Digitális aláírás

Laikusok szemében a digitális aláíráson azt sejtik, hogy egy asszisztens szkenner segítségével bedigitalizálja a főnöke aláírását egy képállományba és szükség esetén ez a kép könnyen beilleszthető az aláírandó dokumentumokba. Sajnos ez a módszer komoly büntetőjogi szankciókkal is járna ha így járnának el, de a digitális aláírás a valóságban egészen más.

A nyilvános kulcsú rendszereket **aszimmetrikus** rendszereknek is szokás nevezni, mert a kódoláshoz és a dekódoláshoz már más kulcs szükséges. A **szimmetrikus** rendszerekben ugyanaz a kulcs kódol és dekódol.

Az **aszimmetrikus** rendszerekben Annának bárki küldhet titkos üzenetet. Hogyan bizonyosodhatunk meg a küldő kilétéről? A digitális aláíró algoritmusok is speciális aszimmetrikus rendszerek. Van egy titkos kulcs az aláíráshoz és egy nyilvános kulcs az aláírás hitelességének ellenőrzéséhez.

A digitális aláírás követelményei

- **Az aláírás legyen hiteles**: az aláírás meggyőzi a dokumentum olvasóját, hogy az aláírás tulajdonosa tudatosan írta alá a dokumentumot.
- **Legyen hamisíthatatlan**: az aláírás bizonyítja, hogy az aláírás tulajdonosa maga és nem más írta alá a dokumentumot.
- **Az aláírás nem lehet felhasználni fel más dokumentumon**: az aláírás a dokumentum szerves része, nem helyezhető át egy másikra.
- Az aláírt dokumentumot ne lehessen megváltoztatni észrevétlenül.
- **Legyen letagadhatatlan**: az aláíró később nem tagadhatja le, hogy aláírta a dokumentumot.

Ezek a követelmények a manuális (analóg) aláírásnál sokkal biztonságosabb megoldást jelentenek.

Egyszerű digitális aláírás RSA közvetlen alkalmazásával

Egyszerű esetben az RSA algoritmus is alkalmas lehet digitális aláírásra.

Az alábbi pontok felsorolják a lépéseket:

- saját titkos kulcsunkkal kódolni kell a dokumentumot.
- RSA-ban a titkos és nyilvános kulcsok szerepe felcserélhető: akármelyikkel rejtjelezhetünk, mindig a másikkal (és csakis azzal) lehet visszafejteni az üzenetet.
- Ha valaki titkosít egy üzenetet a titkos kulcsával, akkor a nyilvános kulccsal visszafejthető (így ellenőrizve a hitelességet).
- Az egész dokumentum el van kódolva az aláírásban. (maga a kódolt dokumentum az aláírás)
- Az aláíró nem tagadhatja le az aláírás tényét, mert ő az egyetlen aki az előállításhoz szükséges titkos kulcsot ismeri.

Az RSA aláíró módszer használatával a dokumentum olvashatatlan marad, ahhoz hogy el tudjuk olvasni, ellenőrizni kell az aláírást.

Ez a módszer kényelmetlen, ha:

- ha nem áll rendelkezésre a nyilvános kulcs,

- ha nincs elegendő számítási kapacitás a visszafejtéshez.

Hash függvények

A sima **RSA** nagy hátránya, hogy a dokumentum maga az aláírás. Hogyan lehetne az aláírást a dokumentumtól elválasztani? Ehhez vezessük be a **Hash** függvényeket.

Hash függvények jellemzése:

- olyan speciális függvények, amelyek változó hosszúságú input esetén, fix hosszúságú outputot adnak,
- y outputhoz egy olyan x inputot találni nehéz, amelyre igaz, hogy $y = H(x)$,
- nehéz olyan x' inputot találni, amely esetén $H(x)=H(x')$ azaz ugyanaz a Hash kód,
- de ennek ellenére $H(x)$ könnyen számolható,
- jól szórjon: azaz ha az x csak 1 bitben is megváltozik, várhatóan y bitjeinek a fele megváltozzon.

A legismertebb Hash-függvények: SHA, MD2, MD5 (Message Digest 5).

Digitális aláírás Hash függvénnyel

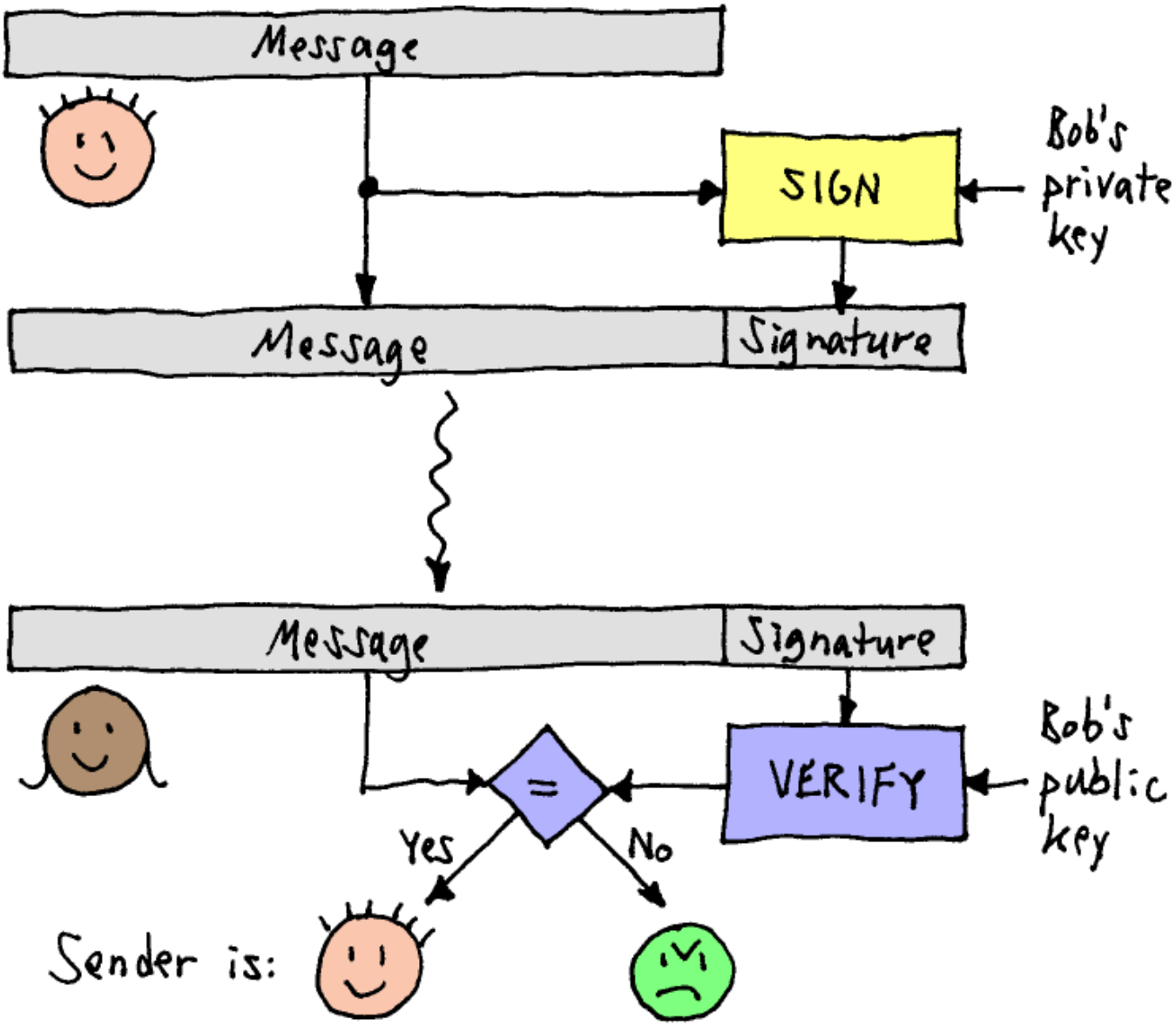
A Hash függvénnyel végzett művelet úgy viselkedik mint egy digitális ujjlenyomat. A függvény biztosítja, hogy tetszőleges dokumentumnál a kód elég változatos lesz. Hogyan is működik ezzel a digitális aláírás?

- $y=H(x)$ alapján az y-t egy x dokumentumra kiszámítani. Ez az ujjlenyomat készítés.
- y kódolása a titkos kulccsal
- az eredmény csatolása a dokumentumhoz (aláírás)

Következmények

- A dokumentum aláírt formában is olvasható.
- Az aláírás a dokumentumtól elkülönítve is tárolható. pl. egy közjegyzőnél vagy adatbázisban

A következő kép ezt a folyamatot mutatja:



A hálózati kommunikáció során a következő adatokat továbbítjuk:

- eredeti dokumentum
- a dokumentumból képzett Hash, titkosítva feladó titkos kulcsával
- a feladó nyilvános kulcsa

Az aláírás sértetlenségét a következőképpen állapíthatjuk meg:

- számítsuk ki a kapott dokumentum Hash kódját
- a nyilvános kulccsal dekódoljuk a kódolt Hash-t
- az előző lépéseknek ugyanazt a Hash kódot kell adniuk