عنوان: **ساخت کلیدهای امنیتی GunPG**
نویسنده: علی یگانه مقدم
تاریخ: ۱۳۹۴/۰۸/۰۲ ۱۹:۳۵
آدرس: www.dotnettips.info
گروه‌ها: Security, Cryptography, Linux

یکی از روش‌های ارسال و رمزگذاری اطلاعات، استفاده از کلیدهای امنیتی مورد استفاده‌ی در سیستم یونیکس یا GnuPG است. استفاده از نرم افزار Gnu Privacy Guard یا گارد حفاظتی گنو، به ما این اجازه را می‌دهد که بتوانیم اطلاعاتمان را در بسترهای ارتباطی، با خیالی راحت‌تر ارسال کنیم و تا حد زیادی مطمئن باشیم که تنها فرد هدف توانایی دسترسی به اطلاعات را خواهد داشت. گارد امنیتی گنو زیر مجموعه‌ای از پروژه‌ی گنو است که دولت آلمان پایه ریز اصلی آن بوده است. این نرم افزار از یک روش رمزگذاری ترکیبی استفاده می‌کند که الگوریتم‌های کلیدهای برابر(متقارن) و کلیدهای عمومی (نامتقارن) جهت تبادل آسان کلید را شامل می‌شود. در حال حاضر که نسخه‌ی دو این برنامه ارائه شده است، برای رمزگذاری‌ها از کتابخانه‌ای به اسم libgcrypt استفاده می‌کند. یکی از مشکلات فعلی این پروژه، عدم وجود apiهای مناسبی جهت دسترسی راحت‌تر است و برای حل این مشکل، GPGME که مخفف GnuPG Made Easy ایجاد شد. بسیاری از برنامه‌ها و پلاگین‌های ارسال اطلاعات، امروزه همچون ارسال ایمیل، از این کلیدها بهره می‌برند.

پروژه‌های مرتبط با این قضیه اسم‌های مشابهی دارند که گاها بعضی افراد، هر کدام از اسم‌ها را که دوست دارند، به همه اطلاق می‌کنند؛ ولی تفاوت‌هایی در این بین وجود دارد:

OpenPGP : یک برنامه نیست و یک قانون و استانداری برای تهیه‌ی آن است؛ که رعایت اصول آن الزامی است و برنامه‌ی بالا، یک پیاده سازی از این استاندارد است.
PGP : یک برنامه، برای رمزگذاری اطلاعات است که مخفف Pretty Good Privacy است.
و **GnuPG یا GPG** که در بالا به آن اشاره شد.
برای ساخت کلید، ما از دستور یا برنامه‌ی GPG که که عمدتا در همه‌ی لینوکس‌ها مثل دبیان و مشتقات آن نصب است، استفاده می‌کنیم و اگر نصب نیست از طریق توزیع آن اقدام نمایید.
در صورتیکه از ویندوز استفاده می‌کنید، نیاز است ابتدا خط فرمان یونیکس را روی آن نصب کنید. برنامه‌ی Cygwin این امکان را به شما می‌دهد تا خط فرمان یونیکس و دستورات پیش فرض آن را داشته باشید. این برنامه در دو حالت ۳۲ بیتی و ۶۴ بیتی ایجاد شده است. از آنجا که گفتیم این برنامه شامل دستورات پیش فرض آن است، برای همین GPG باید به صورت یک بسته‌ی جداگانه نصب شود که در سایت آن می‌توانید بسته‌های مختلف آن‌را برای پلتفرم‌های مختلف را مشاهده کنید.

ساخت کلید

برای ساخت کلید دستور زیر را صادر کنید:

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

اگر از نسخه‌های جدیدتر GPG استفاده می‌کنید، گزینه‌هایی به شکل زیر ایجاد می‌شوند؛ ولی اگر خیر، ممکن است تعداد و شماره‌ی گزینه‌ها متفاوت باشند که در این مورد دقت کنید. من در اینجا همان حالت پیش فرض، یعنی ۱ را انتخاب می‌کنم. این گزینه نحوه‌ی امضاء و یا رمزگذاری شما با استفاده از الگوریتم‌های RSA و DSA را مشخص می‌کند.

```
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
```

در کل در هر حالتی، استفاده‌ی از RSA پیشنهاد می‌شود. بعد از آن، از شما اندازه‌ی کلید را می‌پرسد که همان مقدار پیش فرض خودش را وارد می‌کنیم:

```
What keysize do you want? (2048)
```

البته بسیاری ۱۰۲۴ بایت را نیز کافی می‌دانند.
بعد از آن مدت زمان اعتبار این کلید را از شما جویا می‌شود:

```
Key is valid for? (0)
```

هنگام این پرسش نحوه‌ی ورود زمان را به شما خواهد گفت که می‌تواند به شکل‌های زیر باشد:

```
دو هفته
2w
دو سال
2y
```

پس از آن هم یک تاییدیه از شما می‌گیرد و تاریخ انقضاء را به طور کامل برای شما می‌نویسد و سپس نیاز است که اطلاعاتی از قبیل نام و ایمیل و توضیح را وارد کنید:

```
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: ali yeganeh.m
Email address: yeganehaym@gmail.com
Comment: androidbreadcrumb
You selected this USER-ID:
    "ali yeganeh.m (androidbreadcrumb) <yeganehaym@gmail.com>"
```

بعد از آن از شما می‌خواهد که کل عملیات را تایید و یا کنسل کنید؛ یا اگر اطلاعات بالا را اشتباه وارد کرده‌اید، اصلاح کنید. با زدن کلید O عملیات را تایید کنید. در این حین از شما یک کلید برای رمزگذاری می‌پرسد که باید آن را دو بار بدهید و کارتان در اینجا به پایان می‌رسد و کلید ایجاد می‌شود.
اگر مشکلی در ساخت کلید نباشد با ارسال دستور زیر باید آن را در لیست کلیدها ببینید:

```
ali@alipc:~$ gpg --list-keys
/home/ali/.gnupg/pubring.gpg
----------------------------
pub   2048R/8708016A 2015-10-23 [expires: 2065-10-10]
uid                  ali yeganeh.m (androidbreadcrumb) <yeganehaym@gmail.com>
sub   2048R/533B7E96 2015-10-23 [expires: 2065-10-10]
```

در اینجا کلید عمومی در خط pub بعد از / قرار دارد؛ یعنی عبارت ۸۷۰۸۰۱۶A کلید عمومی ماست که بر روی هر سیستم و هر کلیدی متفاوت است.

تبدیل کد متنی به کد دودویی

یکی از روش‌های ارسال کدهای دودویی تبدیل آنان به یک قالب متنی ASCII است که به آن قالب ASCII Armor هم می‌گویند. سایت‌های زیادی وجود دارند که این عبارت متنی را از شما می‌خواهند. چرا که مثلا این امکان وجود دارد که کلیدی که کاربر به سمت آنان می‌فرستد، آسیب دیده باشد یا اینکه KeyServerها در دسترس نباشند. در مورد این سرورها در ادامه صحبت خواهیم کرد. مثلا یکی از سایت‌هایی که به این عبارت‌ها نیاز دارد Bintray است.

برای دریافت این کلید متنی باید دستور زیر را صادر کنید:

```
gpg --output mykey.asc --export -a $GPGKEY
```

که برای مثال ما می‌شود:

```
gpg --output mykey.asc --export -a 8708016A
```

و اگر کلید را با یک ویرایشگر متنی باز کنید، محتوایی شبیه محتوای زیر را خواهید دید:

```
ali@alipc:~$ cat mykey.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBFYqAJABCADcw5xPonh5Vj7nDk1CxDskq/VsO08XOa/i2OLOzatB4oK5x+0x
jxORxXMnIAR83PCK5/WkOBa64jnu3eiP3jKEwAykGGz/Z1bezC9TIP8y+PnsiDhT
aFArluUJx+RT5q7s27aKjqoc3fR/xuwLWopZt9uYzE/DQAPDsHdUoUg+fh4Hevm+
a8/3ncR7q6nM8gc9wk621Urb1HaRrILdmeh7ZpJcl8ZUbc+NObw357fGsjnpfHXO
rdCr7ClvNUq6I+IeGMQG/6040LeeaqhaRxPrUhbFjLA155gkSqzecxl7wQaYc71M
Zdlv+6Pt1B8nPAA3WXq0ypjU8A5bvmAQRD5LABEBAAG0OGFsaSB5ZWdhbmVoLm0g
KGFuZHJvaWRicmVhZGNydW1iKSA8eWVnYW5laGF5bUBnbWFpbC5jb20+iQE+BBMB
AgAoBQJWKgCQAhsDBQld/A8ABgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRDS
Lhq8hwgBanaHB/4reGxUjR6dB08ykfwQOx+raYHGqJlgawisE4qUHTkGaspyQaNy
yxh0vwKkGvg6nNy2VN1XFBc7jlHlrYqPPuPdg2B+1LvEghb30ESDbHUvk8NrJgDJ
C0257gxqWvUQTWvMC3FkSLdw3tyQ8dF7FxmSU79XcxVqGeseaDzMQrEasP0yJHsm
NJf8pvuD6qiWu3KSSoQmI/17Sj8s7eGJMh6o5YRFGHc1Bt9tCD+52bvt579Ju4vZ
tmQvxR4fNQo9sAeMqAJhIpF7IYcuyCEy+CQ847UkzE4f/OCCPxfV3samV/nnBJJ9
Ouu+68lk6Fpx4A0a3nEwqoAmMWxrbSSUFW97uQENBFYqAJABCAC4CzrUOKskE4hK
GVCjaOJKxhbuUdOrep6n3vof0fscs5Dy7h2oVh2vb12WH9X6pijJVPiUpGR4Mpu0
lO2Bu9Rwt38AQ6mRmL/hfzjEXSvKkdX7osk+1CVnnUaSdM9Ek2hWUH8JcN28z/WT
X9Bw8MCdZF7j1HvX/5ojghzMZyYM4elWJLBr1gON6xXAI6HR7DlnRkaVr8L9SYGm
FyAXZ0LzWYwG1Z1AnTyxff6v/Mn3p1/1E3aBA+LkQqBzHg2nBm4jCaFWfeCdiNBf
CHkY9r/Evo9hUPD+CtBNFwsUm1D4maZ0FFtIQ701QhVmupnub+rKoObC0AFj3abK
MCw9uo8TABEBAAGJASUEGAECAA8FAlYqAJACGwwFCV38DwAACgkQ0i4avIcIAWrz
rAf+K1IIMtBq3WlabfZQrgzFHQ62ugVJO/yI1ITkm4l08XHDf+ShqDg4urNuMDEe
oQD35MvB2BhER1jL6VR3qjLkZyZYJ+EQiSxEDWXooav3KvpWjhcqjQy79GFs8waH
E7ssGmWwaugVS/PJAmGQ+s8YWDNa6aCClmp2dJRiwBTyFdewNBLA2V32xzWCYxhI
YtEp+Kg15XuCDTRatOPWSFGSPe/paytmpGZc0XzU/W9sBpabhxVmcL4H6L07uCef
IOn/S5QXo3P9X/3ckmJ9GUb7rjdq1ivYgX53xI75jlePsmN/2f+3fNffUaZgFTTd
Uls+XCun7OVYSBBfjgRfQbTvoA==
=6j7i
-----END PGP PUBLIC KEY BLOCK-----
```

در صورتی که قصد دارید متن کلید خصوصی را به دست بیاورید، لازم است بعد از export- عبارت secret-key- را نیز اضافه کنی د؛ یعنی:

```
gpg --output mykey.asc --export-secret-key -a 8708016A
```

آپلود کلید به سرورهای کلید (Key Servers)

یکی از روش‌های به اشتراک گذاری کلید برای کاربران این است که از سرورهای کلید استفاده کنیم. یکبار آپلود روی یکی از این سرورها باعث می‌شود که به بقیه‌ی سرورها هم اضافه شود. یکی از این سرورهای کلید که خودم از آن استفاده می‌کنم، سرور ابونتو است و با استفاده از دستور زیر، همان کلید بالا را برای آن سرور ارسال می‌کنم:

```
gpg --send-keys --keyserver keyserver.ubuntu.com $GPGKEY

==>
gpg --send-keys --keyserver keyserver.ubuntu.com 8708016A
```

سپس از طریق کلید متنی، کلید آپلود شده را تایید می‌کنیم. به این آدرس رفته و محتوای کلید متنی خود را به طور کامل به همراه تگ‌های شروع و پایان کپی کنید و حتی می‌توانید کلید خود را از طریق کادر جست و جو پیدا کنید.

رمزگذاری

ابتدا در محیط یونیکس، یک فایل متنی ساده با متن hello ubuntu را ایجاد میکنم. در ادامه قصد دارم این فایل را رمزنگاری کنم:

```
ali@alipc:~$ cat >ali.txt
hello ubuntu
```

سپس همین فایل را رمزنگاری می‌کنم:

```
ali@alipc:~$ gpg --output myali.gpg --encrypt --recipient yeganehaym@gmail.com ali.txt
```

در این دستور ابتدا گفتیم که نام فایل خروجی ما myali.gpg است و می‌خواهیم آن را رمزگذاری کنیم که توسط کلیدی با ایمیل yeganehaym@gmail.com می‌باشد فایل ali.txt را رمزگذاری می‌کنیم.

رمزگشایی

برای رمزگشایی می‌توانید از طریق دستور زیر اقدام کنید:

```
gpg --output output.txt --decrypt myali.gpg

You need a passphrase to unlock the secret key for
user: "ali yeganeh.m (androidbreadcrumb) <yeganehaym@gmail.com>"
2048-bit RSA key, ID 533B7E96, created 2015-10-23 (main key ID 8708016A)
```

در اینجا دستور دادیم محتوای فایل رمزشده‌ی myali.gpg را رمزگشایی کن و محتوای آن را داخل فایلی با نام output.txt قرار بده. بعد از اجرای این دستور از شما عبارت رمزی را که در مرحله‌ی ساخت کلید دوبار از شما پرسید، درخواست می‌کند. در بعضی سیستم‌ها در همان ترمینال می‌پرسد، ولی بعضی سیستم‌ها مثل ابونتو که من از آن استفاده می‌کنم، به صورت گرافیکی یک کادر باز کرده و از شما خواهش می‌کند عبارت رمز را وارد کنید.

عبارت رمز را وارد کنید و حالا فایل output.txt را باز کنید:

```
ali@alipc:~$ cat output.txt
hello ubuntu
```