1 Hash

Hash, neboli hašovací funkce se rozumí v kryptografii funkce, která slouží k převodu vstupu o libovolné velikosti do výstupu o pevné délce, s takovou vlastností že není jednoduché z výstupu zpětně získat vstupní data.

Mezi hlavní vlastnosti hashe patří:

1. Vstupní data mohou být o libovolné délce, ale výstup musím mít délku fixní.
2. Jakákoliv změna vstupních data by měla zásadně změnit podobu výstupních dat.
3. Mělo by být výpočetně a časově obtížné získat zpět vstupní data.

V současnosti se hashe používají například pro tvorbu podpisů, ukládání hesel, podepisování zpráv/dat apod.. Mezi známé hashovací funkce paří například MD5, SHA-1 a další hashe z rodiny SHA.

Vzhledem k základní povaze hashovacích funkcí je vznik kolize, tj. nalezení buď originálního vstupu (kolize prvního typu) nebo jiného vstupu k získání stejného výstupu (kolize druhého typu). Tento fakt je zapříčiněn omezením délky výstupních dat například u MD5 128 bitů, což dává pouze 2^{128} možných výstupů, tudíž existuje pravděpodobnost že lze prostým testováním náhodných vstupů nalézt kolizi.

Tento postup pro hledání kolizí není nijak optimální, pro alespoň nějak efektivní hledání hashů je vhodné použít tzv. slovníkové útoky, kde již vytvořená databáze častých vstupů, které lze očekávat, například hesla, tím lze alespoň otestovat ty nejvíce pravděpodobné vstupy. Po otestování slovníku k nalezení kolize je opět nutné pokračovat v útoku hrubou silou.

2 MD5

MD5 neboli message-digest algorithm je hashovací funkce. Je v současnosti již prolomená hashovací funkce, která sloužila ke kontrole integrity dat a ke kontrole hesel na operačních systémech Windows. Její výstup je o délce 128 bitů.

V rámci OS Windows byl tento hash používán například v rámci protokolu NTLM, který sloužil k ověření identity uživatele při přihlašování do systému. Po objevení zranitelností, které tento hash měl byl ale postupně nahrazen novými a bezpečnějšími algoritmy jako například SHA-256, který se používá v moderních verzích Windows. Avšak lze stále manuálně zapnout MD5 pro ukládání hesel na Windows.