

# Şifrelenmiş Kök Dosya Sistemi NASIL

Yazan:  
**Christophe Devine**

Çeviren:  
**Necdet Yücel**

Temmuz 2005

## Özet

Bu belgede güçlü bir şifreleme tekniği kullanarak Linux kök dosya sisteminizin şifrelenmesiyle kişisel bilgilerinizin nasıl güvenli hale getirileceğini anlatmaktadır.

## Konu Başlıkları

<b>1. Sistemin Hazırlanması</b>	3
1.1. Bölümleme düzeninin hazırlanması	3
1.2. Gerekli paketler	3
1.3. Linux-2.4.29 çekirdeğinin kurulması	3
1.4. Linux-2.6.10 çekirdeğinin kurulması	5
1.5. Util-linux-2.12p paketinin kurulması	5
<b>2. Şifrelenmiş Kök Dosya Sisteminin Oluşturulması</b>	5
<b>3. Önyükleme Aygıtının Ayarlanması</b>	6
3.1. Ramdisk'in oluşturulması	6
3.2. CD-ROM'dan önyükleme yapılması	8
3.3. Sabit disk bölümünden önyükleme yapılması	8
<b>4. Son Adımlar</b>	9
<b>5. Belge Hakkında</b>	10
GNU Free Documentation License	10

### Bu çevirinin sürüm bilgileri:

1.0	Temmuz 2005	NY
İlk çeviri		

### Özgün belgenin sürüm bilgileri:

v1.3	2005-03-13	cd
Paket sürümleri güncellendi.		
v1.2	2004-10-20	cd
Paket sürümleri güncellendi.		
v1.1	2003-12-01	cd
GRUB desteği eklendi.		
v1.0	2003-09-24	cd
LDP tarafından gözden geçirilen ilk sürüm.		
v0.9	2003-09-11	cd
Güncellendi ve DocBook XML biçimine dönüştürüldü.		

Telif Hakkı © 2003, 2004, 2005 Christophe Devine – Özgün belge

Telif Hakkı © 2005 Necdet Yücel – Türkçe çeviri

### Yasal Açıklamalar

Bu belgenin çevirisinin, *Şifrelenmiş Kök Dosya Sistemi NASIL* 1.0 sürümünün **telif hakkı © 2005 Necdet Yücel**e aittir. Bu belgeyi, Free Software Foundation tarafından yayınlanmış bulunan GNU Özgür Belgeleme Lisansının 1.1 ya da daha sonraki sürümünün koşullarına bağlı olarak kopyalayabilir, dağıtabilir ve/veya değiştirebilirsiniz. Bu Lisansın bir kopyasını [GNU Free Documentation License](#) (sayfa: 10) başlıklı bölümde bulabilirsiniz.

BU BELGE "ÜCRETSİZ" OLARAK RUHSATLANDIĞI İÇİN, İÇERDİĞİ BİLGİLER İÇİN İLGİLİ KANUNLARIN İZİN VERDİĞİ ÖLÇÜDE HERHANGİ BİR GARANTİ VERİLMEMEKTEDİR. AKSİ YAZILI OLARAK BELİRTİLMEDİĞİ MÜDDETÇE TELİF HAKKI SAHİPLERİ VE/VEYA BAŞKA ŞAHISLAR BELGEYİ "OLDUĞU GİBİ", AŞIKAR VEYA ZIMNEN, SATILABİLİRLİĞİ VEYA HERHANGİ BİR AMACA UYGUNLUĞU DA DAHİL OLMAK ÜZERE HİÇBİR GARANTİ VERMEKSİZİN DAĞITMAKTADIRLAR. BİLGİNİN KALİTESİ İLE İLGİLİ TÜM SORUNLAR SİZE AİTTİR. HERHANGİ BİR HATALI BİLGİDEN DOLAYI DOĞABİLECEK OLAN BÜTÜN SERVİS, TAMİR VEYA DÜZELTME MASRAFLARI SİZE AİTTİR.

İLGİLİ KANUNUN İCBAR ETTİĞİ DURUMLAR VEYA YAZILI ANLAŞMA HARİCİNDE HERHANGİ BİR ŞEKİLDE TELİF HAKKI SAHİBİ VEYA YUKARIDA İZİN VERİLDİĞİ ŞEKİLDE BELGEYİ DEĞİŞTİREN VEYA YENİDEN DAĞITAN HERHANGİ BİR KİŞİ, BİLGİNİN KULLANIMI VEYA KULLANILAMAMASI (VEYA VERİ KAYBI OLUŞMASI, VERİNİN YANLIŞ HALE GELMESİ, SİZİN VEYA ÜÇÜNCÜ ŞAHISLARIN ZARARA UĞRAMASI VEYA BİLGİLERİN BAŞKA BİLGİLERLE UYUMSUZ OLMASI) YÜZÜNDEN OLUŞAN GENEL, ÖZEL, DOĞRUDAN YA DA DOLAYLI HERHANGİ BİR ZARARDAN, BÖYLE BİR TAZMİNAT TALEBİ TELİF HAKKI SAHİBİ VEYA İLGİLİ KİŞİYE BİLDİRİLMİŞ OLSA DAHİ, SORUMLU DEĞİLDİR.

Tüm telif hakları aksi özellikle belirtilmediği sürece sahibine aittir. Belge içinde geçen herhangi bir terim, bir ticari isim ya da kuruma itibar kazandırma olarak algılanmamalıdır. Bir ürün ya da markanın kullanılmış olması ona onay verildiği anlamında görülmemelidir.

## 1. Sistemin Hazırlanması

### 1.1. Bölümleme düzeninin hazırlanması

Sabit diskiniz (hda) en azından aşağıdaki üç bölümden oluşmalıdır:

- **hda1**: Bu küçük şifrelenmemiş disk bölümü şifrelenmiş kök dosya sistemini bağlayabilmeniz için gerekli parolayı soracaktır.
- **hda2**: Bu bölüm şifrelenmiş kök dosya sisteminiz olacak, yeterince büyük olduğundan emin olun.
- **hda3**: Bu bölüm çalışan GNU/Linux sisteminizdir.

Bu aşamada **hda1** ve **hda2** kullanılmamaktadır. **hda3** ise kurulu Linux dağıtımınızın bulunduğu dizindir. **/usr** ve **/boot** farklı disk bölümleri *olmamalıdır*.

Bölümleme düzeniniz aşağıdaki örneğe benzemelidir:

```
# fdisk -l /dev/hda

Disk /dev/hda: 255 heads, 63 sectors, 2432 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1            1           1         8001    83   Linux
/dev/hda2            2          263       2104515   83   Linux
/dev/hda3          264          525       2104515   83   Linux
/dev/hda4          526         2047      12225465   83   Linux
```

### 1.2. Gerekli paketler

Eğer Debian kullanıyorsanız, aşağıdaki paketleri kurmak zorundasınız:

```
# apt-get install gcc make libncurses5-dev patch bzip2 wget
```

Kopyala/yapıştır işlemlerini kolaylaştırmak için şu paketleri de kursanız iyi olur:

```
# apt-get install lynx gpm
```

### 1.3. Linux-2.4.29 çekirdeğinin kurulması

Çekirdekte geridönüş şifreleme desteği veren iki temel proje bulunmaktadır: **cryptoloop** ve **loop-AES**. Bu belgede **loop-AES** temel alınmıştır. Bunu nedeni oldukça hızlı olması, Rijndael'in çevirici dilinde en iyi şekilde kullanılmış hali olması ve IA-32 (x86) işlemcilerde en iyi performansı vermesidir. Bunun yanında **cryptoloop** ile ilgili [güvenlik sorunları](#)<sup>(B3)</sup> da vardır.

Öncelikle, **loop-AES** paketini indirin ve açın::

```
$ cd /usr/src
$ wget http://loop-aes.sourceforge.net/loop-AES/loop-AES-v3.0b.tar.bz2
$ tar -xvjf loop-AES-v3.0b.tar.bz2
```

Ardından çekirdeğin kaynak kodunu indirip yamayı uygulayın:

```
$ wget http://ftp.kernel.org/pub/linux/kernel/v2.4/linux-2.4.29.tar.bz2
$ tar -xvjf linux-2.4.29.tar.bz2
$ cd linux-2.4.29
$ rm include/linux/loop.h drivers/block/loop.c
```

```
$ patch -Np1 -i ../loop-AES-v3.0b/kernel-2.4.28.diff
```

Klavye düzeninizi ayarlayın:

```
$ dumpkeys | loadkeys -m - > drivers/char/defkeymap.c
```

Çekirdeğinizi aşağıdaki seçenekleri de dahil ederek yapılandırın:

```
$ make menuconfig

Block devices --->

  <*> Loopback device support
  [*]   AES encrypted loop device support (NEW)

  <*> RAM disk support
  (4096) Default RAM disk size (NEW)
  [*]   Initial RAM disk (initrd) support

File systems --->

  <*> Ext3 journalling file system support
  <*> Second extended fs support

(ÖNEMLİ: /dev dosya sistemi desteğini etkinleştirmeyin.)
```

Çekirdeği derleyin ve kurun:

```
$ make dep bzImage
$ make modules
# make modules_install
# cp arch/i386/boot/bzImage /boot/vmlinuz
```

Eğer önyükleyici olarak **grub** kullanıyorsanız, /boot/grub/menu.lst veya /boot/grub/grub.conf dosyasını güncelleyin:

```
# cat > /boot/grub/menu.lst << EOF
default 0
timeout 10
color green/black light-green/black
title Linux
    root (hd0,2)
    kernel /boot/vmlinuz ro root=/dev/hda3
EOF
```

Lilo kullanıyorsanız /etc/lilo.conf dosyasını güncelleyin ve **lilo** komutunu çalıştırın:

```
# cat > /etc/lilo.conf << EOF
lba32
boot=/dev/hda
prompt
timeout=60
image=/boot/vmlinuz
    label=Linux
    read-only
    root=/dev/hda3
EOF
# lilo
```

Artık sisteminizi yeniden başlatabilirsiniz.

## 1.4. Linux-2.6.10 çekirdeğinin kurulması

Yukarıdaki işlemleri `loop-aes`'in `kernel-2.6.10.diff` yamasını kullanarak yerine getirin ve `cryptoloop` desteğinin etkin olmadığından emin olun. Modül desteğinin `module-init-tools` paketine ihtiyaç duyduğunu unutmayın.

## 1.5. Util-linux-2.12p paketinin kurulması

util-linux paketinin bir parçası olan **losetup** programının güçlü kriptografi desteğine sahip olması için yamanması ve yeniden derlenmesi gerekir. util-linux paketini indirip, açın ve yamayın:

```
$ cd /usr/src
$ wget http://ftp.kernel.org/pub/linux/utils/util-linux/util-linux-2.12p.tar.bz2
$ tar -xvzf util-linux-2.12p.tar.bz2
$ cd util-linux-2.12p
$ patch -Np1 -i ../loop-AES-v3.0b/util-linux-2.12p.diff
```

20 karakterden daha kısa parolalar kullanabilmek için aşağıdaki komutu girin:

```
CFLAGS="-O2 -DLOOP_PASSWORD_MIN_LENGTH=8"; export CFLAGS
```

Temel kaygınız güvenlik olduğundan lütfen 20 karakterden daha kısa parolaları girebilmeyi etkin yapmayın. Bilgi gizliliği bedava değildir, uzun parolalar bunun 'bedeli'dir.

**losetup**'ı derleyin ve root olarak kurun:

```
$ ./configure && make lib mount
# mv -f /sbin/losetup /sbin/losetup~
# rm -f /usr/share/man/man8/losetup.8*
# cd mount
# gzip losetup.8
# cp losetup /sbin
# cp losetup.8.gz /usr/share/man/man8/
# chattr +i /sbin/losetup
```

## 2. Şifrelenmiş Kök Dosya Sisteminin Oluşturulması

Hedef disk bölümünü rastgele veri ile doldurun:

```
# shred -n 1 -v /dev/hda2
```

Şifrelenmiş geridönüş aygıtını ayarlayın:

```
# losetup -e aes256 -S xxxxxx /dev/loop0 /dev/hda2
```

Sözlük ataklarından korunmak için `-S xxxxxx` seçeneğini eklemeniz tavsiye edilir. Burada "xxxxxx" rastgele seçilmiş anahtar olmalıdır (örneğin "gPk4lA" olabilir). Bu anahtarı unutmamak için bir kağıda yazmanız iyi olur. Ayrıca önyükleme sırasında klavye sorunları yaşamamak için parolanızda ASCII olmayan karakterleri kullanmayın. [Diceware<sup>\(B4\)</sup>](http://diceware.sourceforge.net/) sitesinde hatırlaması kolay ama güçlü parolalar hazırlanmasına yardımcı olunmaktadır

Şimdi ext3 dosya sistemini oluşturalım:

```
# mke2fs -j /dev/loop0
```

Girdiğiniz parolanın doğruluğunu sınavın:

```
# losetup -d /dev/loop0
# losetup -e aes256 -S xxxxxx /dev/loop0 /dev/hda2
```

```
# mkdir /mnt/efs
# mount /dev/loop0 /mnt/efs
```

Şifrelenmiş ve çözülmüş verileri karşılaştırabilirsiniz:

```
# xxd /dev/hda2 | less
# xxd /dev/loop0 | less
```

Artık şifrelenmiş Linux sisteminizi kurmanın zamanı geldi. Eğer bir GNU/Linux dağıtımı (Debian, Slackware, Gentoo, Mandrake, RedHat/Fedora, SuSE, gibi) kullanıyorsanız, aşağıdaki komutu çalıştırın:

```
# cp -avx / /mnt/efs
```

Eğer Linux From Scratch kitabını takip ediyorsanız, aşağıdaki düzeltmelerle birlikte kitabı takibe devam edin:

- Bölüm 6 – Util-linux paketinin kurulması:  
Kodları açtıktan sonra loop-AES yamasını uygulayın.
- Bölüm 8 – LFS sisteminin önyüklenabilir hale getirilmesi:  
Bir sonraki bölüme (Önyükleme Aygıtının Ayarlanması) bakın.

## 3. Önyükleme Aygıtının Ayarlanması

### 3.1. Ramdisk'in oluşturulması

Başlamak için, şifrelenmiş disk bölümüne hapsolmalı (**chroot**) ve önyükleme aygıtı için bağlama noktasını oluşturmalısınız:

```
# chroot /mnt/efs
# mkdir /loader
```

Ardından, daha sonra ihtiyacınız olacak başlangıç ramdisk'ini (**initrd**) oluşturun:

```
# cd
# dd if=/dev/zero of=initrd bs=1k count=4096
# mke2fs -F initrd
# mkdir ramdisk
# mount -o loop initrd ramdisk
```

**grsecurity** kullanıyorsanız "Permission denied" hatasını alabilirsiniz. Bu durumda **mount** komutunu kafesin (**chroot**) dışında çalıştırmanız gerekir.

Dosya sistemi ağacını oluşturun ve gerekli dosyaları içine kopyalayın:

```
# mkdir ramdisk/{bin,dev,lib,mnt,sbin}
# cp /bin/{bash,mount} ramdisk/bin/
# ln -s bash ramdisk/bin/sh
# mknod -m 600 ramdisk/dev/console c 5 1
# mknod -m 600 ramdisk/dev/hda2 b 3 2
# mknod -m 600 ramdisk/dev/loop0 b 7 0
# cp /lib/{ld-linux.so.2,libc.so.6,libdl.so.2} ramdisk/lib/
# cp /lib/{libncurses.so.5,libtermcap.so.2} ramdisk/lib/
```

```
# cp /sbin/{losetup,pivot_root} ramdisk/sbin/
```

Eğer "/lib/libncurses.so.5: No such file or directory" veya "/lib/libtermcap.so.2: No such file or directory" hata iletileri ile karşılaşsanız dert etmeyin; **bash** bu kütüphanelerden sadece birine ihtiyaç duyar. Gerçekte hangisinin gerekli olduğunu şöyle kontrol edebilirsiniz:

```
# ldd /bin/bash
```

Parolanızın çekirdek iletileri (usb aygıtlarının kaydedilmesi gibi) tarafından taşırılmasını önlemek için aşağıdaki **sleep** programını derleyin.

```
# cat > sleep.c << "EOF"
#include <unistd.h>
#include <stdlib.h>

int main( int argc, char *argv[] )
{
    if( argc == 2 )
        sleep( atoi( argv[1] ) );

    return( 0 );
}
EOF

# gcc -s sleep.c -o ramdisk/bin/sleep
# rm sleep.c
```

**init** betiğini oluşturun:

```
# cat > ramdisk/sbin/init << "EOF"
#!/bin/sh

/bin/sleep 3

echo -n "Enter seed value: "
read SEED

/sbin/losetup -e aes256 -S $SEED /dev/loop0 /dev/hda2
/bin/mount -r -n -t ext3 /dev/loop0 /mnt

while [ $? -ne 0 ]
do
    /sbin/losetup -d /dev/loop0
    /sbin/losetup -e aes256 -S $SEED /dev/loop0 /dev/hda2
    /bin/mount -r -n -t ext3 /dev/loop0 /mnt
done

cd /mnt
/sbin/pivot_root . loader
exec /usr/sbin/chroot . /sbin/init
EOF

# chmod 755 ramdisk/sbin/init
```

Geridönüş aygıtını dosya sesteminden ayırın ve **initrd**'yi sıkıştırın:

```
# umount -d ramdisk
# rmdir ramdisk
```

```
# gzip initrd
# mv initrd.gz /boot/
```

### 3.2. CD-ROM'dan önyükleme yapılması

Sisteminizi CD-ROM gibi salt okunur bir ortamı kullanarak yüklemenizi öneririm.

`syslinux` paketini indirin ve açın:

```
$ wget http://ftp.kernel.org/pub/linux/utils/boot/syslinux/syslinux-3.07.tar.bz2
$ tar -xvjf syslinux-3.07.tar.bz2
```

`isolinux`'u yapılandırın:

```
# mkdir bootcd
# cp /boot/{vmlinuz,initrd.gz} syslinux-3.07/isolinux.bin bootcd
# echo "DEFAULT /vmlinuz initrd=initrd.gz ro root=/dev/ram0" > bootcd/isolinux.cfg
```

Yüklenabilir cd-rom eşlemini oluşturun ve yakın:

```
# mkisofs -o bootcd.iso -b isolinux.bin -c boot.cat \
          -no-emul-boot -boot-load-size 4 -boot-info-table \
          -J -hide-rr-moved -R bootcd

# crecord -dev 0,0,0 -speed 4 -v bootcd.iso

# rm -rf bootcd{,.iso}
```

### 3.3. Sabit disk bölümünden önyükleme yapılması

Eğer yükleme cd'nizi kaybederseniz sabit disk bölümünüz yükleme yapabilmeniz için elinizin altındadır. *Hda1 yazılabilir bir ortam olduğundan güvenilir olmadığını unutmayın ve ancak acil durumlarda kullanın!*

Ext2 dosya sistemini oluşturun ve bağlayın:

```
# dd if=/dev/zero of=/dev/hda1 bs=8192
# mke2fs /dev/hda1
# mount /dev/hda1 /loader
```

Çekirdeği ve başlangıç ramdisk'ini kopyalayın:

```
# cp /boot/{vmlinuz,initrd.gz} /loader
```

`grub` kullanıyorsanız:

```
# mkdir /loader/boot
# cp -av /boot/grub /loader/boot/
# cat > /loader/boot/grub/menu.lst << EOF
default 0
timeout 10
color green/black light-green/black
title Linux
    root (hd0,0)
    kernel /vmlinuz ro root=/dev/ram0
    initrd /initrd.gz
EOF
# grub-install --root-directory=/loader /dev/hda
# umount /loader
```



**lilo** kullanıyorsanız:

```
# mkdir /loader/{boot,dev,etc}
# cp /boot/boot.b /loader/boot/
# mknod -m 600 /loader/dev/hda b 3 0
# mknod -m 600 /loader/dev/hda1 b 3 1
# mknod -m 600 /loader/dev/hda2 b 3 2
# mknod -m 600 /loader/dev/hda3 b 3 3
# mknod -m 600 /loader/dev/hda4 b 3 4
# mknod -m 600 /loader/dev/ram0 b 1 0
# cat > /loader/etc/lilo.conf << EOF
lba32
boot=/dev/hda
prompt
timeout=60
image=/vmlinuz
    label=Linux
    initrd=/initrd.gz
    read-only
    root=/dev/ram0
EOF
# lilo -r /loader
# umount /loader
```

## 4. Son Adımlar

Kafesin içinde iken, `/etc/fstab` dosyasını aşağıdaki satırı içerecek şekilde düzenleyin:

<code>/dev/loop0</code>	<code>/</code>	<code>ext3</code>	<code>defaults</code>	<code>0</code>	<code>1</code>
-------------------------	----------------	-------------------	-----------------------	----------------	----------------

`/etc/mtab` dosyasını silip kafesten çıkın. Son olarak, **umount -d /mnt/efs** komutunu çalıştırın ve sisteminizi yeniden başlatın. Eğer ters giden bir şey olursa hala **LILO:** komut satırında **Linux root=/dev/hda3** yazarak sisteminizi başlatabilirsiniz.

Herşey yolunda gitmişse diskinizi yeniden bölümlendirerek `hda4`'ün yanı sıra `hda3`'ü de şifreleyebilirsiniz. Aşağıdaki betiklerde `hda3`'ü takas alanı ve `hda4`'ü `/home` dizini olduğunu kabul ediyoruz. Önce bu iki disk bölümü ilklendirilmelidir:

```
# shred -n 1 -v /dev/hda3
# shred -n 1 -v /dev/hda4
# losetup -e aes256 -S xxxxxx /dev/loop1 /dev/hda3
# losetup -e aes256 -S xxxxxx /dev/loop2 /dev/hda4
# mkswap /dev/loop1
# mke2fs -j /dev/loop2
```

Bir başlatma betiği yazın ve `fstab` dosyasını güncelleyin:

```
# cat > /etc/init.d/loop << "EOF"
#!/bin/sh

if [ "`/usr/bin/md5sum /dev/hda1`" != \
    "5671cebdb3bed87c3b3c345f0101d016 /dev/hda1" ]
then
    echo -n "WARNING! hda1 integrity verification FAILED - press enter."
    read
fi
```

```

echo "1st password chosen above" | \
    /sbin/losetup -p 0 -e aes256 -S xxxxxx /dev/loop1 /dev/hda3

echo "2nd password chosen above" | \
    /sbin/losetup -p 0 -e aes256 -S xxxxxx /dev/loop2 /dev/hda4

/sbin/swapon /dev/loop1

for i in `seq 0 63`
do
    echo -n -e "\33[10;10]\33[11;10]" > /dev/tty$i
done

EOF

# chmod 700 /etc/init.d/loop
# ln -s ../init.d/loop /etc/rcS.d/S00loop
# vi /etc/fstab
...
/dev/loop2          /home                ext3                defaults            0                  2

```

## 5. Belge Hakkında

Şifrelenmiş Kök Dosya Sistemi NASIL ilk olarak Kasım 2002'de [Linux From Scratch<sup>\(B5\)</sup>](#) projesi için yazıldı. O tarihten itibaren bu belgeye katkıda bulunan birçok kişiye teşekkür etmek isterim (ters tarih sırasına göre): Micha Bormann, Dennis Lemckert, Oleg Vyushin, Ellen Bokhorst, Daczi László, Gaetano Zappulla, Guillaume Lehmann, Claude Thomassin, Jean-Philippe Guérard, Luc Vo Van, Jacobus Brink, Ernesto Pérez Estévez, Matthew Ploessel, Mike Lorek, Lars Bungum, Michael Shields, Julien Perrot, Grant Stephenson, Cary W. Gilmer, James Howells, Pedro Baez, Josh Purinton, Jari Ruusu and Zibeli Aton.

Bu NASIL belgesi farklı dillere tercüme edildi:

- [Fransızca<sup>\(B6\)</sup>](#)
- [İtalyanca<sup>\(B7\)</sup>](#)
- [Macarca<sup>\(B8\)</sup>](#)
- [Danca<sup>\(B9\)</sup>](#)
- [Türkçe<sup>\(B10\)</sup>](#)

Lütfen yorumlarınızı [Christophe Devine<sup>\(B11\)</sup>](#)'a gönderin.

## GNU Free Documentation License

Version 1.2, November 2002

Copyright © 2000,2001,2002 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### 1. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without

modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## 2. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ascii without markup, Texinfo input format, LaTeX input format, [SGML](#) or [XML](#) using a publicly available [DTD](#), and standard-conforming simple

HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

### 3. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

### 4. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible

at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

## 5. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

## 6. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

## 7. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

## 8. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

## 9. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

## 10. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

## 11. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

## ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C) year your name.  
Permission is granted to copy, distribute and/or modify this document
```



under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being *list their titles*, with the Front-Cover Texts being *list*, and with the Back-Cover Texts being *list*.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

## Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(B3) <http://groups.google.com/groups?selm=1emrG-1Ck-25%40gated-at.bofh.it>

(B4) <http://www.diceware.com/>

(B5) <http://www.linuxfromscratch.org/lfs/news.html>

(B6) <http://www.traduc.org/docs/HOWTO/lecture/Encrypted-Root-Filesystem-HOWTO.html>

(B7) <http://www.linux.it/~gaetano/erfs/>

(B8) <http://tldp.fsf.hu/HOWTO/Encrypted-Root-Filesystem-HOWTO-hu/>

(B9) <http://doc.nl.linux.org/HOWTO/Encrypted-Root-Filesystem-HOWTO-NL/article.html>

(B10) <http://docs.comu.edu.tr/homemade/Encrypted-Root-Filesystem-HOWTO/>

(B11) <http://www.cr0.net:8040/about/>

Bu dosya (encrypted-rootfs-howto.pdf), belgenin XML biçiminin  $\text{\TeX}$ Live ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

23 Ocak 2007