Dokumentumok védelme (titkosítás)

A dokumentumok védelmének célja az olvasásvédelem, írásvédelem, illetve a dokumentumok egyértelmű beazonosíthatósága.

Alapfogalmak

Nyílt szöveg: titkosítandó üzenet

Kulcs: paraméterezhető függvény (algoritmus)

Titkosított szöveg / kriptogram: kulccsal átalakított nyílt szöveg.

Kriptológia: a rejtjelezés tervezésével és megfejtésével foglalkozó tudományág.

A dokumentum védelem az alábbi két szempont teljesülését jelenti

⇒ **Bizalmasság (confidentiality)**:
Az információt csak az arra jogosultak és csak a jogosultsági szintjüknek megfelelően ismerhetik meg és kezelhetik.
⇨ Jelszavas védelem

⇒ **Sértetlenség (integrity)**:
Az információ az elvárt forrásból származik, megfelel az eredeti állapotának és a származás ellenőrizhető – ezáltal letagadhatatlan
⇨ Üzenetkivonat, titkosítás, digitális aláírás

Jelszavas védelem

Az irodai programcsomagokban használható programok beépített funkciókat tartalmaznak a szöveg jelszavas védelmének megteremtéséhez, más szóval a dokumentum-titkosításhoz. Amennyiben használjuk ezt a funkciót, a szövegszerkesztő bekér tőlünk egy jelszót, aminek segítségével a teljes dokumentumot kriptográfiailag titkosítja, így azt a jelszót nem ismerő számára teljesen olvashatatlanná teszi.

A dokumentum tartalmának védelmére van lehetőség csak olvashatóra állítani a dokumentumot, és a szerkesztést letiltani, illetve jelszóhoz kötni.

A dokumentum titkosítása, a jelszó beállítása a C# kódból is elvégezhető a dokumentum példány `Password` tulajdonságának beállításával. A csak olvasható tulajdonságot a `word Document Protect` metódusának első paraméterével tudjuk megadni a `Word.WdProtectionType.wdAllowOnlyReading` értékkel.

Message digest (üzenet kivonat)

- ⇒ ún. Hash-függvények használatával a bemeneti adatból egy fix, 128 bit hosszúságú kimeneti adatot állít elő – ezt nevezzük hash-értéknek,
- ⇒ adott bemeneti adatból mindig ugyanazt a kimenetet adja,
- ⇒ a kimeneti adatból nem állítható elő a bemeneti adat (egyirányú függvény),
- ⇒ a bemeneti adat legkisebb változása is teljesen más kimenetet eredményez,
- ⇒ mivel a bemenet hossza tetszőleges nagy lehet, a kimenet pedig rögzített, eltérő bemenetek eredményezhetik ugyanazt a kimenetet, ezt nevezzük ütközésnek.

Ilyen üzenetkivonatoló eljárások az MD5 és SHA nevű algoritmusok. Jelszavak titkosítására is szokták használni, a nagyobb biztonság érdekében az ún. „sózás" módszerével együtt. (só: a szöveg/jelszó elejéhez és/vagy végéhez hozzáfűzött karaktersorozat) Ha valaki meg akar bizonyosodni egy üzenet/adat eredetiségéről, annak kell készíteni az üzenetről egy ellenőrzőösszeget, ugyanazzal az MD algoritmussal és összehasonlítani a az eredeti szövegből készített hash értéket, és a kérdéses szövegből készített hash-értéket; a két érték csak akkor fog egyezni, ha az üzenet/adat nem változott.

Titkosítás

A bizalmasság biztosításához titkosításra van szükség, amelyből a kódolt üzenet helyreállítható. A titkosítások két fajtája a szimmetrikus (egykulcsú) és az aszimmetrikus (kétkulcsú) titkosítás.

Szimmetrikus titkosítás

A szimmetrikus titkosítás esetén a küldőnek és a fogadónak is ismerni kell a titkosításhoz használt kulcsot, illetve lényegileg ugyanazzal a módszerrel titkosítunk és fejtünk. Ilyen módszer az összes klasszikus módszer, de mai korunkban is találunk ilyeneket, például a DES, illetve annak továbbfejlesztett változata, az AES is így működik. Nagy adatfolyamok gyors kódolására és dekódolására kiválóan alkalmas.

A DES (=Data Encryption Standard) az IBM által LUCIFER néven kifejlesztett titkosítási algoritmus továbbfejlesztése, amelyet 1997-ben az USA-ban szabványosítottak. 64 bites blokkokból egy 56 bites kulccsal állít elő szintén 64 bites kódolt üzenetet. A kód feltörése a brute force módszerrel (minden lehetséges kulcs kipróbálása) a számítógépek fejlődésével könnyűvé vált, ezért továbbfejlesztették a módszert.

Utódja a 2001-ben AES néven megjelent titkosítási módszer: ez 128 bites blokkokat használ, és a kulcsméret is jóval nagyobb: 128, 192 illetve 256 bites. A titkosítási algoritmus továbbra is gyors, ugyanakkor a mai hardver mellett biztonságosnak tekinthető.

A szimmetrikus titkosítási módszerekben, így az AES-ben is, a biztonság záloga a kulcs titkossága. Ugyanakkor a kulcsot meg kell osztani a résztvevő felekkel (különben nem tudják visszafejteni az üzenetet) és ez nem mindig egyszerű dolog.

Aszimmetrikus titkosítás

A fenti problémát a nyilvános kulcsú titkosító algoritmusok oldják meg. Sokáig elképzelhetetlen volt, hogy legyen olyan módszer, amely jól működik a két fél közös titka nélkül, illetve úgy, hogy hiába ismerjük a titkosító kulcsot, megfejteni nem tudjuk az üzenetet. Aztán a 20. században sikerült megoldani a talányt, az ilyen módszereket asszimetrikus kulcsú titkosításnak nevezzük.

Ezek a módszerek egy összetartozó kulcspárt használnak: az egyik neve privát, vagy más néven titkos kulcs (private key), ezt - mint a neve is mutatja - titokban tartjuk; a másik, nyilvános kulcsot (public key) pedig szabadon elérhetővé tesszük bárki számára. Fontos, hogy a privát kulcsból könnyen elő lehet állítani a nyilvános kulcsot, azonban ez fordítva már nem, vagy nagyon nehezen lehetséges. Ez magyarul azt jelenti, hogy a kellően biztonságosnak ítélt titkosítási eljárással létrehozott rejtjelezett szöveg visszafejtése a jelenleg elérhető komputeres számítási kapacitással legalább néhány emberöltőig eltartana.

A legfontosabb tulajdonság, hogy az egyik kulccsal kódolt információt kizárólag a másik kulccsal lehet visszafejteni. Ha titkos üzenetet akarunk küldeni valakinek, a következő lépések történnek:

1) Egy nyilvánosan elérhető, megbízható forrásból, pl. magától a címzettől, vagy kulcsszerverről **megszerezzük a címzett nyilvános kulcsát.**
2) **Az üzenetet kódoljuk ezzel a kulccsal, majd elküldjük**. (A kódolt üzenet csakis a címzett privát kulcsával nyitható, tehát ha az eredeti üzenetet elvesztettük, vagy töröltük, a titkosított üzenetből még mi sem tudjuk visszafejteni.)
3) A megkapott üzenetet **a címzett saját privát kulcsával visszafejti**, a végeredmény az eredeti, titkosítatlan szöveg lesz.

A nyilvános kulcs és a magánkulcs kulcs között matematikai összefüggés van, a nyilvános kulccsal kódolt adat csak a hozzá tartozó magánkulccsal dekódolható, valamint a magánkulccsal kódolt adat is dekódolható, kizárólag a nyilvános párjával. Ugyanakkor, nem szabad, hogy a nyilvános kulcsból (hatékonyan, reális mennyiségű erőforrással) ki lehessen számítani a magánkulcsot.

Mint látható, a módszer nagy előnye a szimmetrikus megoldással szemben, hogy itt nincs szükség védett csatornán történő előzetes kulcsegyeztetésre. Hátránya, hogy sebessége jóval lassabb, mint a szimmetrikus megoldásé, így nagy mennyiségű adat védelmére egyelőre nem használják. Remekül hasznosítható azonban a kettő kombinációja: az üzenetet magát szimmetrikus titkosítással kódolják (ami gyorsabb), de a szimmetrikus kulcsot aszimmetrikus titkosítással küldik el a címzettnek. Legismertebb algoritmusok: Diffie-Hellmann, RSA, DSA. Az RSA módszer azon a matematikai tényen alapul, hogy két nagy prímszámot könnyű összeszorozni, de csak a szorzat ismeretében nagyon nehéz a tényezőket megtalálni. A mai számítógépes teljesítmények mellett a szorzatnak több, mint 300 jegyű számnak kell lennie.

Digitális aláírás

A nyilvános kulcsú titkosítás más módon is használható: ha a saját magánkulcsunkkal kódolunk egy dokumentumot, az így kapott adatról – a nyilvános kulcsunk alapján – bárki megállapíthatja, hogy azt mi hoztuk létre. E műveletet aláírásnak nevezzük.

Akár titkos üzenetet akarunk küldeni valakinek, akár az elektronikus aláírását akarjuk ellenőrizni, alapvető követelmény, hogy hitelesen jussunk hozzá a másik fél nyilvános kulcsához. Egy kulcs használata előtt meg kell bizonyosodnunk róla, hogy a kulcs valóban annak a személynek (szervezetnek) a birtokában van, akinek titkos üzenetet szeretnénk küldeni, vagy akinek az aláírását ellenőrizni szeretnénk. E célra tanúsítványokat szokás használni. A tanúsítvány egy megbízható szervezet, egy hitelesítés szolgáltató által kiállított igazolás arról, hogy egy adott magánkulcs egy adott személyhez vagy szervezethez tartozik. Aláíráskor nem a teljes dokumentumot szokás kódolni a magánkulccsal. Ez nagyon lassú és időigényes volna. Ezért egy lenyomatképző függvénnyel (hash-függvénnyel) lenyomatot képzünk az aláírandó dokumentumból, és csak ezt a lenyomatot kódoljuk a magánkulcsunkkal. A magánkulcsunkkal kódolt, aláírt lenyomatot nevezzük aláírásnak. Aki ellenőrizni szeretné az aláírást, annak az ellenőrzéshez neki lenyomatot kell képeznie az aláírt dokumentumból, majd az aláíró nyilvános kulcsával kódolnia kell a dokumentumhoz tartozó aláírást (így azt a lenyomatot kapja vissza, amit az aláíró aláírt). Ha az általa képzett lenyomat megegyezik az aláírásból visszanyert lenyomattal, akkor az aláírás érvényes. Mivel a digitális aláírás nem hamisítható ezért letagadhatatlan.