**1.initrepo.sh**

REPODIR=~/Public

REPONAME="cosrepo"

RELEASE="iceblue"

cd ${REPODIR}

if [ -e ${REPONAME} ] ; then

echo "dir ${REPONAME} already exist. exit"

exit

else

echo "make dir ${REPONAME}."

mkdir ${REPONAME}

fi

echo "make sub directory."

cd ${REPONAME}

mkdir -p dists/${RELEASE}/{main,restrict,universe,multiverse}/{binary-i386,binary-amd64}

mkdir -p pool/{main,restrict,universe,multiverse}

mkdir -p project

echo "create gpg."

#gpg -K

#gpg --gen-key

#gpg --export -a 81383BF8 > project/keyring.gpg

2.refreshrepo.sh

REPODIR=~/Public

REPONAME="cosrepo"

RELEASE="iceblue"

if [ ! -e ${REPODIR}/${REPONAME} ]; then

echo "directory ${REPODIR}/${REPONAME} not exist. exit"

exit

fi

cd ${REPODIR}/${REPONAME}

echo "make apt.conf"

echo "APT::FTPArchive::Release {" > dists/${RELEASE}/apt.conf

echo "Origin \"cos\";" >> dists/${RELEASE}/apt.conf

echo "Label \"cos\";" >> dists/${RELEASE}/apt.conf

echo "Suite \"iceblue\";" >> dists/${RELEASE}/apt.conf

echo "Codename \"iceblue\";" >> dists/${RELEASE}/apt.conf

echo "Versin \"0.5\";" >> dists/${RELEASE}/apt.conf

echo "Architecture \"i386\";" >> dists/${RELEASE}/apt.conf

echo "Components \"main\";" >> dists/${RELEASE}/apt.conf

echo "Description \"cos iceblue\";" >> dists/${RELEASE}/apt.conf

echo "};" >> dists/${RELEASE}/apt.conf

echo "make index file : Package, Package.gz, Package.bz2 ."

apt-ftparchive packages pool/main > dists/${RELEASE}/main/binary-i386/Packages

cat dists/${RELEASE}/main/binary-i386/Packages | gzip > dists/${RELEASE}/main/binary-i386/Packages.gz

cat dists/${RELEASE}/main/binary-i386/Packages | bzip2 > dists/${RELEASE}/main/binary-i386/Packages.bz2

echo "make content file : Contents-i386.gz"

apt-ftparchive contents pool/ | gzip -9c > dists/${RELEASE}/Contents-i386.gz

echo "make release file : Release, Release.gpg"

apt-ftparchive -c dists/${RELEASE}/apt.conf release dists/${RELEASE} > dists/${RELEASE}/Release

gpg -a --detach-sign -o dists/${RELEASE}/Release.gpg dists/${RELEASE}/Release

**关于gpg**

GPG :（全称 GnuPG ) 是一款非对称加密(PGP)的免费软件，非对称加密方式简单讲就是指用公钥加密文件，用私钥解密文件。如果你想给谁发送加密信息，首先你要得到他的公钥，然后通过该公钥加密后传给他，对方利用自已的私钥就可解密并读取文件了。

GPG 配置文件目录:~/.gnupg

~/.gnupg/gpg.conf – 配置文件

~/.gnupg/trustdb.gpg – 信任库

~/.gnupg/pubring.gpg – 公钥库

~/.gnupg/secring.gpg – 私钥库

# 基本操作

**1、生成密钥对**

**gpg --gen-key**

生成过程中会让你选择加密方式，一般选 (1) RSA and RSA (default) 就可以了，然后还需要选择加密位数、过期日期及输入姓名，邮件地址，备注，Passphrase(访问密码）等信息。最后你就可以干点别的事，比如上上网，玩玩游戏什么的，以便让机器生成一些随机数，回头你就可以看到密钥对已经生成完毕。

**2、传播公钥：**

导出公钥:生成后你可以把公钥中公钥库中导出来，以便传播给你的朋友。

**gpg --export --armor mypubkeyID > keyring.pub.gpg**

# mypubkeyID部分可以用 name 或 mail 地址代替

注： - -armor 表示加内容转换成可见的 ASCII 码输出,否则是二进制不可见内容。

现在你可以把导出的公钥通过 Email 等途径发送给你的朋友了，或者你也可以不导出公钥直接上传公钥到密钥服务器。

gpg --keyserver keyserverAddress --send mykeyID

注： --keyserver 可以不加，默认为 keys.gnupg.net

然后只要把公钥 ID 和服务器地址告诉给朋友就可以了，朋友可以通过搜索你的公钥 ID，Email 地址或名字来获取并导入你的公钥，如下：

gpg --keyserver keyserverAddress --search-keys keyid/name/Email

比如搜索我的：

gpg --keyserver keyserver.ubuntu.com --search-keys rikulu

**3、导入朋友的公钥**

当你获得朋友的公钥文件后，你首先需要导入公钥到公钥库

**gpg --import gpgkey.pub.asc**

或直接从公钥服务器导入

gpg --keyserver keyserverAddress --recv-keys pubkeyID

# 私钥备份与密钥回收

1. 密钥的导出和导入

以便用来备份密钥或导入到其它机器上。

导出

**gpg --export-secret-keys --armor mysecurekeyID > keyring.sec.gpg**

gpg -oa seckey.asc --export-secret-keys mykeyID

导入

gpg --import seckey.asc

2 密钥回收:当您的密钥对生成之后，您应该立即做一个公钥回收证书，如果您忘记了您的私钥的口令或者您的私钥丢失或者被盗窃，您可以发布这个证书来声明以前的公钥不再有效。

生成回收证书

gpg --output revoke.asc --gen-revoke mykeyID

导入回收证书

gpg --import revoke.asc

发送回收证书到服务器，声明原 GPG Key 作废

gpg --keyserver keyserverAddress --send mykeyID

# 列出机器中保存的所有密钥

列出所有公钥

gpg -k

列出所有私钥

gpg -K

gpg --list-keys，查看现有的key。

删除key需要先删除密钥

gpg --delete-secret-keys 6A3682B9

gpg --delete-keys xifei

备份密钥分为备份公钥和私钥两个部分，备份公钥：

gpg -o keyfilename --export KeyID

如果没有KeyID则是备份所有的公钥，-o表示输出到文件keyfilename中，如果加上-a的参数则输出文本格式的信息，否则输出的是二进制格式信息。

备份私钥：

gpg -o keyfilename --export-secret-keys KeyID

如果没有KeyID则是备份所有的私钥，-o表示输出到文件keyfilename中，如果加上-a的参数则输出文本格式的信息，否则输出的是二进制格式信息。

然后在别的机器上可以通过

gpg --import filename

导入这些信息。

**关于客户端**

#!/bin/sh

set -e

if [ "$USER" != "root" ] ; then

echo "error: you are not run as root user, you should excute sudo."

exit

fi

#添加密钥文件

wget -q -O - http://124.16.141.172/cos/project/keyring.gpg | apt-key add -

#添加源

echo "deb http://124.16.141.172/cos iceblue main" > /etc/apt/sources.list.d/cos-repository.list

#为新加源赋予优先级

sed -i '1i\Package: \*\

Pin: release o=cos\

Pin-Priority: 700\

' /etc/apt/preferences

关于：pgp - Not enough random bytes available.

sudo apt-get install rng-tools

如果没有足够信息：

ls -l /dev/urandom

rngd -r /dev/urandom