Óbudai Egyetem

Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

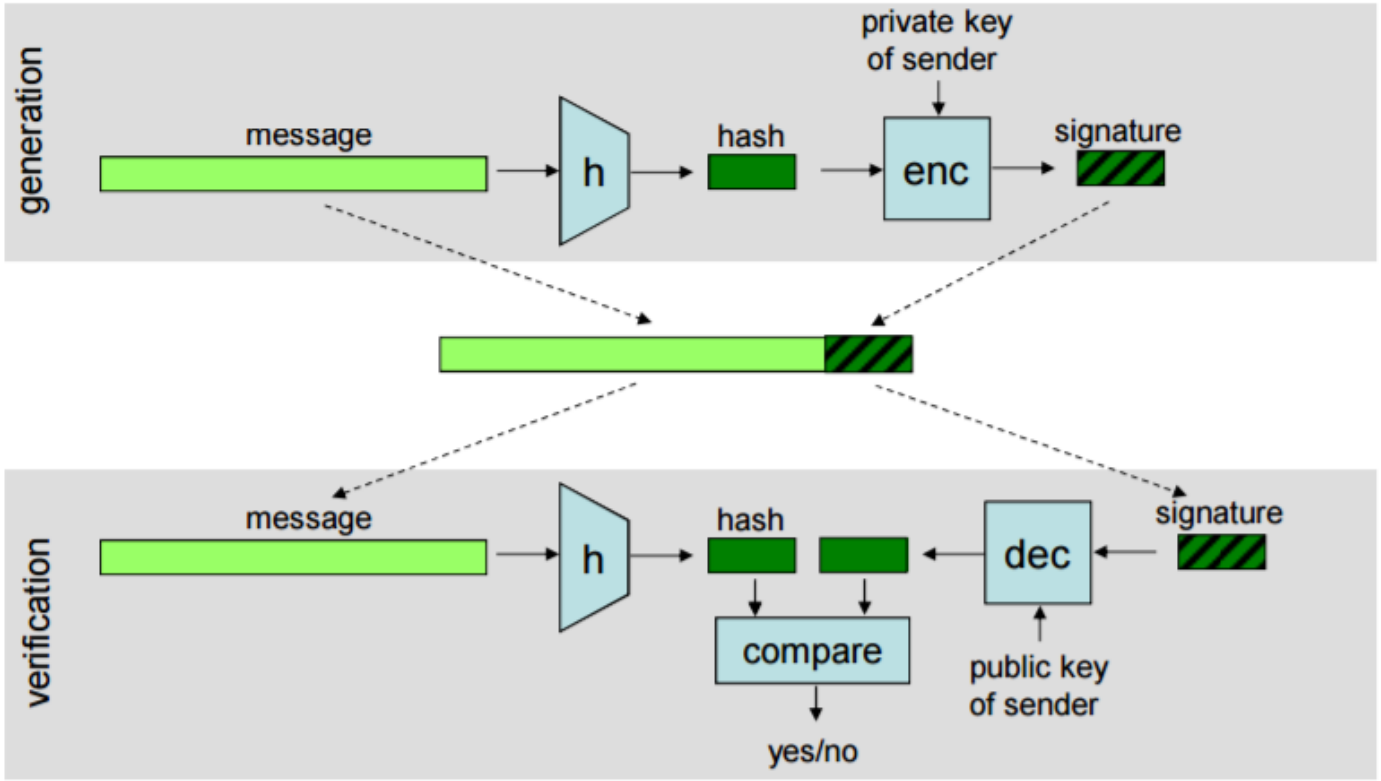
Műszaki területek informatikai biztonsága
Jelszavak

ZENTAI DÁNIEL

ZENTAI.DANIEL@BGK.UNI-OBUDA.HU

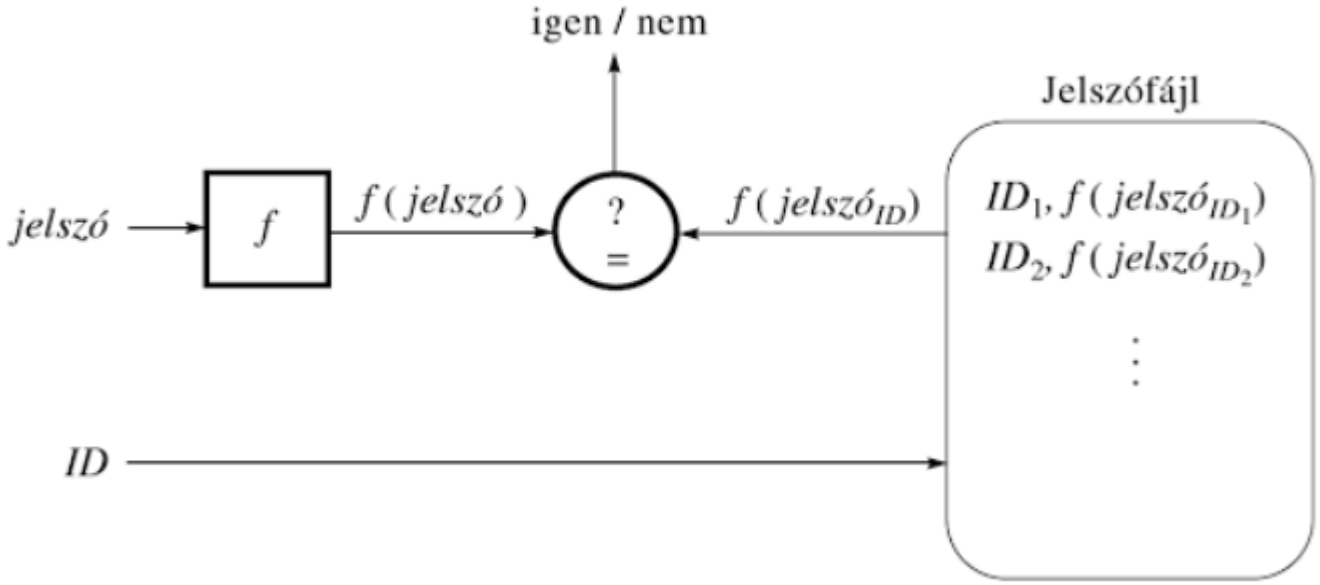
Hash függvények

Digitális aláírás:



Jelszavak tárolása

A jelszó helyett csak a jelszó egy hash lenyomatát tároljuk el. Belépéskor egy y lenyomatot összehasonlítunk a h(pwd) hash értékkel, és ha egyezést találunk, akkor sikeres az autentikáció.



Hash függvények

H egy hash függvény, ha tetszőleges hosszúságú bitsorozatot fix hosszúságú bitsorozatba képez le, azaz $H:\{0,1\}^* \rightarrow \{0,1\}^n$

Követelmények:

1) Egyirányú: Adott y hash értékhez nehéz olyan x inputot találni, amire $y = H(x)$

2) Gyenge ütközés ellenálló: Adott x inputhoz nehéz olyan $x' \neq x$ inputot találni, amire $H(x') = H(x)$

3) Ütközés ellenálló: Nehéz olyan x és x' input párt találni, amire $x' \neq x$, de $H(x') = H(x)$

Hash függvények

Születésnap paradoxon:

Egy 23 fős csoportban nagyjából 50% valószínűséggel van 2 ember, akinek ugyanakkor van a születésnapja.

Általánosabban: Egy n elemű halmazból $\sqrt{n}$ elemet választva visszatevéssel, nagyjából 50% valószínűséggel ismétlődő elem.

Hash függvényekre vonatkoztatva: Egy n bites hash függvénynek 2^n féle outputja lehet, tehát $\sqrt{(2^n)} = 2^{n/2}$ esetet kipróbálva nagy valószínűséggel lesz ütköző pár.

Következmény: n-et úgy kell választani, hogy még n/2 is nagy legyen.

Támadási módszerek

Brute force:

A teljes kulcstér végigpróbállása

Szótár alapú:

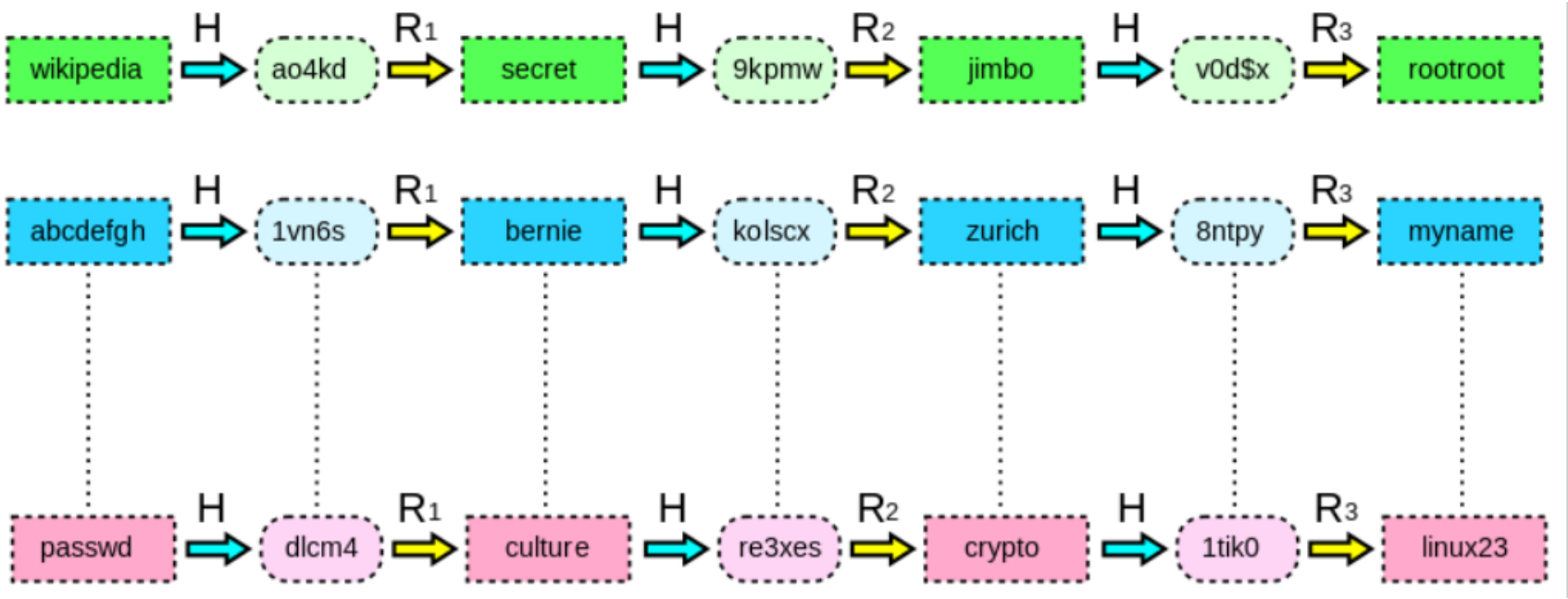
Egy gyakori jelszavakat tartalmazó szótár alapján próbáljuk végig a lehetséges jelszavakat

Szivárvány tábla:

Egy redukciós függvénnyel leképezzük a hash lenyomatokat a lehetséges jelszavak halmazára. Így hash-láncok jönnek létre. Ezeknek az elejét és a végét elég eltárolni. Fontos, hogy a redukciós függvény determinisztikus legyen.

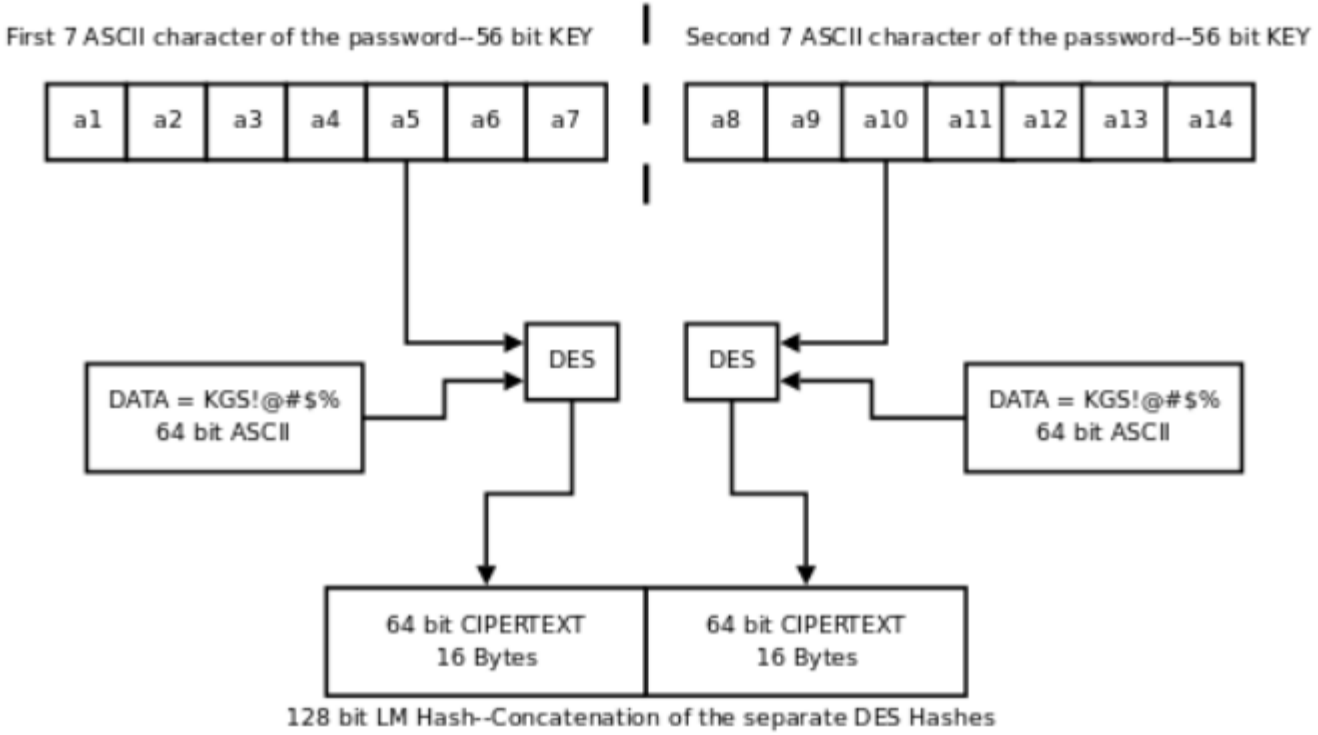
Támadási módszerek

Szivárvány tábla:

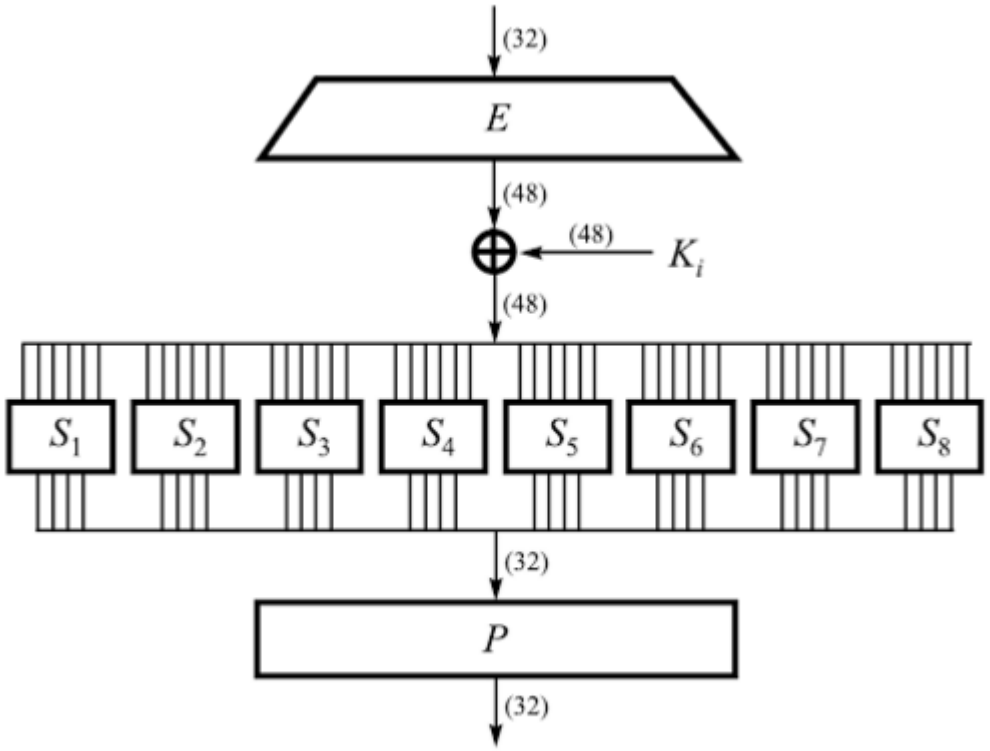


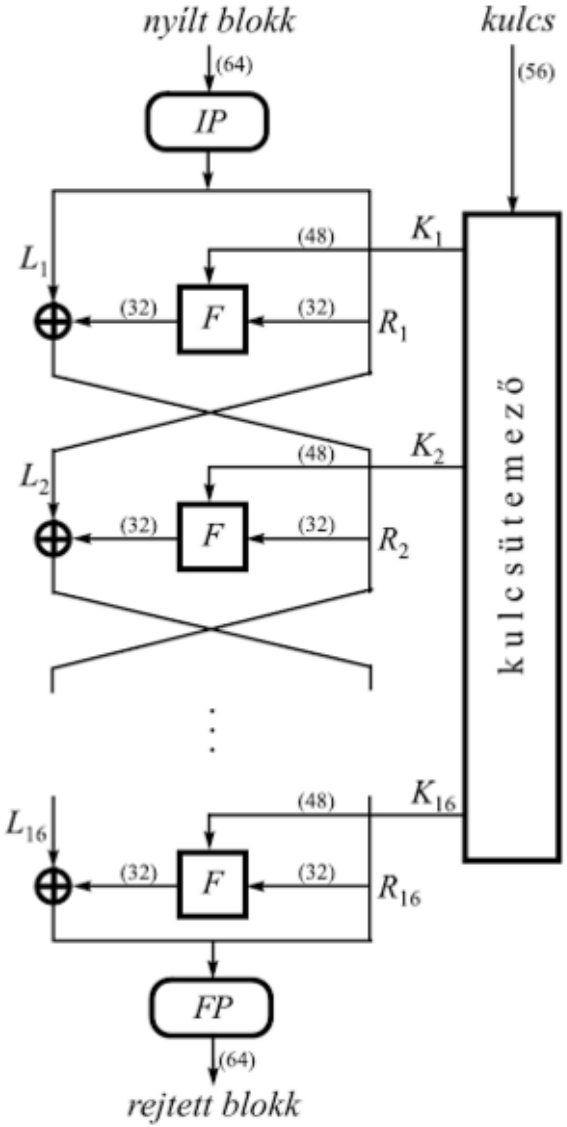
Windows jelszavak

LM hash:



DES (emlékeztető)





Windows jelszavak

NTLM hash:

H(password)=MD4(unicode(password))

Unicode: nem titkosítás, csak karakter kódolás

Köszönöm a figyelmet!