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

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