Tartalomjegyzék

A titkosításról

A szimmetrikus és az aszimetrikus titkosítás

A titkosítás célja: bizalmas információk továbbítása egy nem biztonságos közegen keresztül (pl. Internet) egy erre alkalmas algoritmus segítségével.

A titkosítás kiindulópontjának az egykulcsos, úgynevezett szimmetrikus rendszereket tekinthetjük, amelyek még ma is jelent?s szerepet játszanak a kriptográfiában.
(Képvisel?i pl. a TripleDES, AES, TwoFish, IDEA algoritmusok.)
A szimmetrikus titkosítás el?nye a gyorsaság, hátránya viszont a legf?bb tulajdonságából származik: a titkosításhoz és kódoláshoz ugyanaz a kulcs használatos, így azt a feladónak és a címzettnek is ismernie kell. A kulcsot biztonságosnak vélt úton kell eljuttatni a másik félhez, például személyes találkozáskor, ami nem minden esetben kivitelezhet?. Más megoldás nem lévén ez az út valószín?leg ugyanaz a nem biztonságos csatorna lesz, amelyen a további kommunikáció is folyna. Ez azonban megnehezíti az azonnali és globális kommunikációt.

Az aszimmetrikus titkosítás alapja egy 1977-ben született matematikai megoldás. Legismertebb megvalósítása az RSA algoritmus, amelynek kidolgozása három matematikus nevéhez f?z?dik (Rivest, Shamir és Adleman). Lényege: minden felhasználó (feladó és címzett egyaránt) rendelkezik egy kulcspárral, ami egy nyilvános (public) és egy titkos (private) kulcsot tartalmaz. A nyilvános kulcs a titkosításhoz, a privát kulcs a visszafejtéshez használatos. Fontos megjegyezni, hogy a két kulcs egymásból nem számítható ki, vagyis nem állítható el? a nyilvános kulcsból a titkos kulcs.

Gyakorlati m?ködése: a titkos kulcsot optimális esetben csak tulajdonosa ismerheti, viszont publikus kulcsát minél szélesebb körben ismertté kell tennie, hiszen így tudnak neki -címzettnek- titkosított üzenetet küldeni. A két kulcs egymást kiegészítve m?ködik; a címzett nyilvános kulcsával titkosítjuk az üzenetet, amit rajta kívül más nem tud elolvasni, hiszen csak ? rendelkezik a visszafejtést végz? titkos kulccsal. A módszer er?sségét a szimmetrikus kulcsos titkosítás hátrányának kiküszöbölése adja: azok is tudnak titkosított üzeneteket váltani, akik nem ismerik egymást (elég, ha el?z?leg kicserélték nyilvános kulcsaikat). Ez a csere történhet Interneten keresztül is, hiszen attól, hogy valaki megszerzi a nyilvános kulcsunkat még nem fér hozzá bizalmas információkhoz. További el?nyös tulajdonsága, a digitális aláírás készítésének lehet?sége, mely opciót a hitelességvizsgálat céljából érdemes kihasználni.

Kulcsok és tulajdonságaik

- Titkos kulcs

Minden kulcspár egy titkos (magánkulcs) és egy nyilvános kulcsból áll. A titkos kulcsot csak a kulcspár tulajdonosa ismeri. A titkos kulcsot használjuk a nekünk küldött kódolt üzenetek visszafejtésére és elektronikus leveleink digitális aláírására.

- Nyilvános kulcs

A nyilvános kulcs arra szolgál, hogy a rejtjelezett üzeneteket tudjunk váltani partnereinkkel. A nyilvános kulcsot használjuk a kódolt üzenetek készítésekor és a digitálisan aláírt levelek hitelességének ellen?rzésekor. A hatékony levelezés érdekében a nyilvános kulcsot minél szélesebb körben kell ismertté tenni. A nyilvános kulcsból nem számítható ki a titkos kulcs, és nem alkalmas a rejtjelzett üzenet visszafejtésére sem; az üzenetet csak az tudja elolvasni, akinek birtokában van a titkos kulcs.

- Session key (egyszer használatos titkosító kulcs)

Hibrid titkosítási módszer alkalmazásakor az ideiglenes titkosító kulcs, amelyet a nagy adatmennyiséget jelent? üzenettörzs vagy csatolt állomány szimmetrikus algoritmussal történ? kódolásakor használunk (gyors), majd a kulcsot aszimmetrikus (er?s) algoritmus használatával szintén kódoljuk.

A PGP technológia

A PGP m?ködése

A PGP m?ködése a két titkosítási módszer kombinációjaként létrejött úgynevezett hibrid titkosításon alapul. A módszer egyesíti a szimmetrikus titkosítás gyorsaságát az aszimmetrikus titkosítás biztonságával. A PGP a titkosítási eljárás során tömöríti a titkosítani kívánt adatot ZIP algoritmussal, majd azt egy véletlen generálású kulccsal (session key) titkosítja.

Ez a folyamat még nagy méret? adatfolyam esetében is gyorsnak tekinthet?, hiszen a hibrid titkosítás ezen részében szimmetrikus algoritmussal történik a kódolás. Következ? lépésként a session kulcs kerül titkosításra, ez azonban már a az aszimmetrikus titkosításból ismert publikus kulccsal lesz titkosítva. Így létrejön egy olyan csomag, amely tartalmazza a titkosított adatot és a visszafejtéshez szükséges kulcsot - titkosítva.

Az üzenet titkosításának lépései

1. Tömörítés
2. Szimmetrikus titkosítás egy véletlen generálású kulccsal (session key)
3. A véletlen generálású kulcs (session key) titkosítása a címzett nyilvános kulcsával (aszimmetrikus titkosítás)
   - mivel a session kulcs kis méret?, a titkosítás gyorsan megtörténik
4. Küldés

A titkosított üzenet visszafejtése a címzettnél fordított sorrendben történik

1. Üzenet fogadása
2. A véletlen generálású kulcs (session key) visszafejtése a címzett titkos kulcsával (aszimmetrikus eljárás)
3. Az üzenet visszafejtése a véletlen generálású kulcs (session key) segítségével
4. Megjelenítés

Digitális aláírás

A digitális aláírás segítségével a címzett meggy?z?dhet a neki küldött üzenet hitelességér?l. Vagyis arról, hogy a levél feladója tényleg az, akinek mondja magát, és a levél tartalma továbbítás közben nem változott meg. Ennek megvalósításához egy ún. hash függvényt alkalmaznak, amely az üzenetb?l egy kis méret? ellen?rz? összeget készít. Ha valaki akár egy karakternyit változtat az üzenetben, a hash függvény más ellen?rz? összeget fog létrehozni a feladó, illetve a címzett oldalán. Mivel az ellen?rz? összeg az üzenet részeként jut el a címzetthez, az ellen?rzés során azonnal kisz?rhet? az esetleges módosítás.

A digitális aláírás és az üzenet hitelességének ellen?rzése

- Aláírás a feladó titkos kulcsával
- Ellen?rz? összeg készítése és beillesztése az üzenetbe
- Küldés
- Fogadás
- Ellen?rzés a feladó nyilvános kulcsával

A PGP alkalmazása

Saját kulcs készítése

Ha használni akarjuk a PGP-t elõször is saját kulcsunk, illetve kulcspárunk generálása az elsõ feladat. A home könyvtárunkban létre kell hozni egy .pgp nevû alkönyvtárat (mkdir .pgp), és ebbe belépve (cd .pgp) adjuk ki a következõ parancsot: pgp -kg

A program megkérdezi, hogy milyen méretû kulcsot szeretnénk generálni. Három választási lehetõséget kinál fel. Minél hosszabb kulcsot választunk, annál lassabb lesz maga a kulcs generálás és a titkosítás, de nagyobb biztonságot nyújt. Ezután kér egy felhasználói azonosítót a program. Célszerû megadni a nevünket és az e-mail cimünket, például:

Iksz Iplszilon <ikszipszilon@freemail.hu>

Ezután a PGP kér tõlünk egy jelszót. Fontos, hogy jól jegyezzük meg ezt a jelszót. A titkos kulcsunk használatához ugyanis ez, és az a fájl kell (secring.pgp) ahova ezután a program a generált titkos kulcsot teszi. A titkos kulcsot tartalmazó fájl és a jelszó azonosít bennünket.A PGP két fájlt használ a nyilvános/titkos kulcsok tárolására. Ezeket keyring-nek (kulcstartó) nevezik. A nyilvános kulcsok a pubring.pgp, a titkos kulcs(ok) a secring.pgp fájlban vannak. Amikor saját kulcsunkat generáljuk, nemcsak titkos kulcsunk kerül a secring-re, hanem nyilvános kulcsunk is a pubring-re.

Egy fájl titkosítása

Levél titkosításánál a puring.pgp kulcstartónak van szerepe. A következõ parancs segítségével Nagy János titkosíthatja a levelét Kis számára, Kis nyilvános kulcsának felhasználásával:

pgp -e level.txt Kis

A PGP program ekkor egy bináris outputot generál a level.pgp fájlba. Ha a parancsot kiegészítjük egy -a kapcsolóval, akkor karakteres outputot kapunk, amit levélként továbbíthatunk:

pgp -ea level.txt Kis

Az üzenetet -s kapcsoló-val írhatjuk alá. Az aláírást és a titkosítást végezhetjük egyszerre:

pgp -sea level.txt Kis

A PGP a secring.pgp kulcstartón talált elsõ titkos kulcsot használja az aláíráshoz.

Egy fájl dekódolása, aláírásának ellenõrzése

Üzenet dekódolásánál, aláírás ellenõrzésnél csak a kódolandó fáj nevét kell megadni.

pgp dekódolandó fájl név.pgp

A PGP felismeri a titkosítás módját, a kulcsot ami szerint kódolva lett, és kéri a felhasználótól a titkos kulcshoz tartozó jelszót. A jelszó ismerete szükséges a dekódoláshoz. Az aláírás ellenõrzése a pubring.pgp kulcstartó segítségével történik, szintén automatikusan.