

## Jelszó (pin) tárolás

Adott egy képzeletbeli bankjegy automata, amelybe bankkártyát helyezve akkor is lehet pénzt felvenni, ha nincs kapcsolat a bankkal. Ehhez az kell, hogy a pin kódokat tároljuk az automatában.

De mi történne, hogyha éjjel valaki ellopná a kódokat az adatbázisból és megszerezné a bank ügyfeleinek a pin kódját? Hogyan lehetne ezt kivédeni? Pl. egyszerű Hash függvényel Neumann János ötlete alapján.

1. Adott egy ügyfél pin kódja:  $\{(4531)\}$
2. Emeljük a négyzetére:  $\{(4531)^2 = 20529961\}$
3. Az eredményből vegyünk el a középső 4 számjegyet, hogy újra 4 jegyű számot kapjunk:  $\{(2061)\}$ . Azaz csak a két-két szélső számok maradtak.
4. Emeljük újra négyzetre:  $\{(2061)^2 = 4247721\}$
5. Az eredményből vegyünk el a középső 3 számjegyet, marad az első 2 és az utolsó 2.  $\{(4221)\}$
6. Csináljuk meg a négyzetre emelést és a számjegyek elvételét 1000-szer!
7. Tegyük fel hogy a végeredmény:  $\{(6538)\}$  lesz.

Milyen viszonyban van a kezdeti 4531 és a 6538? Olyan mintha egy párt alkotnának. Ha valaki tudja, hogy 6538 a tárolt érték és ellopja az adatbázist, nem tudja megmondani, hogy melyik számból jött ki, mivel a számjegyek elvétele olyan mértékű adatvesztés, amit már nem lehet visszaállítani/kitalálni, viszont akárhányszor végezzük el, akkor is a kívánt eredményt kapjuk meg.

A weboldalak a jelszókat is hash kódokkal tárolják, azaz nem a beírt kódot tárolják, hanem egy algoritmus szerint átalakítják a bevitt jelszót és az eredményét tárolják.

Ezen az oldalon egy beírt jelszónak különböző hash kódjait lehet online generálni:

<http://www.fileformat.info/tool/hash.htm>

Például az '1234' kód MD5 hash-e:  $\text{md5}(1234) = 81dc9bdb52d04dc20036dbd8313ed055$

Ezek alapján mondhatjuk, hogy a hash-ek tárolása teljes biztonságot ad? Sajnos nem. Tegyük fel, hogy egy hacker ellopta az adatbázist és éppen a mi jelszónkat böngészi. Ezen az oldalon beírja a hosszú hash kódot:

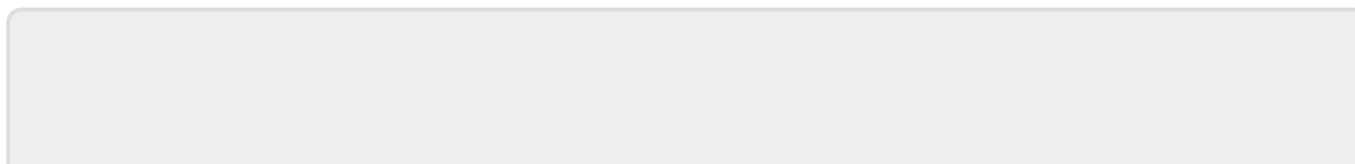
<http://md5cracker.org/decrypted-md5-hash/81dc9bdb52d04dc20036dbd8313ed055>

Sajnos már tudja is a jelszónkat. A megoldás egyrészt az, hogy hosszú jelszót használunk, de azt nehéz megjegyezni. Másik megoldás, hogy minden jelszóhoz a hash képzéskor egy ún. só-t adunk, ami egy fix string és azzal együtt generáljuk a kódot:

$\text{\$ \$ md5}(1234 + \text{\textit{my\_strong\_salt}}) = 0e0db19d64ce23edc1bfb52063f25028\text{\$ \$}$

Próbáljuk rákeresni az eredményre a cracker oldalon!

Mostmár csak az a fontos, hogy a só-t jól elrejtjük!



From: <https://edu.iit.uni-miskolc.hu/> - Institute of Information Science - University of Miskolc

Permanent link: [https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai\\_architekturak:informacio\\_titkositas\\_es\\_hitelesites:jelszo\\_tarolas?rev=1731522004](https://edu.iit.uni-miskolc.hu/tanszek:oktatas:infrendalapjai_architekturak:informacio_titkositas_es_hitelesites:jelszo_tarolas?rev=1731522004)

Last update: **2024/11/13 18:20**

