François, tudsz titkot tartani?

Ismerjük meg a nyilvános kulcsú titkosítás alapjait, és a GNU Privacy Guard csatlakoztatását levelezőprogramunkhoz.

Valóban szégyen, François, a következő alkalomra egyszerűen meg kell győződnünk arról, hogy elérhető-e. Minden más hibátlannak tűnik, mon ami, az összes munkaállomás a beléptetésre készen áll. Nagyszerű! Óh, látom, vendégeink már meg is érkeztek. François, irány a borospince keleti szárnya, az öreg zárt ajtó mellett találsz egy kis készletet az 1999-es Côte-Rôtie-ból. Igen, azt az ajtót soha nem tudtuk kinyitni. Siess François, megígérem, hogy semmi ijesztőt nem találsz arrafelé. Foglaljatok helyet, mes amis. A mai menünk majdnem tökéletes, de egy fogás sajnos hiányzik belőle. Talán a Côte-Rôtie Rhône, ez a pikáns és misztikus vörös enyhíteni fogja hiányérzetünket. Mára nagyon szerettem volna elkészíteni a híres Crème Linuxaise-t, de gondok adódtak. Tudjátok, ez egy régi családi recept, nem szeretném megkockáztatni, hogy rossz kezekbe kerüljön. Elektronikus levélben való küldését sem vállaltam attól tartva, hogy valaki lehallgatja a hálózatot, különben François már elő is készíthette volna. Ilyen nagy titokról van szó!

A következő alkalommal mindez már nem jelenthet gondot, ugyanis az étterem minden felhasználóját GnuPG-vel és nyilvános kulcsú titkosítással szerelem fel, így kényes adatokat is biztonságosan küldhetünk majd. A GnuPG teljes neve GNU Privacy Guard (GNU magánéletőr).

A GnuPG az üzenetek és adatok általános titkosítását teszi lehetővé. Ez a PGP (Pretty Good Privacy) jogdíj nélküli, nyílt forrású megfelelője. Számos linuxos levelezőprogram teszi lehetővé, hogy GnuPG-vel titkosított leveleket küldjünk és fogadjunk, ezt szeretném ma bemutatni nektek.

A legtöbb telepítőkészlet tartalmazza a GnuPG-t, amennyiben a feltelepített rendszerünkön nem találjuk, először a telepítőlemezeken érdemes keresgélnünk. A legfrissebb változatot a ➲ http://www.gnupg.org címről is letölthetjük, de előbb járjuk körül egy kicsit a témát.

Hol is tartottam? Ja igen. Az előzményeket megvizsgálva, láthatjuk, hogy minden titkosítási eljárás egy megosztott kulcsállományon alapul. A kulcsot, amellyel az üzenetet titkosítottuk, annak a személynek adjuk oda, akivel titkosított kapcsolatot fenn szeretnénk tartani. Gondoljunk a titkos dekódoló gyűrűre, és már nem is állunk messze az igazságtól. A baj csak az, hogy aki megszerzi a kulcsot, minden üzenetünket meg tudja fejteni. A GnuPG esetén az üzenetek titkosítására két kulcsot használunk, az egyik

1. kép A KMail a kulcs importálásának megerősítését kéri

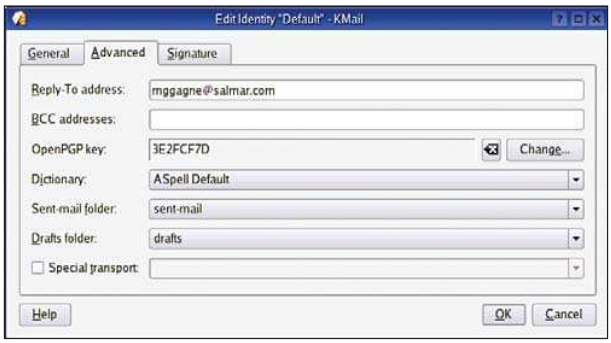
2. kép A KGpg-vel nem jelent gondot a kulcsok kezelése

a személyes kulcs (private key), amit féltve őrzünk és senkinek nem adunk ki. Amikor egy üzenetet titkosítunk, a személyes kulcsunk és egy nyilvános kulcs (public key) segítségével tesszük. A nyilvános kulcs nem a sajátunk, hanem azé a személyé, akinek az üzenetet küldeni szeretnénk, például François-é. A titkosító-visszafejtő folyamathoz mindkét kulcs szükséges, és ha valaki csak az egyikkel rendelkezik, nem megy vele semmire, ezért nem adjuk ki soha a kezünkből a személyes kulcsunkat. Ahhoz, hogy ilyen szupertitkos tevékenységet folytathassunk, előbb el kell készítenünk a kulcspárunkat, amely egyrészt a személyes (nagyon jól őrzött) kulcsunkat, másrészt pedig a nyilvános (a barátainknak szétküldendő) kulcsunkat tartalmazza. Ezt az alábbi paranccsal tehetjük meg:

```
gpg --gen-key
```

Ezt egy kis kérdés-felelet szakasz követi. Az első kérdés a titkosító algoritmussal, a rejtjelezéssel kapcsolatos. Az alapértelmezett a DSA és ElGamal, fogadjuk is el. Amikor a kulcs hosszát kell megadnunk, a 768, 1024 és 2048 közül

3. kép A KMail beállítása a GnuGP-vel való titkosítás használatára



4. kép A nyilvános kulcsunk megadása a KMailben

választhatunk. Mivel a DSA szabványos kulcshossza 1024, most válasszuk ezt. Ezt követően a kulcs érvényességének lejártát kell megadnunk, alapértelmezett esetben az érvényesség nem jár le, de valahány napot, hetet, hónapot, akár még évet is választhatunk. Egyelőre itt ismét fogadjuk el az alapértelmezett beállítást és erősítsük is meg választásunkat. Végül a program a kulcs használójának nevét, elektronikus levélcímét és egy megjegyzést kér tőlünk.
Már csak a jelszókifejezés megadása maradt hátra, ez a befejező lépés. Olyat válasszunk, ami biztonságos, de megjegyezhető. Amikor ezt is beírtuk, a GnuPG előállítja számunkra a kulcspárunkat. Az eredményt pedig a saját könyvtárunkban lévő *.gnupg* könyvtárban ellenőrizhetjük:

```
$ cd /home/marcel/.gnupg
$ ls
gpg.conf      pubring.gpg   random_seed
secring.gpg   trustdb.gpg
```

A *gpg.conf* fájl a gpg parancs alapértelmezett beállításait tartalmazza, ezért hasznos olvasmány. A *pubring.gpg* és *secring.gpg* fájlok rendkívül fontosak. Azonnal készítsünk róluk biztonsági másolatot, és helyezzük biztonságba a számítógépen kívül. Ezeket nem szabad elveszítenünk – a *secring.gpg* tartalmazza a személyes titkos kulcsunkat. Az utolsó fájl, a *trustdb.gpg* a bizalmi adatbázis. Ez azt a bizalmi szintet határozza meg, amit az összegyűjtött nyilvános kulcsokhoz rendelhetünk. Ahhoz, hogy a felhasználók egymás közt titkosított adatokat cserélhessenek, a kulcsaikat is egymás rendelkezésére kell bocsátaniuk. Kitalálhatjuk, hogy kulcs exportálására a `--export` kapcsolót használhatjuk, ami mellé valószínűleg a `-a` kapcsolót is be fogjuk írni, hogy a kimenet ASCII formátumú legyen:

```
gpg -a --export 3E2FCF7D > marcelkey.asc
```

A létrejövő fájl egy egyszerű ASCII szövegfájl; hogy miként juttatjuk el a címzettekhez, rajtunk múlik. Léteznek olyan kulcsok tárolására szolgáló kiszolgálók, ahova a nyilvános kulcsunkat feltölthetjük, bárki számára letölthetővé téve őket (ez jól jöhet, ha sokfelé szeretnénk szétosztani a kulcsunkat). Sőt kulcscserélő összejöveteleket (key-signing parties) is rendeznek, amelyeken a tagok összejönnek, és kicserélik nyilvános kulcsaikat vagy levélmellékleteiket.
A kulcs fogadójának a következő módon kell importálnia a kulcsot:

```
gpg --import marcelkey.asc
```

Az alábbi paranccsal bármikor megnézhetjük a kulcskarikánkon összegyűjtött kulcsainkat:

```
gpg --list-keys
```

A parancs eredménye attól függ, hogy hány kulccsal rendelkezünk, és a következő listából láthatjuk, hogy mire is számíthatunk. Különösen az 1024D után következő hexadecimális szám fontos, ez ugyanis a kulcsazonosító, amelyre a jövőben hivatkozni fogunk:

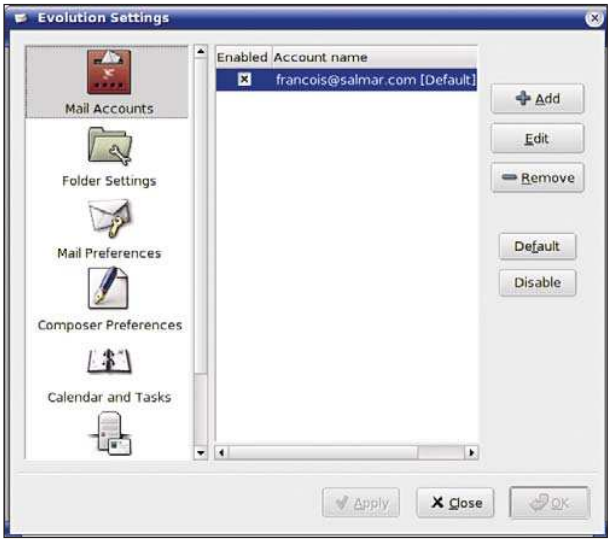
```
/home/marcel/.gnupg/pubring.gpg
-------------------------------
pub  1024D/3E2FCF7D 2004-01-07 Marcel Gagné
(Writer and Free Thinker at Large)
<mggagne@salmar.com>
sub  1024g/B24717BE 2004-01-07

pub  1024D/EE392B87 2004-01-07 Francois (I am but
a humble waiter) <francois@salmar.com>
sub  1024g/F4E07040 2004-01-07
```

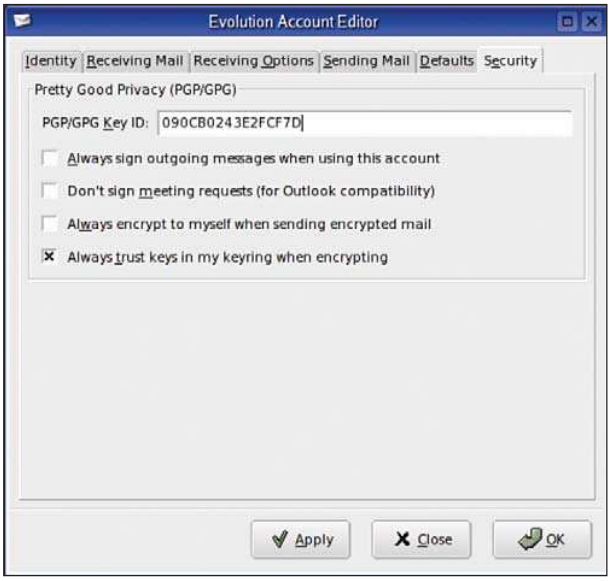
Mielőtt barátaink kulcsaival leveleket kezdenénk kódolni, először az érvényesség ellenőrzésével hitelesítenünk szükséges őket. Ez két lépésből áll. Ha teljesen biztosak vagyunk a kulcs eredetét illetően, az elsőt kihagyhatjuk, ugyanis ez a kulcs ujjlenyomatát szerzi meg:

```
$ gpg --fingerprint francois
pub  1024D/EE392B87 2004-01-07 Francois (I am but
a humble waiter) <francois@salmar.com>
Key fingerprint = 8C5B 775C 33F8 E97C 5ADC  019D
➥C6C8 4B83 EE39 2B
sub  1024g/F4E07040 2004-01-07
```

Láthatjátok, hogy a fenti parancsban a kérdéses személy nevét használtam, ez része a kulcshoz tartozó adatoknak.



5. kép Az Evolution levélfiók-szerkesztője



6. kép A GnuPG-kulcsunk megadása az Evolutionben

Ha a kulcsadatok között több azonos nevű kulcsunk akad, helyette a kulcsazonosítót is használhatjuk. Kérjük meg barátunkat – ennek az ujjlenyomatnak az ellenőrzéséhez –, hogy ugyanezzel a módszerrel ő is ellenőrizze személyes kulcsának ujjlenyomatát. A befejező lépés a kulcs hitelesítése. Ezt a `--edit-key` kapcsolóval tehetjük meg:

```
gpg --edit-key francois
```

Egyszerű az egész folyamat. A program megerősítést kér arra vonatkozóan, hogy tényleg hitelesíteni szeretnénk-e ezt a nyilvános kulcsot, majd végső nyomatékként a jelszókifejezést is bekéri. Ezt minden egyes személlyel végig kell csinálnunk, akivel titkosított leveleket szeretnénk váltani, de ha egyszer elkészültünk, többé semmi sem állhat a titkos üzenetek áramlásának útjába.

Mellesleg számos tetszetős grafikus eszköz létezik a GnuPG-hez, ezek lényegében barátságos külsőt adnak a parancssoros eszköznek. A KDE részeként kapjuk a KGpg-t, amely jól beépül munkakörnyezetünkbe és levelezőrendszerünkbe. Például, ha valaki egy levél mellékleteként egy nyilvános kulcsot küld a KMailen keresztül és a KGpg (a parancs neve `kgpg`) fut, akkor ahelyett, hogy a mellékletet fájlként kellene mentenünk, meghívjuk a parancssort és végrehajtjuk a fenti lépéseket. Az *1. képen* láthatóhoz hasonló barátságos felugró ablaknak kell megjelennie.

Ezzel a tálcán helyet foglaló kis eszközzel szerkeszthetjük is a kulcsokat; újakat vehetünk fel, eltávolíthatunk, megváltoztathatjuk a bizalmi szintet, vagyis mindenre képes, amit a parancssoros GnuPG-vel is végrehajthatunk, de itt csak egy egérkattintásba kerül. Ezenkívül a világhálón lévő kiszolgálókon kulcskeresést is végre tud hajtani, illetve fotóazonosítást használ. Az egyéb KDE-eszközökbe való beépítése annyit jelent, hogy a titkosításhoz a húzd és ejtsd módszert használhatjuk, és a Konquerorból vagy a vágólapról is egyetlen egérkattintással elérjük a GnuPG lehetőségeit.

A KDE 3.1-esnél a KGpg még csak kiegészítés, a KDE 3.2-es változatban azonban már a csomag szerves részét alkotja. A *2. képen* működés közben láthatjuk a KGpg-t.

Egy másik grafikus felügyeleti eszköz, amely figyelmet érdemel, a `gpa`. Ez a GnuPG projekt alapértelmezett GNU Privacy Assistant programja és hivatalos kulcskarika szerkesztője, amely a ➲http://www.gnupg.org címről tölthető le.

Itt az ideje, hogy a titkosított levelek küldését ki is próbáljuk. Nyissuk meg a KMailt, kattintsunk a menüsor ***Settings*** (beállítások) menüjére és válasszuk ki a ***Configure KMail*** (beállítások) menüpontot. Ennek hatására a ***Configure KMail*** (beállítások – KMail) párbeszédablak fog megjelenni. A bal oldalon lévő sávban keressük meg a ***Security*** (biztonság) ikont (*3. kép*).

A jobb oldalon megjelenő ablakban három fület láthatunk: ***General*** (Általános), ***OpenPGP*** és ***Crypto Plugins*** (titkosítási bővítőmodulok). Pillanatnyilag az ***OpenPGP*** fül érdekel bennünket. Ezen a fülön keressük meg a ***Select encryption tool*** (a használni kívánt titkosítási eszköz) feliratú lenyíló listát és ebből válasszuk ki a ***GnuPG – GNU Privacy Guard*** tételt. Egyelőre ne válasszuk ki a ***Sign and encrypt all messages automatically*** (az üzenetek önműködő aláírása és titkosítása) lehetőséget. A jelszókifejezést érdemes megőrizni a memóriában (***Keep the passphrase in memory***), de a program az első titkosított levél előfordulásakor így is kérni fogja. Kattintsunk az ***Apply*** (alkalmazás) gombra.

Ezután kattintsunk a bal oldalon lévő ***Identity*** (azonosító) fülre. Hacsak nem hoztunk létre több levelezési fiókot, itt egyetlen bejegyzést találunk. Kattintsunk a ***Modify*** (módosítás) gombra és a megjelenő párbeszédablakon válasszuk ki az ***Advanced*** (speciális) fület. E panel közepén (*4. kép*) találunk helyet az OpenPGP kulcs számára. Ez a saját, személyes kulcsunk. Kattintsunk a ***Change*** (Módosítás) gombra, ennek hatására egy ablak jelenik meg, amelyben a személyes kulcsunkhoz tartozó adat helyét jelölhetjük ki.

Ha készen vagyunk, kattintsunk az ***OK*** gombra az ***Edit Identity*** (azonosító módosítása) ablak bezárásához, majd ismét az ***OK*** gombra, amellyel ezúttal a ***Configure KMail*** (beállítás – KMail) ablakból lépünk ki. Ahhoz, hogy a KMail megfelelő módon újra beolvassa a beállított értékeket, állítsuk le a programot, majd indítsuk el ismét.

Elvileg készen állunk rá, hogy titkosított leveleket küldjünk. Ha a kulcskarikánkon már szerepel barátunk nyilvános kulcsa és hitelesítettük is, nincs más teendőnk, mint megírni a levelet. Nyissunk egy új levelet és írjuk bele a mondandónkat. Ha küldésre készen állunk, kattintsunk az üzenet menüsorának ***Options*** (jellemzők) menüjére. Itt két titkosítással kapcsolatos lehetőséget vehetünk észre. Az egyik a ***Sign Message*** (az üzenet elektronikus aláírása), a másik pedig az ***Encrypt Message*** (az üzenet titkosítása). A levél aláírása azt jelenti, hogy a nyilvános kulcsunkat elektronikus aláírásként mellékeljük az üzenethez, de nem titkosítjuk. A levél címzettje ily módon rendelkezik egy eszközzel annak ellenőrzésére, hogy a levél valóban a feladótól származik, ha meg akar győződni erről. Mivel az üzenet nem titkosított, bárki elolvashatja. Ez az eszköz csak annak megerősítésére szolgál, hogy valóban attól a személytől kaptuk a levelet, akit feladóként látunk feltüntetve. A titkosítás annyiban jelent további lépést, hogy azt a nyilvános kulcsot használjuk, amit a barátunk bocsátott rendelkezésünkre a titkosításhoz. A KMail mindkét esetben az üzenet elküldése előtt kérni fogja a jelszókifejezést.
Sajnos nem minden levelezőprogram használja ugyanazokat a szabályokat a titkosításhoz. Túl egyszerű is lenne, non? Feltételezett esetünk leírásához használjuk fel a 17-es asztalnál ülő két személyt, Larryt és Michaelt. Mindketten kényes üzleti adatokat szeretnének küldeni, tehát az információknak titkosított formában kell haladniuk. Larry a levelezéséhez az Evolutiont használja, Michael pedig a KMailt. A KMail esetében már megismertük a titkosított levelek kezelésének módját, most pedig vizsgáljuk meg, hogyan történik mindez a Ximian Evolution esetében. Kattintsunk a futó Evolution programunk bejövő üzeneteket tároló könyvtárára. Ezután válasszuk ki a menüsor ***Tools*** (eszközök) menüjének ***Settings*** (beállítások) menüpontját. Ekkor az ***Evolution Settings*** (az Evolution beállításai) ablaknak kell előttünk lennie (*5. kép*). Amennyiben a ***Mail Accounts*** (postafiókok) ikon a bal oldali navigációs sávban még nincs kiválasztva, tegyük meg. A legtöbb embernek egyetlen fiókja van. Ha mégis többel rendelkezünk, válasszuk ki azt, amelyiket a titkosított üzenetek küldésére szeretnénk használni, majd kattintsunk a jobb oldalon lévő ***Edit*** (szerkesztés) gombra. Erre a számos fület tartalmazó ***Account*** (postafiók-szerkesztő) párbeszédablak jelenik meg. A bennünket pillanatnyilag érdeklő fül a ***Security*** (Biztonság) feliratot viseli. Keressük meg a ***PGP/GPG Key ID*** (PGP/GPG kulcs azonosítója) feliratú mezőt és ide írjuk be kulcsazonosítónkat. A párbeszédablak bezárásához kattintsunk az ***OK***-ra, majd az Evolution beállítóablakából való kilépéshez ismét válasszuk az ***OK*** gombot. Feltéve, hogy Larry és Michael kicserélték nyilvános kulcsaikat, Larry készen áll rá, hogy titkosított üzeneteket küldjön. Ehhez először a megszokott módon létrehoz egy üzenetet, majd még az elküldés előtt kipipálja a menüsor ***Security*** (biztonság) menüjéből a ***PGP Encrypt*** (PGP titkosítás) lehetőséget. Amikor Larry a ***Send*** (küldés) menüpontra kattint, a program kérni fogja tőle a GPG jelszókifejezését, amennyiben tudja, az üzenetet azonnal elküldi. Mielőtt továbblépnénk, meg kell említenem, hogy a ***Security*** (biztonság) menüből ugyanígy választható ki a ***PGP Sign*** (PGP-aláírás) lehetőség is, ha az üzenetet csupán alá szeretnénk írni.

Bár ez a kódolás-dekódolás nagyszerű, akadnak azért nehézségek is. Például nagyon sok levelezőprogram (a KMail is ezek közé tartozik) a levélen belül végzi el a kódolást, míg néhány más program, így az Evolution is, más utat követ, ezeknél a kódolt üzenet MIME-csatolmányként jelenik meg. Ebből következően egy KMailből (vagy Eudorából, vagy Outlookból) érkező levelet az Evolutionben csak úgy tudunk megnézni, ha előtte szöveges állományként mentjük, majd a következő paranccsal dekódoljuk:

```
gpg -d message.txt
```

Egy Evolutionban kódolt, KMailnek (vagy néhány másik programnak) küldött levél esetében a csatolt fájlt – és nem a levelet magát – szükséges hasonlóan mentenünk, majd a fenti módszerrel dekódolnunk.
Nagyon sok levelező ügyfélprogram érhető el Linuxra. A KMail és az Evolution népszerű grafikus programok, ugyanakkor a Mozilla sem maradhat ki a sorból. A Mozilla használói számára az Enigmail nevű bővítmény (plugin) teszi lehetővé az üzenetek zökkenőmentes aláírását és titkosítását. A szöveges ügyfélprogramok szintén támogatják a titkosítást, akár önmagukban, akár bővítményeiken keresztül, erre a `mutt` és a `pine` mutat két népszerű példát.
Mon dieu! Ilyen hamar elszaladt az idő? Attól tartok, mes amis, hogy a záróra megint utolért bennünket. François még egyszer teletölti a poharaitokat, mielőtt elválnánk. Miközben kényelmesen szopogatjátok az utolsó kortyokat, hozzátok létre és cseréljétek ki egymással a saját nyilvános kulcsaitokat. Talán valamelyiktekkel megosztom majd a Crème Linuxaise receptjét – természetesen a megfelelő biztonsági intézkedések megtétele mellett. Ki tudja, talán éppen a túlzott biztonság az oka, hogy az az ajtó a pincében még mindig ilyen szorosan zárva van. Viszontlátásra a következő alkalommal! A vôtre santé! Bon appétit!

Linux Journal 2004. április 120. szám

Marcel Gagné (mggagne@salmar.com)
Mississaguában, Ontario államban él.
Ő a szerzője a Kiskapu kiadásában tavaly szeptemberben megjelent Linux-rendszerfelügyelet (ISBN 96-9301-40) című könyvnek.

KAPCSOLÓDÓ CÍMEK

A Gnu Privacy Guard (GnuPG) oldala
➲ http://www.gnupg.org
A KMail honlapja
➲ http://kmail.kde.org
A Mozilla elérhetősége
➲ http://www.mozilla.org
A Mozilla Enigmail webcíme
➲ http://enigmail.mozdev.org
A Ximian Evolution oldala
➲ http://www.ximian.com/products/evolution