احراز هویت و امنیت محتوا

GnuPG

سر فصل ها

- مفاهیم اولیه
- GNU Privacy Guard چیست ؟
- نصب نرم افزار و ایجاد یک کلید جدید
- گواهینامه فسخ (revocation certificate) و انتشار کلید عمومی
- اضافه کردن کلید عمومی افراد و امضا کردن کلید ها
- روش امضای یک فایل و بررسی صحت امضا
- روش رمزگذاری و رمزگشایی یک فایل
- شبکه اعتماد (web of trust) و روش اعتماد به افراد
- سازگاری با سایر نرم افزار ها
- برنامه های گرافیگی

GnuPG

مفاهیم اولیه

- رمز نگاری (*cryptography*)
- امضای دیجیتال
- کلیدهای متقارن و نامتقارن
- کلید عمومی و خصوصی

GnuPG

مفاهیم اولیه

There are two kinds of cryptography in this world:
cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

—— Bruce Schneier

GnuPG

GNU Privacy Guard چیست ؟

- یک نرم افزار آزاد برای حفظ امنیت اطلاعات بر اساس کلیدهای نامتقارن
- سازگار با استاندارد Openpgp
- سازگار با pgp
- استفاده نکردن از الگوریتم های دارای Patent
- دارای مجوز GPL
- توانایی استفاده از سرورهای کلید عمومی
- پیاده سازی در سیستم عامل های مختلف

GnuPG

نصب نرم افزار و ایجاد یک کلید جدید

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

```
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)
Your selection?
```

```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
```

GnuPG

نصب نرم افزار و ایجاد یک کلید جدید

Please specify how long the key should be valid.

0 = key does not expire

<n> = key expires in n days

<n>w = key expires in n weeks

<n>m = key expires in n months

<n>y = key expires in n years

Key is valid for? (0)

Key does not expire at all

Is this correct? (y/N)

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>"

GnuPG

نصب نرم افزار و ایجاد یک کلید جدید

You need a Passphrase to protect your secret key.

Enter passphrase:

Repeat passphrase:

.....

.....

gpg: key 09BF7F0E marked as ultimately trusted

public and secret key created and signed.

pub 2048R/09BF7F0E 2010-10-22

Key fingerprint = F6C9 6EA0 D10F DCFA ECF5 F130 3913 CFE0 09BF 7F0E

uid yourname (your comment) <email@domain.com>

sub 2048R/3A78DCB6 2010-10-22

GnuPG

گواهینامه فسخ

```
gpg --output revoke.asc --gen-revoke 09BF7F0E
```

```
Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 3
```

GnuPG

گواهینامه فسخ

```
Enter an optional description; end it with an empty line:
> your optional description
>
Reason for revocation: Key is no longer used
your optional describtion
Is this okay? (y/N) y
You need a passphrase to unlock the secret key for
user: "username (comment) <user@email.com>"
2048-bit RSA key, ID 09BF7F0E, created 2010-10-22
Enter passphrase:
ASCII armored output forced.
Revocation certificate created.
```

GnuPG

گواهینامه فسخ

فایل نمونه :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.10 (GNU/Linux)
Comment: A revocation certificate should follow

iQE4BCABAgAiBQJMwwsvGx0DeW91ciBvcHRpb25hbCBkZXNjcmlidGlvbgAKCRA5
E8/gCb9/DnB0CACouyi6HkDJeonL74vcwbhEJe1PCH7fy938Qzen47y05QnwiNdV
zC8kl8e1uEF1Zp7VOhY9ErMwJHMy9xyAoMjvZ7J4pj/ombdZQUpZTFyuilfcJpst
m4V7xbs+kzuhr++9g2CNnAQX5wA4AYoivS3gMYzLpIuRLwhSq640doBWa+El9pbv
xec1zauf+hgVODAcrhVgBb7gsTsXksi3qb7SerDLlWYaE16E1JEKu9VzicCFgha/
mxGBY58P8mPqm47UurlNOF3Nq6EDV8/WftbzXzdKF2+d5HP/FebVw+h1GJEkENmR
HwQD1EykwGFkXtYGtnH7BigADgLmuef5XH9T
=P/1C
-----END PGP PUBLIC KEY BLOCK-----
```

GnuPG

انتشار کلید عمومی

```
$-- gpg --export --armor yourname
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.10 (GNU/Linux)
[...]
-----END PGP PUBLIC KEY BLOCK----
```

```
gpg --output publickey.asc --export --armor  name
```

```
$gpg --send-key --keyserver  keyserver.ubuntu.com 0115D0BC
```

GnuPG

اضافه کردن کلید عمومی افراد و امضا کردن کلید ها

```
$gpg –import  yourfriend.gpg
```

```
$gpg –import  revoke.asc
```

```
$gpg --recv-keys  --keyserver  keyserver.ubuntu.com 09BF7F0E
```

```
$ gpg --search-keys  --keyserver  keyserver.ubuntu.com name
```

```
$ gpg --sign-key name
```

GnuPG

روش امضای یک فایل

```
$gpg --sign document.ext
```

```
$gpg --sign --armor document.ext
```

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.10 (GNU/Linux)

owGbwMvMwCTIGSGWzCh6YQ/jGvEk1pDUihJDn8OPq4sTcwtyUhVSEksSuTrcWBgE
mRjYWJlAMgxcnAIwPQU3GObpX+5Ss7vT28Py+syKuZaZIiJlRWIMc3hTmzyKXO9N
eLOG4z7zq7VhfXbbVQA=
=RfQT
-----END PGP MESSAGE-----
```

GnuPG

روش امضای یک فایل (clearsign)

```
$ gpg --clearsign document.ext
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

your document body
can be in ascii or binary format
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.10 (GNU/Linux)

iEYEARECAAYFAkzD4KYACgkQCVgWYwEV0LxtNwCePr8oM070UtJAGeHZO2ynpw17
awcAni5wMwCxSecPAEyhqpA9pAFNlk4Y
=d0TA
-----END PGP SIGNATURE-----
```

GnuPG

روش امضا در یک فایل جداگانه

```
$gpg --detach-sign document.ext
```

```
$gpg --detach-sign --armor document.ext
```

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.10 (GNU/Linux)

iEYEABECAAYFAkzD5iEACgkQCVgWYwEV0Lwp0ACgo0q9kexjfewX0PJWIns2jC4A
zn0AoKI981t+xXZrb0xs/qgVsdWdWe7b
=T3N0
-----END PGP SIGNATURE-----
```

GnuPG

بررسی صحت امضا

امضای معمولی و Clear Sign

```
$gpg --verify document.gpg
```

امضا در فایل جداگانه (detached)

```
$gpg --verify sign.sig original.ext
```

استخراج فایل اصلی از فایل امضا شده

```
$gpg --output doc.ext --decrypt doc.gpg
```

GnuPG

رمزگذاری و رمز گشایی یک فایل

رمز گذاری ساده

```
$ gpg --recipient name1 --armor --encrypt doc.ext
```

رمز گذاری همراه با امضا

```
$gpg --armor --sign --encrypt --recipient name1 doc.ext
```

رمز گشایی

```
$gpg --output doc.ext --decrypt doc.gpg
```

GnuPG

شبکه اعتماد (web of trust) و روش اعتماد به افراد

تنظیم میزان اعتماد به افراد

```
$ gpg --edit-key richard
gpg (GnuPG) 1.4.10; Copyright (C) 2008 Free Software Foundation, Inc.
Command> trust
Please decide how far you trust this user to correctly verify other
   users' keys
(by looking at passports, checking fingerprints from different
   sources, etc.)
  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu
Your decision? 4
Command> quit
```

GnuPG

سایر نرم افزار ها

نرم افزار های ایمیل

Gmail™

Firefox + FireGPG

Kmail & Kontact

evolution

Thunderbird + Enigmail

Balsa

واسط های گرافیکی

Seahorse

KGPG

http://www.gnupg.org/related_software/frontends.en.html

GnuPG

موارد بیشتر

```
$gpg --ist-keys
$gpg --list-key
$gpg --list-sigs
$gpg --delete-key name
$gpg --fingerprint name
$gpg --update-trustdb
$gpg --refresh-keys --keyserver keyserver.ubuntu.com
$gpg --help
```

GnuPG

منابع اصلی

http://www.gnupg.org/gph/en/manual.html

http://fa.wikipedia.org/wiki/رمزنگاری

http://en.wikipedia.org/wiki/OpenPGP

http://en.wikipedia.org/wiki/GNU_Privacy_Guard

http://www.gnuiran.org

```
$man gpg | less
```