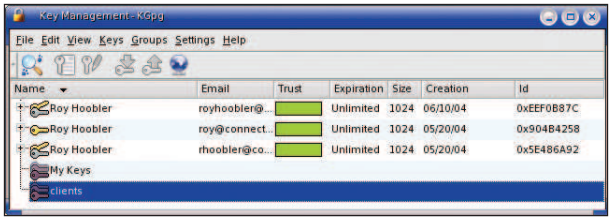
Levéltitkosítás egyetlen kattintással

A titkosított levelek küldését, fogadását és ellenőrzését grafikus eszközökkel végezve a biztonságos levelezés mindennapjaink természetes részévé válhat.

Jómagam egy hordozható gépet használok ***Linuxszal***, és nem szeretném, hogy mások is el tudják olvasni a leveleimet, ha netán rossz kezekbe kerülne. Leveleimet figyelik is, és az se tetszene, ha a rendszergazda belelátna a személyes dolgaimba. A ***GnuPG*** kiváló titkosítási lehetőséget kínál, és bárki számára elérhető. A ***KDE KGPG*** és ***KMail*** alkalmazásával a dolgok még egyszerűbbekké válnak. Írásomban a ***KGPG*** elektronikus levelek és fájlok titkosítására való használatát tárgyalom. Lehet, hogy a téma kicsit összetettnek fog tűnni, ám mire a végére érünk, bárki üzemképes rendszerrel rendelkezhet – ráadásul mindehhez elég lesz egy óra. Ha valakinek kérdése maradna, nyugodtan írjon a cikkben szereplő címemre, legalább ki tudja próbálni új, biztonságos levelezőrendszerét.

Mi az a GnuPG?

A ***Gnu Privacy Guard (GnuPG)*** az ***OpenPGP*** szabvány egy megvalósítása. A szabvány ***Philip Zimmerman*** munkája nyomán és ***PGP (Pretty Good Privacy)*** programjából fejlődött ki. A ***PGP*** 1991 tájékán jelent meg, jelenleg zárt alkalmazás. Az ***OpenPGP*** szabványok 1997-ben készültek el, a ***GnuPG 1.0***-s változata pedig 1999-ben látott napvilágot.
A ***GnuPG*** teljes egészében parancssori program, és meglehetősen bonyolult a kezelése. Szerencsére léteznek a használatát megkönnyítő eszközök, ezek közül a ***KDE***, a ***KGPG*** és a ***KMail*** szerepéről lesz szó.
A ***GnuPG*** és a ***PGP*** egymással kompatibilisek. Aki már használja a ***PGP***-t, azon belül is az ***IDEA*** algoritmust, annak némi munkával jár az áttérés, a többiek számára viszont semmilyen nehézséget nem okoz. Ha valakinek ***PGP 2.x*** változattal kell adatcserét folytatnia, esetleg ezt a programot szeretné lecserélni, akkor tanulmányozza át a cikkhez tartozó forrásokat, a ➲ www.linuxjournal.com/article/7863 címen.
Az adatvédelmi és adatbiztonsági házirendek összeállításához és betartatásához minden szervezetben vasfegyelemre van szükség. Amikor katonai hírszerzőként dolgoztam, a biztonságot nagyon komolyan vették. Ha valaki nem követte a házirendeket, annak súlyos következményei voltak. Minden szervezetben ki kell jelölni egy biztonsági igazgatót, akinek megfelelő hatalmat kell biztosítani az irányelvek követésének ellenőrzésére. Mint minden jól kidolgozott gyakorlati megoldásnál – mint például a ***CVS*** használata a kódok tárolására –, ha az embereket megtanítjuk, rászoktatjuk az érzékeny adatok titkosítására, akkor az eljárás hétköznapivá válik. A szervezet méretétől függően a házirend hatályba léptetése egy-négy hét alatt végbe vihető.



1. ábra A kulcskezelő eszköz segítségével a GnuPG kulcsok között név és levélcím alapján is kereshetünk

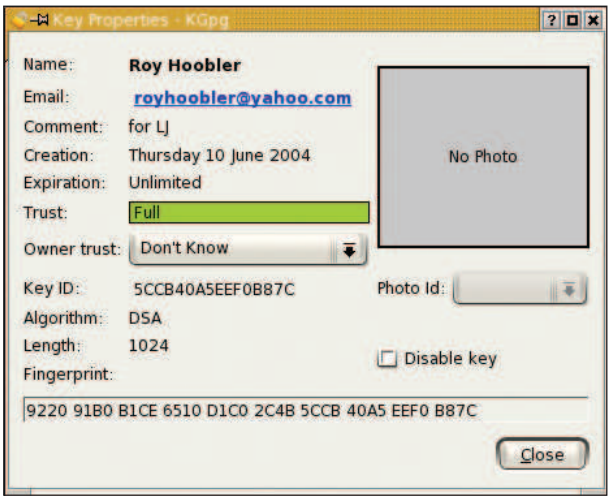
Saját kulcsunk előállítása

Példaként egy üzenetet fogok titkosítani, majd elküldöm azt munkahelyi címemről az ***rhoobler@comcast.net*** címemre. Mindkét fiókot ***KMail*** segítségével érem el. Ezután küldeni fogok egy titkosított választ a munkahelyi címemre. Természetesen előbb beállítom és elérhetővé teszem a ***comcast.net*** fiók kulcsait.
Miután telepítettük a ***KGPG***-t, a rendszertálcán kell hozzá tartoznia egy ikonnak. Ha nem lenne ilyen, akkor terminál alól, a `KGPG -k` paranccsal tudjuk elindítani. A `-k` kapcsolót ne hagyjuk el, ugyanis ez hozza elő a kulcskezelő felhasználói felületet. (*1. ábra*) A -k kapcsoló nélkül indítva a ***KGPG*** a háttérben, szolgáltatásként fut – ilyenkor jelenik meg a tálcán az ikonja. A felhasználói felület a tálcán található ikonra kattintva is megjeleníthető.
Első lépésként előállítom comcast.netes fiókom nyilvános és magánkulcsát. A kulcskezelőn belül válasszuk a ***Keys›Generate Key Pair (Kulcsok›Kulcspár előállítása)*** parancsot, amely egy meglehetősen egyszerű párbeszédpanelt jelenít meg. Ha az ***Expert Mode-ot (Szakértői mód)*** választjuk, a ***GnuPG*** terminálban indul. Most írjuk be nevünket, elektronikus levélcímünket, illetve a kívánt megjegyzést. A biztonsági házirendtől függően szükség lehet arra is, hogy a kulcsok lejáratát is beállítsuk.
A következő – rendkívül fontos – lépés a ***GnuPG*** jelszó megadása. Ha elhagyjuk, akkor egyetlen üzenetet sem tudunk majd megnyitni, a ***KGPG*** mindig jelszót fog kérni tőlünk, amikor bármit is megpróbálunk elolvasni. Várjunk

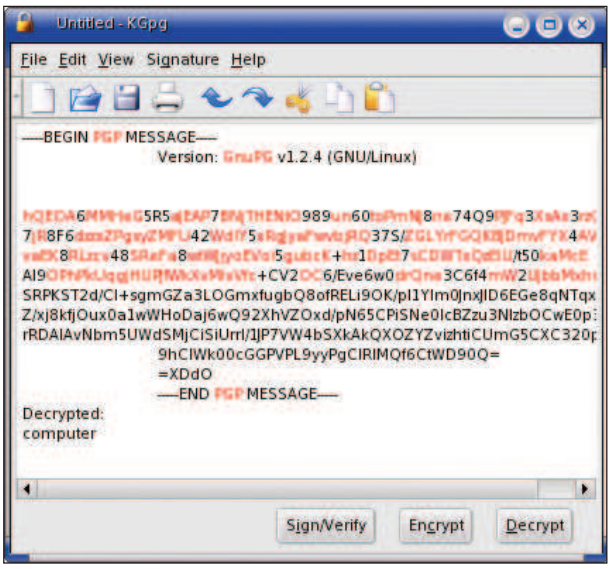
néhány másodpercet, amíg a *GnuPG* elkészíti kulcsainkat. A biztonság növelése érdekében javaslom egy ***visszavonási tanúsítvány (revocation certificate)*** elkészítését is (a fájl neve olyasféle legyen, mint az ***rhooblerrev.asc***). Ha ellopják vagy megtörik a gépünket, akkor ezt a tanúsítványt szétküldve értesíthetjük ismerőseinket nyilvános kulcsunk érvénytelenné válásáról.
Ennyi. Van nyilvános és titkos kulcsunk az ***rhoobler@comcast.net*** címhez. Két dolog van még hátra: a nyilvános kulcs és a titkos kulcs kimentése, utóbbi művelet elhagyható. A kulcsok kimentése külön-külön történik. A nyilvános kulcsnál az ***rhoobler.asc*** fájlnevet választottam, a titkos kulcs esetében pedig az ***rhooblerprivate.asc***-t. Vigyázzunk! Ha valaki megszerzi titkos kulcsunkat, és kitalálja jelszavunkat, akkor el tudja olvasni titkosított leveleinket, valamint a nevünkben tud titkosított, aláírt leveleket küldeni! A titkos kulcsot és a visszavonási kulcsokat kimentésük után írjuk CD-lemezre, helyezzük őket biztonságos helyre, majd töröljük a visszavonási (***rhooblerrev.asc***) és a titkos kulcsot (***rhooblerprivate.asc***) a merevlemezről.
A *GnuPG* a következő fájlokat helyezi el az egyes felhasználók *.gnupg* könyvtárába. A fájlokat csak az egyes felhasználók tudják írni és olvasni:

- *gpg.conf*: a *GPG* általános beállításai
- *pubring.gpg*: a nyilvános kulcsok listája
- *secring.gpg*: a biztonságos (magán) kulcsok listája
- *trustdb.gpg*: adatbázisfájl, az egyes személyek közötti megbízási viszonyokat adja meg

A kényelem kedvéért most az ***rhoobler@comcast.net*** nyilvános kulcsát egy alapértelmezett kulcskiszolgálóra mentem ki. A kulcskezelő eszköz segítségével válasszuk ki a kulcsot, kattintsunk rá az egér jobb gombjával, majd válasszuk az ***Export Public Key(s) (Nyilvános kulcs(ok) kimentése)*** parancsot. Újabb egyszerű párbeszédpanel jelenik meg, három lehetőséggel. Én az alapértelmezett kulcskiszolgálót választottam, majd az ***OK*** gombra kattintottam. A kulcskiszolgálót a ***Settings (Beállítások)*** menüben adhatjuk meg, alapesetben ez a ***subkeys.pgp.net***, ami – legalábbis nálam – mindig működött. Megtehetjük azt is, hogy fájlba mentjük ki a kulcsot, majd elektronikus levélben továbbítjuk, esetleg a weboldalunkon tesszük közzé. Abból, hogy bárki megismerheti a nyilvános kulcsunkat, semmi gondunk nem származhat, ám módot kell adnunk a kulcs eredetiségének ellenőrzésére – erről később lesz szó. Aki rendelkezik a nyilvános kulcsunkkal, az képes lesz fájlokat úgy titkosítani, hogy azokat csak mi tudjuk majd megnyitni.
Eljutottunk tehát odáig, hogy tudunk fájlokat titkosítani és titkosított leveleket küldeni. Mindennek azonban csak akkor van értelme, ha van kivel megosztanunk adatainkat. A próba kedvéért én átsétáltam a másik gépemhez, majd ugyanezeket a lépéseket végrehajtva létrehoztam a kulcsokat a munkahelyi levélfiókomhoz.
A következő művelet az ***rhoobler@comcast.net*** nyilvános kulcsának beemelése a kulcskiszolgálóról a kulcskezelő segítségével, majd a földgömb ikon vagy a menü ***File›Key Server Dialog (Fájl›Kulcskiszolgáló párbeszéd)*** parancsának kiválasztása. Adjuk meg az elektronikus levélcímet, majd emeljük be a kulcsot. Mielőtt használni kezdenénk a kulcsot, válasszuk ki a főablakban, majd válasszuk a menü ***Keys›Sign Keys (Kulcsok›Kulcsok aláírása)*** parancsát.
Ha nagyobb csoportot akartam volna összeállítani, akkor létrehozhattam volna egy saját kulcskiszolgálót, aláírhattam volna a kulcsokat és továbbadhattam volna őket. Egy másik megoldás, hogy mindenki elküldi levélben másoknak saját kulcsát, majd a való életben is találkoznak, amikor ellenőrzik és aláírják egymás kulcsát. Így jön létre a bizalmi hálózat. Én például aláírom ***Berci*** kulcsát, ő pedig ***Katiét***. Ha levelet kapok ***Katitól***, akkor kulcsát nyugodtan hozzáadhatom megbízási viszonyokat tároló adatbázisomhoz.
A kulcsoknak van egy ujjlenyomatuk, és ha nem vagyok biztos abban, hogy egy kulcs hiteles-e, akkor megnézhetem az ujjlenyomatát, majd felhívhatom a tulajdonosát, és segítségével ellenőrizni tudom a kulcsot. Az ujjlenyomat a kulcskezelő segítségével tekinthető meg, ehhez válasszuk ki a kulcsot, majd válasszuk a menü ***Edit Key (Kulcs szerkesztése)*** parancsát. (*2. ábra*)



2. ábra Ha ellenőrizni akarjuk egy levél hitelességét, akkor hívjuk fel a küldőt, és egyeztessük vele a kulcs ujjlenyomatát



3. ábra A vágólap visszafejtése

Fájlok titkosítása

A *KGPG*-t szinte észrevétlenül beépítették a *KDE*-be és a *KDE*-s alkalmazásokba. Ennek előnyeit leginkább a *Konqueror* böngésző használatakor élvezhetjük. A *KGPG* telepítése után kattintsunk az egér jobb gombjával a kívánt dokumentumra, majd az ***Actions (Műveletek)*** menüben létrehozhatjuk a dokumentum titkosított változatát. Lehetőség nyílik az eredeti példány megsemmisítésére is, aminek főleg akkor van értelme, ha a titkosítatlan változat megtartása valamiért nemkívánatos. A fájlok titkosításakor több kulcsot is kiválaszthatunk, így több különböző személy is el tudja olvasni a dokumentumot. Ha az eredeti fájlt megsemmisítjük, akkor ügyeljünk arra, hogy a titkosítás során saját kulcsunkat is kiválasszuk. Nálam, ha például csak az ***rhoobler@comcast.net*** kulcsot választom ki, akkor én leszek az egyetlen, aki vissza tudja fejteni a fájlt.

Elektronikus levél küldése

Végre készen állunk arra, hogy titkosított leveleket küldjünk. A *KMail* (vagy a *Kontact*) segítségével írjuk meg üzenetünket. Nálam a címzett az ***rhoobler@comcast.net***. Kattintsunk a *Lock* ikonra, vagy válasszuk az ***Options›Encrypt (Beállítások›Titkosítás)*** parancsot a menüből. Amikor a ***Send (Küldés)*** gombra kattintunk, egy párbeszédpanel jelenik meg. Ha nem látjuk a címzett kulcsát, kattintsunk a ***Refresh (Frissítés)*** gombra. Ha nem írtuk alá a kulcsot, nem fog megjelenni, ekkor vissza kell lépnünk, a kulcskezelő segítségével alá kell írnunk a kulcsot, majd rá kell kattintanunk a Refresh gombra. Fejezzük be az üzenetet, majd kattintsunk a *Send* gombra.
A *KMail* esetében az üzenetek visszafejtése beépített szolgáltatás. Ha titkosított üzenetet kapunk, csak be kell írnunk a jelszót, és máris megnyílik az üzenet. Ha titkosított üzenetet küldünk, és a címzett címe szerepel a kulcsgyűrűnkben, akkor a levél titkosítása és elküldése önműködően történik. Az üzenetet egyszerre több embernek is elküldhetjük titkosítva, feltéve, hogy mindannyiuk nyilvános kulcsával rendelkezünk. További lehetőség a fájl *KGPG* segítségével végzett titkosítása, majd mellékletként való továbbítása.
A *KMail* önműködően visszafejti a mellékleteket; ehhez egyébként a megtekintés, és nem a megnyitás parancsot kell választanunk. Ha webes levelező ügyfelet használunk, akkor töltsük le a fájlt, majd a *Konquerorral* tudjuk visszafejteni vagy megnézni a tartalmát. Ha olyan webes levelezőt használunk, mint például a *Yahoo mail*, akkor másoljuk ki a vágólapra a titkosított üzenetet, az egér jobb gombjával a tálca ikonjára kattintva válasszuk a ***Decrypt clipboard (Vágólap visszafejtése)*** parancsot, majd illesszük be a vágólap tartalmát a *KGPG* szerkesztőjébe. Hasonló módon lehet elvégezni az üzenetek titkosítását is.

Elektronikus levél aláírása

A titkosításnál népszerűbb alkalmazás a levelek aláírása. Ilyenkor maga a szöveg nem kerül titkosításra, ám az aláírás igazolja az üzenet hitelességét. Ha minden levelemet aláírom, mert ez a házirend, és valaki kap tőlem egy aláíratlan vagy hibás aláírású levelet, akkor nyugodtan feltételezheti, hogy hamis, és értesítheti a megfelelő személyt. A *KMail* a leveleket különféle színekkel jelöli meg, a színekből tudhatjuk, hogy az egyes üzenetek megbízható féltől érkeztek-e. Sárgák az aláírt, zöldek az aláírt és megbízható levelek.

Csoportok létrehozása és egyéb lehetőségek

A *KGPG* további érdekes szolgáltatása a kulcscsoportok létrehozásának lehetősége. Lehet például egy Felügyelet csoportom, amelybe három-négy kulcsot helyezek el. Üzenet küldésekor ki tudom választani a csoportot. Később, ha az egyik címzett továbbítja a levelet a csoport egy másik tagjának, akkor az már készen fog állni az elolvasásra.
A ***Configure KGPG (KGPG beállítások)*** alatt az ***ASCII Armor (ASCII védelem)*** beállítást is érdemes engedélyezni, ahogy valószínűleg ez is az alapbeállítás. Ilyenkor az aláírások és a titkosítás tisztán szövegesen tárolódnak, így könnyebben lehet továbbítani, nyomtatni, másolni és beilleszteni az anyagot. Az ***ASCII*** védelem kikapcsolásakor bizonyos fájlok bináris formátumot kapnak, ami esetleg gondokat okozhat.

Összegzés

Amint lesz időm, ígérem, minden titkosított bejövő levelemet vissza fogom fejteni, és válaszolni is fogok. Mivel a *KGPG* a *KDE* része, a legtöbb *Linux* terjesztésben eleve megtalálható. Néhány kulcsot létrehozni és kipróbálni a lehetőségeket mindössze egy-két órát igényel.
A *GnuPG* és a *KGPG* telepítése után a kulcsok és a titkosítás használata a mindennapok gyakorlatában sem okozhat gondot, ha ügyelni akarunk a biztonságra. Eddigi munkáim során mindig nagy figyelmet fordítottak az összeköttetések és például az *SSL* feletti tranzakciók biztonságára, ám a fájlok és az elektronikus levelek valahogy kiestek ebből a körből. *KDE* használatakor a biztonságos levelezőrendszer megteremtése nem okozhat különösebb nehézséget. Érdemes úgy kezdeni, hogy először csak a felettünk álló vezetőknek szánt leveleket titkosítjuk; vagy jó ötlet lehet olyan magánmappát nyitni a hálózaton, amely kizárólag titkosított dokumentumokat tárol. Ha ezeket a biztonsági házirendeket már elfogadtattuk, a szélesebb körű titkosítást is könnyebb lesz megvalósítani.

Linux Journal 2005. január, 129. szám

Roy Hoobler a Connect Computing, Inc. tulajdonosa. (www.connectcomputing.com) Független tanácsadóként, a zárt szoftverek világában szerzett tíz éves tapasztalatával vállalkozása jelenleg kisvállalkozásokat segít a Linux használatában és nyílt forrású üzleti alkalmazások megvalósításában.