.

Az adatok csak közelítőlegeseek, azt a maximális időt mutatják, amely ahhoz szükséges, hogy egy ún. **BruteForce** (nyers erő) lefusson - vagyis, ha minden lehetséges kombinációt kipróbálnánk.

Ez az ellentéte annak, amikor csak néhány szóba jöhető jelszóval kísérletezünk.

## A tesztekben használt számítógép-típusok jellemzői:

- ▶ A típus (10 000 jelszó/mp)
- ▶ B típus (100 000 jelszó/mp)
- ▶ C típus (1 000 000 jelszó/mp)
- ▶ 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.

Mennyi a maximális idő, míg az összes kombinációt lefuttatja egy kódfejtő program??

Nézzük meg a különböző jelszavakat!!

# 10 szám kombinációjából alkotott jelszó feltörése - 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,**  
 amelyben csak az angol ábécé kis- vagy nagybetűi találhatóak:  
*ABCDEFGHIJKLMNOPQRSTUVWXYZ vagy abcdefghijklmnopqrstuvwxyz*

| 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**  
A teljes angol ábécé (csak kis vagy csak nagybetűk) és a számok együttes használatával:  
*ABCDEFGHIJKLMNOPQRSTUVWXYZ vagy  
abcdefghijklmnopqrstuvwxyz és 0123456789*

| 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: vegyítsük a kis és nagybetűket

AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz

| 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  |

**62 karakter kombinációjából alkotott jelszó:**  
a kis és nagybetűk mellett számokat is használunk a jelszóban:  
*0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz*

| Jelszó |             | A feltöréshez használt számítógép típusa |         |          |         |         |         |
|--------|-------------|------------------------------------------|---------|----------|---------|---------|---------|
| Hossz  | Kombinációk | A típus                                  | B típus | C típus  | D típus | E típus | F típus |
| 2      | 3844        | azonnal                                  | azonnal | azonnal  | azonnal | azonnal | azonnal |
| 3      | 238 328     | 23 mp                                    | 3 mp    | azonnal  | azonnal | azonnal | azonnal |
| 4      | 15 millió   | 24½ perc                                 | 2½ perc | 15 mp    | 2 mp    | azonnal | azonnal |
| 5      | 916 millió  | 1 nap                                    | 2½ óra  | 15¼ perc | 1½ perc | 9 mp    | azonnal |
| 6      | 57 billió   | 66 nap                                   | 6½ nap  | 16 óra   | 1½ óra  | 9½ perc | 56 mp   |
| 7      | 3,5 trillió | 11 év                                    | 1 év    | 41 nap   | 4 nap   | 10 óra  | 58 perc |
| 8      | 218 trillió | 692 év                                   | 69¼ év  | 7 év     | 253 nap | 25¼ nap | 60½ óra |

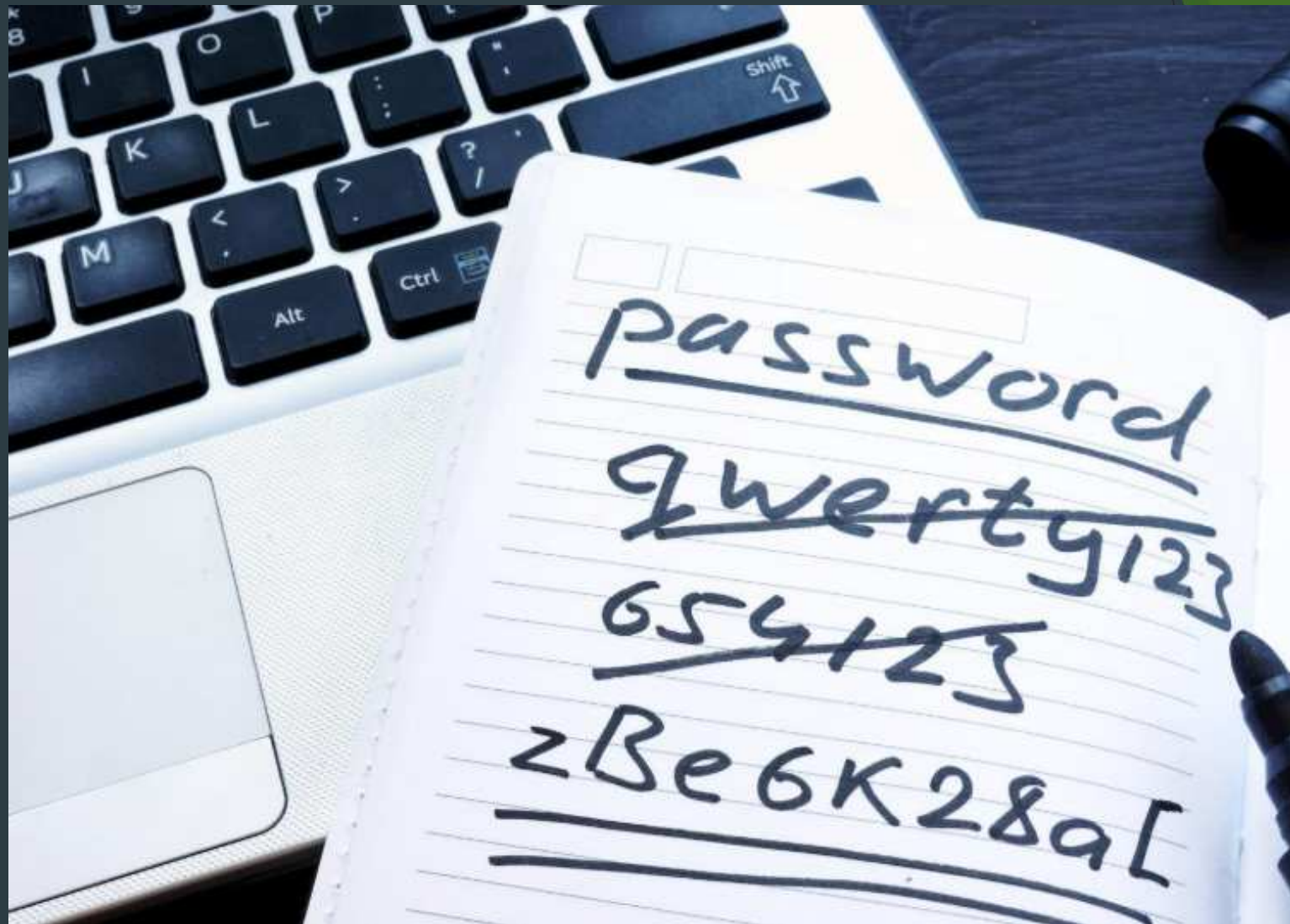
# 96 karakter kombinációjából alkotott jelszó, ahol felhasználjuk az összes lehetséges karaktert!

Kis- és nagybetűk, számok, valamint néhány gyakori szimbólum van a jelszóban:  
!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz

| 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 |

# Konkrét példák

| Jelszó   |                | A feltöréshez használt számítógép típusa |          |         |         |         |         |
|----------|----------------|------------------------------------------|----------|---------|---------|---------|---------|
| Jelszó   | Kombinációk    | A típus                                  | B típus  | C típus | D típus | E típus | F típus |
| lacika   | 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 |



## Leggyakoribb jelszavak

Nézzük a 10 leggyakrabban használt jelszótípust: megdöbbentő, hogy milyen sok ember használ ezekhez hasonló, könnyen kitalálható és feltörhető jelszavakat, még erősen biztonságkritikus helyeken is, mint például bankszámlák, adminisztrációs felületek vagy postafiókok esetében.

- ▶ **123456** - Ez a leggyakrabban használt jelszó. És igen, létezik olyan, aki fontos adatok hozzáférésehez használja ezt a jelszót. Hihetetlen igaz?
- ▶ **jelszó** - A kreativitás csúcsa, amikor valaki ezt a szót választja jelszóként. A csalók ilyenkor köszönik szépen a segítséget.
- ▶ **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 keresztnévének becézése. Még durvább, ha még csak nem is becézi, hanem egyenesen beírja a nevét - ez már nagyon súlyos.
- ▶ **0740174156** - A csajom vagy pasim telefonszáma, ne adj Isten a saját számom. Azért csak meg lehet jegyezni egy új számot a sok ismerős mellett, ne válasszuk már a saját számunkat!

- ▶ **asdf** - Miből gondolod, hogy csak te tudod sorjában leütni azt a 4-5 billentyűt? A csalóknál valószínű az első 5 próbálkozásban szerepelni fog ez a kombináció is.
- ▶ **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.

Próbáltad már, hogy  
**Cirmi123?**



Ellenőrizd a jelszavad erősségét a

<https://howsecureismypassword.net/> webcímen!!

Használj jelszóellenőrző Chrome bővítményt!!



### Jelszóvizsgálat bővítmény

A Jelszóvizsgálat bővítmény segít újra biztonságossá tenni az adatvédelmi incidens által érintett fiókokat.

Értesítést kap, ha bejelentkezéskor olyan felhasználónevet és jelszót ad meg, amelyek egy Google által ismert adatvédelmi incidens miatt már nem biztonságosak.

<https://chrome.google.com/webstore/detail/password-checkup-extensio/pncabnpcffmalkkjpaodfhijclecjno/related>

# Hogyan védj a jelszavadat? I.

- ▶ **Ne mondd el és ne add oda másnak!** Tartsd a jelszavaidat távol a családotól, barátaitól és a gyerekeidről, akik esetleg továbbadhatnák másnak. Légy elővigyázatos a jelszó-émlekeztető 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? II.

- ▶ **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 mindenhol beléphetnének.
- ▶ **Az interneten általános szabály, hogy mielőtt bármilyen jelszót megadjunk egy űrlapon, előbb győződjünk meg arról, hogy azon a címen vagyunk, ahol lenni szeretnénk - mindenképpen ellenőrizzük a böngésző címsorát!**

10-20 hely esetében mindent megjegyezni már problémás lehet! Ilyen esetekre találták ki a jelszómenedzser alkalmazásokat.

**JELSZAVAK ÉS PIN KÓDOK TELJES BIZTONSÁGBAN  
HASZNÁLJUNK JELSZÓMENEDZSERT!**

**A LEGJOBB JELSZÓMENEDZSEREK, MINDEN ESZKÖZÜNKRE**

Válasszunk cross-platform megoldásokat, hogy a felhőben szinkronizált jelszavainkat minden eszközünkön elérhessük velük.

Vagyis csak egy központi jelszót kell megjegyeznünk, minden mást pedig feljegyez helyettünk az adott program

A legjobb jelszókezelők funkciói termékenként változnak, de az alapfunkciók mindegyiknél ugyanazok:

- ▶ **Mesterjelszó vagy böngészőbe épülő bővítmény** (vagy mindkettő): a legjobb jelszókezelők vagy a weboldalakra automatikus bejelentkezést lehetővé tevő mesterjelszó használatával, vagy pedig egy böngészőbe épülő bővítménnyel biztosítják tárolt jelszavainkat.
- ▶ **Automatikus jelszó-elfogás:** a legjobb jelszókezelők nagy része automatikusan eltárolja jelszavainkat, némelyikük akár már telepítés közben is importálja azokat. A legkevesebb amit minden jelszókezelő megtehet, hogy elfogja a begépet jelszavakat, majd megkérdezi, hogy elmentse-e a saját tárolójába.
- ▶ **Automatikus űrlapkitöltés:** mivel a jelszókezelők képesek a jelszó típusú mezők automatikus kitöltésére, ezért használhatók más adatok tárolására is - például személyes (például személyi igazolványunk vagy TAJ-kártyánk számai), pénzügyi (banki, illetve PayPal-os bejelentkezési adataink) vagy egyéb típusú adatok is megjegyezhetők. A jelszókezelők jelentős részének van valamilyen automatikus kitöltési képessége, melyet telepítést követően állíthatunk be.
- ▶ **Jelszavak erősségének jelentése:** nagy valószínűséggel kapunk jelszóerősség-elemzőt is, amely kielemez jelszavainkat, majd értesít a viszonylag gyenge jelszavakról, melyek cseréjét akár azonnal képes elvégezni!

# Bitwarden jelszókezelő



A Bitwarden a legegyszerűbb és legbiztonságosabb módja a bejelentkezések és jelszavak tárolására, miközben kényelmet nyújtva tartja szinkronizálva az adatokat az összes eszköz között.

A Bitwarden minden bejelentkezési adatodat titkosított széfben tárolja és titkosítva szinkronizálja eszközeid között. Mivel teljesen titkosított, csak te férhetsz hozzá az adataidhoz. Még a bitwarden csapata sem tudja olvasni az adataidat, még ha akarná se tudná. Adataidat AES 256 bites titkosítással és SHA-256 PBKDF2-vel zárja le.

<https://play.google.com/store/apps/details?id=com.x8bit.bitwarden&hl=hu>

# Keepass2Android Password Safe



A Keepass2Android egy ingyenes nyílt forráskódú jelszókezelő alkalmazás az Android számára. Kompatibilis a népszerű KeePass 2.x jelszóval biztonságos Windows rendszerrel, és célja az eszközök közötti egyszerű szinkronizálás.

Az alkalmazás néhány fontos jellemzője:

- Az összes jelszavát biztonságosan titkosított tárolóban tárolja
- QuickUnlock: Nyissa ki az adatbázist egyszer a jelszóval, majd nyissa meg újra néhány karakter beírásával - vagy az ujjlenyomatával
- Szinkronizálja a felhő vagy a saját szerver segítségével (Dropbox, Google Drive).
- Automatikus kitöltési szolgáltatás és beépített billentyűzet a jelszavak biztonságos és egyszerű továbbításához a webhelyekre és az alkalmazásokra

KÖSZÖNÖM A  
FIGYELMET!!

