Linux'ta GPG Kullanımı

Yazan:
Faruk Eskicioğlu
<farukesk (at) comu.edu.tr>

Yazan:
A. Murat Eren
<meren (at) comu.edu.tr>

Nisan 2004

Özet

Bu belgede kısaca Linux'ta komut satırından GPG kullanımı hakkında bilgi verilmektedir. GPG'nin kullandığı kriptografi algoritmalarından bahsedilmeyecektir. Neden GPG kullanmanız gerektiği, anahtarlara neden ihtiyaç duyduğunuz gibi bilgileri zaten biliyor olduğunuz kabul edilmiştir.

Bu belgenin son sürümüne `http://cekirdek.uludag.org.tr/~meren/belgeler/gpg/gpg.html` adresinden ulaşabilirsiniz.

Konu Başlıkları

Geçmiş

0.1	Ağustos 2001	FE ve AME
İlk sürüm.		

1. Giriş

İzleyen bölümlerde PGP sisteminin kullamına yönelik bir kaç komut sunulacak. Bunun için PGP'nin açık kodlu eşdeğeri olan GnuPG (GNU Privacy Guard) kullanılacaktır. Bu yazılımın Linux versiyonu http://www.gnupg.org/download.html adresinden temin edilebilir.

GnuPG, kullanıcılarının güvenli olarak haberleşebilmeleri için genel anahtar kriptografisini kullanmaktadır. Bir genel anahtarlı sistemde, bir kullanıcı, bir ***gizli anahtar*** ve bir ***genel anahtar***'dan oluşan bir anahtar çiftine sahiptir. Kullanıcının gizli anahtarı adından da anlaşılacağı üzere gizli tutulur; asla meydana çıkarılmaz. Genel anahtarı ise, kendisiyle güvenli haberleşmek isteyen herkese verilebilir. GnuPG biraz daha olgun bir şema sunar; kullanıcılar asıl anahtar çiftlerinin dışında isterlerse, ek olarak yardımcı anahtar çiftleri de kullanabilir. Asıl ve yardımcı anahtar çiftleri,anahtar yönetimini kolaylaştırmak için bir bohça olarak birarada sarmalanmıştır, yani basitçe bohça tek bir anahtar çiftidir.

GPG'nin komut satırından kullanımındaki genel sözdizimi şöyledir:

```
gpg [ seçenekler ] [ komut [ seçenekler ] ...]
```

2. Anahtar Kullanımı

2.1. Yeni Bir Anahtar Çiftinin Üretilmesi

Uyarı

Anahtar üretimi belleğin kilitlenmesini gerektirdiğinden (bellek kilitlemesi, işlem sırasına takas alanının kullanılmasını engeller) üretim işleminin `root` kullanıcısı tarafından yapılması gerekir. Böyle yapmazsanız GNUPG anahtar üretiminin güvenli olmayacağı konusunda sizi uyarır. Anahtar üretiminden sonra anahtarları normal kullanıcının ev dizinine kopyalayıp, dosyaların sahipliğini değiştirdikten sonra normal kullanıcı kimliğinizle kullanabilirsiniz.

Bir yeni asıl anahtar çiftini oluşturmak için `--gen-key` komut satırı seçeneği kullanılır.

```
# gpg --gen-key
gpg (GnuPG) 0.9.4; Copyright (C) 1999 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Lütfen istediğiniz anahtarı seçiniz:
   (1) DSA ve ElGamal (öntanımlı)
   (2) DSA (yalnız imzalamak için)
   (4) ElGamal (imzalamak ve şifrelemek için)
Seçiminiz?
```

Bu komut ilk olarak hangi şifreleme algoritmasını kullanmak istediğinizi sorar. 3 seçenek vardır. Öntanımlı değer 1. seçenekle iki anahtar çifti oluşturulur ve kullanılması tavsiye edilen seçenek de budur. Sadece imzaları üretmekte kullanılan bir DSA asıl anahtar çifti ve şifreleme için kullanılan ElGamal (ElCemal) yardımcı anahtar çifti. 2. seçenek, birinciye benzer ancak sadece bir DSA anahtar çifti oluşturur. 4. seçenek[1] hem imzalama hem de şifreleme için kullanılabilen bir ElGamal anahtar çifti üretir. Bütün seçenekler için imzalama ve şifreleme amacıyla ek anahtar çiftlerini daha sonra da üretmek mümkündür.

Daha sonra anahtar boyutunu sorar, öntanımlı ve tavsiye edilen değer 1024'tür.

```
Yeni bir ELG-E anahtar çifti üretmek üzeresiniz.
```

```
                  en küçük anahtar uzunluğu:  768 bit
                 öntanımlı anahtar uzunluğu: 1024 bit
    önerilebilecek en büyük anahtar uzunluğu: 2048 bit
İstediğiniz anahtar uzunluğu nedir? (1024)
```

DSA anahtarının uzunluğu 512 ile 1024 bit arasında, ElGamal anahtarınınki ise herhangi bir uzunlukta olabilirse de GnuPG için anahtar uzunluğunun 768 bitten daha küçük olmaması gereklidir. Diğer yandan 1. seçenek için 1024 bitten daha büyük bir uzunluk belirtirseniz ki, ElGamal için sorun değildir, DSA anahtarı 1024 bitten daha uzun olmayacaktır. 1024 bitlik anahtar son kullanıcı için yeterli güvenliği sağlayacak kadar geniş bir uzay sunar.

Daha uzun anahtar, deneme–yanılmalı saldırılara (brute–force attack) karşı daha güvenlidir, ancak şifrenin kırılmasını engelleyecek yeterliliğe sahip olması gerektiğinden hemen hemen tüm amaçlar için öntanımlı anahtar uzunluğu yeterlidir. Ayrıca, anahtar uzunluğu arttığında şifreleme ve şifre çözme daha yavaş olacak ve büyük anahtar uzunluğundan imzanın uzunluğu da etkilenebilecektir. Bir kere seçildikten sonra anahtar uzunluğu asla değiştirilemez.

Daha sonra anahtarın geçerlilik süresini sorar.

```
Lütfen anahtarın ne kadar süreyle geçerli olacağını belirtin.
         0 = anahtar süresiz geçerli
      <n>  = anahtar n gün geçerli
      <n>w = anahtar n hafta geçerli
      <n>m = anahtar n ay geçerli
      <n>y = anahtar n yıl geçerli
Anahtar ne kadar geçerli olacak? (0)
```

"0" girilirse anahtarın geçerlilik süresi sonsuzdur (eğer bu değer girilirse emin olup olmadığınız sorulur). Çoğu kullanıcı için zamanaşımına uğramayan bir anahtar yeterlidir. Anahtar oluşturulduktan sonra geçerlilik tarihinin değiştirilmesi mümkün olsa da genel anahtarınızı önceden almış olanların elindeki anahtarlara bu değişiklik uygulanamayacağından geçerlilik süresi baştan dikkatli seçilmelidir.

Daha sonra anahtar sahibinin gerçek adı, e–posta adresi ve ek açıklama sorulur (ek açıklama kısmına unvan, kurum gibi bilgiler girilebilir).

```
Anahtarınızın size ait olduğunu belirten bir Kullanıcı-Kimliği olmalı;
Kullanıcı-Kimliği, Gerçek İsminiz, Bir Önbilgi ve e-Posta Adresiniz
alanlarının bir birleşiminden oluşur. Örneğin:
        "Fatih Sultan Mehmed (Istanbul Fatihi) <padisah@osmanli.gov.tr>"

Adınız ve Soyadınız:
```

Ardından girilen tüm bilgiler sunulur ve değişiklik yapmak isteyip istemediğinizi sorulur (girilen bilgiler daha sonra "Anahtar Yönetimi" ile değiştirilebilir. Bu konuya ilerde değinilecektir). Son olarak bir parola girilir ve doğrulaması yapılır.

```
Gizli anahtarınızı korumak için bir Anahtar Parolanız olmalı.

Anahtar parolasını girin:
```

Bir anahtar parolasının uzunluğu için bir sınır yoktur ve çok dikkatli seçilmelidir. Bu parola özel anahtarınızla bir şifreleme ya da deşifreleme yapacağınız zaman sizden istenecektir, özel anahtarınızı sizden başka birisinin kullanması ihtimalini ortadan kaldırmak için bir önlemdir. İdeal olarak bir anahtar parolasında sözlüklerde bulunabilecek sözcükler bulunmamalı ve büyüklü küçüklü alfabetik karakterlerle rakamların ve sembollerin bir karışımından oluşmalıdır. İyi bir anahtar parolası GnuPG'nin güvenli kullanımı için kritik önemdedir.

Parola girildikten sonra anahtar çiftlerinin üretilmesi süreci başlar. Bu sürede farenin hareket ettirilmesi, ölü klavye tuşlarına basılması rastgele sayı üretiminde uygulamaya kaynak sağlar, sistemin etkin çalışmasında

faydalıdır.

2.2. Yürürlükten Kaldırma Sertifikasının Üretimi

Bir anahtar çiftini ürettikten hemen sonra `--gen-revoke` komut satırı seçeneğini kullanarak asıl genel anahtarınız için bir yürürlükten kaldırma sertifikası üretmelisiniz. Anahtar parolanızı unutursanız veya gizli anahtarınız bir şekilde bozulur ya da kaybolursa genel anahtarınızın artık kullanılmaması gerektiğini bildirmek için bu yürürlükten kaldırma sertifikasını yayınlayabilirsiniz. Yürürlükten kaldırılmış bir genel anahtar hala geçmişte kullandığınız imzaları doğrulamakta kullanılabilirse de gelecekte size gönderilecek belgelerin şifrelenmesinde kullanılamaz. Ayrıca, hala gizli anahtarınıza erişiminiz varsa, size geçmişte gönderilmiş şifreli belgelerin şifrelerini çözme gücünüzü etkilemez.

```
# gpg --output revoke.asc --gen-revoke anahtarım
[...]
```

anahtarım argümanı anahtar çiftinizin kullanıcı kimliğinin bir parçası olabileceği gibi asıl anahtar çiftinizin anahtar kimliği de olabilir. Üretilen sertifika `revoke.asc` dosyasında olacaktır. `--output` seçeneği verilmezse sertifika standart çıktıya yazılır. Sertifika kısa olacağından isterseniz, bir yazıcı çıktısı olarak alıp bir kasada da muhafaza edebilirsiniz. Sertifika başkalarının kolayca erişebileceği yerlerde saklanmamalıdır. Aksi takdirde, yürürlükten kaldırma sertifikanız bilginiz dışında yayınlandığında geçerli olan genel anahtarınızın geçersiz hale gelebilir.

2.3. Anahtar Değişimi

Başkaları ile haberleşmek için genel anahtarlarınızı değiş tokuş etmeniz gerekir. Genel anahtarlığınızdaki anahtarların listesini almak için `--list-keys` seçeneğini kullanabilirsiniz.

```
$ gpg --list-keys
/home/nilgun/.gnupg/pubring.gpg
-------------------------------
pub  1024D/86ED4767 2003-06-02 Nilgün Belma Bugüner (http://www.belgeler.org) ¬
 <nilgun@superonline.com>
sub  2048g/44C1CE63 2003-06-02
```

2.3.1. Bir genel anahtarın ihracı

Bir genel anahtarı ilgili kişiye gönderebilmek için onu önce ihraç etmelisiniz. Bu işlem için `--export` komut satırı seçeneği, ihraç edilecek anahtarı belirleyen bir argümanla birlikte kullanılır. Bu argüman, `--gen-revoke` seçeneğindeki gibi, ihraç edilecek anahtar çiftinizin kullanıcı kimliğinin bir parçası olabileceği gibi anahtar çiftinizin anahtar kimliği de olabilir.

```
$ gpg --output nilgun.gpg --export nilgun@superonline.com
```

Bu da genel anahtarınızı insanlara dağıtabilmeniz için genel anahtarınızı bir dosyaya yazma noktasında kullanacağınız bir şeydir. Bu komut seçeneksiz olarak çalıştırıldığında öntanımlı olarak çıktısını standart çıktıya verir. Bu çıktı daha sonra herhangi bir şekilde (keyserver kullanarak, kişisel web sitesine konularak vs.) insanlarla paylaşılır ve insanlar paylaştığınız açık anahtarınızı kullanarak, sizden gelen imzalı bilgileri doğrulayıp okuyabilirler, verileri yalnızca sizin deşifre edebileceğiniz şekilde şifreleyip size gönderebilirler.

Anahtar ikili biçimde ihraç edilir ancak anahtar eposta ile gönderilirken ya da web sayfasında yayınlanacaksa bu elverişli olmaz. Bunun için `--armor` komut satırı seçeneği vardır. Bu seçenekle **uuencode**'lu belgelere benzeyen ASCII zırhlı (ASCII–armored) çıktı üretilebilir. Genelde GnuPG'den çıktılanacak herşey; örneğin, anahtarlar, şifreli belgeler ve imzalar; komut satırına `--armor` seçeneği eklenerek ASCII zırhlı olarak üretilebilir.

```
$ gpg --armor --export nilgun@superonline.com
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (GNU/Linux)

mQGiBD7bos8RBADp2Zqs/P5J187sSMCLaDfMAdcD/Z078OCvAPdPC1oHp5u5xYPq
9NElcYLXkQyfEDc1wMUNAIAbd9MwOKsLAEsxpsS+JyzUOeK7QOrV9nqj3R7IYV/3
8Ow3ENzljR0SouMKjeGOCjSLdwP0qCG6BpU+1ZjOr1e5O2Sakws0czECewCgtSv8
cKXg4FMSalVVeHrQo01YfCED/jUFDa4t5eQyPpy2DHB210XI8cdmoJq+xGCb0I5Q
pR/r5R701AYwLxmY6q0I0vFovpvZBTlL+3PEoHHQwmKi6wzB/170ZDlfSvomOkQl
ylpZpBRraC2JocA5LxjoPFx8VVo2ZX26uBGPj1dZRXcR+IsvuNvX8PcZ+IZIq6Zs
yUJxA/9f9UIix0n6wKUkQVlM0orpZemZGvlosACPjUMsG6fNHmgvNxr2vs6cKMhd
DO5//W6RzqfpuB9j7GlmYfogPpHigcKxfJWqe4f7jDLrlVeRCXcxtXBpmuyMcupX
6qu9BxubQlvreSvN7b+ehivBTPiL9XvVtY6BScrYJePn4nXc0bRJTmlsZ8O8biBC
ZWxtYSBCdWfDvG5lciAoaHR0cDovL3d3dy5iZWxnZWxlci5vcmcpIDxuaWxndW5A
c3VwZXJvbmxpbmUuY29tPohZBBMRAgAZBQI+26LPBAsHAwIDFQIDAxYCAQIeAQIX
gAAKCRB2bxy7hu1HZ5qyAKCl1Lvb40QfSOpDrUjKjuf89+oqegCgkSPhdfyDBmo7
ewcZ0MTy+uJbEKW5Ag0EPtui7hAIAKDjlz7MgzJpEid0EALJ8vwFRZrXXlxM1b+1
mnuLI3tZg5yzNqY1eQTQdixQbK510DePbZFWDhsr4E6gg+991zJ0LyExaNCkpJps
irLYokrls2p3QADiGq9g4GkYEcgjOX4/KMGgHOhnEup70LuXhvjFq5pwn2E4bNhX
tcVi+bTo1lDyMZlMXUfWylkS4+ckCikvNgWeyiHTqPVVqLCWSfrXh57tlWuYjwV9
/Ts83YKOesqXW7XCPwKiZVGl4UFKLsQadF2fZ6pT4vTL0ztkcbt20p7Y2pzBDAgj
yz5ruYuDqnxzwquR2uqBs6WTUiogYG4ZFvCdYtQSTWOqRJwO8RcAAwUH/jTqHUol
9alCgt+WjoEzY6RW8fyx7gZlxcFVdQgcnTK+QmwjX6RTqU+lpfzfxYrkv0vcfuSW
zK6LzM1/f/YqWO0ofuJJuOXyYJR1BUplB2xRLRDuWhttlQksmgoDiJczK20yTlbK
HBJ0G5BZsCq/3pz2KraII2wByNMmsB6DIs+4DMJH0foBBnx+/8GUobzMscUltIaa
itWoogQKytt3bgsUbwGe0WXlzQwbqCzF86BFRznrEaP68nRqI4x6ZCNOW1zcZxsT
07DqivmVXCU0aTLsqxPYrpiRkQTDrqrKl8MwUgyV9R8MOSlSCm0sLtsjyviYkxup
OIGXvr+YumNPgCSIRgQYEQIABgUCPtui7gAKCRB2bxy7hu1HZ54fAJ4k4OkBsBgk
s4XcwiWZzlpebjSRlACeIPple7xUNKbaDse2ii1NsTIOoq8=
 =4wmv
-----END PGP PUBLIC KEY BLOCK-----
```

```
$ gpg --output nilgun.sec.asc --export-secret-key 86ED4767
```

Bu komut özel anahtarı ikili olarak `nilgun.sec.asc` isimli dosyaya yazar. Özel anahtarın gizliliğinin sağlanması gereklidir.

```
$ gpg --keyserver www.keyserver.net --send-keys 86ED4767
```

Ayrıca GPG, anahtarlarınızı paylaşmanız için yukarıdaki gibi bir yol sunar. Internet'e bağlıyken bu komut *nilgun* kullanıcısının genel anahtarını, `www.keyserver.net` adresindeki anahtar sunucusuna gönderir. (Bütün anahtar sunucuları anahtar havuzunu ortak kullanır, herhangi birine gönderilen bir anahtarı bir diğerinden sorgulayabilirsiniz.)

2.3.2. Bir genel anahtarın ithali

Bir genel anahtarı genel anahtarlığınıza `--import` komut satırı seçeneğini kullanarak ekleyebilirsiniz.

```
$ gpg --import isim.gpg
gpg: anahtar 9E98BC16: genel anahtar alındı.
gpg: İşlenmiş toplam miktar: 1
gpg:                alınan: 1
```

Genel anahtarını insanlarla paylaşmak istemiş (genel anahtarını ihracetmiş ve bir anahtar sunucusuna veya sayfasına koymuş ya da bir şekilde size göndermiş) bir kişinin genel anahtarını genel anahtarlığınıza dahil etmenizi sağlar. Örneğin `certserver.pgp.com` sunucusundan, genel anahtarına sahip olmak istediğiniz

kişinin adını ya da e–posta adresini aratabilir, bulunan anahtarı bir dosyaya kopyalayabilir ve bu içeriği bu kişinin genel anahtarı olan dosyayı, yukarıdaki komutla genel anahtarlığınıza dahil edebilirsiniz. Bu işlem sonucunda siz, söz konusu kişiden gelen imzalanmış verileri doğrulayıp okuyabilir ve yalnızca onun deşifre edebileceği şekilde veri şifreleyip kendisine gönderebilirsiniz.

Bir anahtar ithal edilir edilmez doğrulanmalıdır. GnuPG ithal ettiğiniz her anahtarı kişisel olarak doğrulamanızı gerektirmeyen güçlü ve esnek bir güvence modeli kullanır. Ancak bazı anahtarlar yine de kişisel olarak doğrulanmayı gerektirebilir. Bir anahtar onun parmakizinden doğrulandıktan sonra anahtar imzalanarak geçerli bir anahtar haline gelebilir. Bir anahtarın parmakizi `--fingerprint` komut satırı seçeneği ile çabucak görüntülenebilir. Ancak anahtarı geçerli hale getirmek için onu düzenlemelisiniz.

```
$ gpg --fingerprint
```

Bir anahtarın parmakizi anahtarın sahibi ile doğrulanır. Bunu anahtar sahibi ile ya telefonla görüşerek veya sizin için güvenli olan herhangi bir yöntemle haberleşerek yapabilirsiniz. Eğer sizdeki parmakizi sahibinden aldığınız parmakizi ile aynıysa sizdeki anahtarın doğru kopya olduğundan emin olabilirsiniz.

Parmakizi denetimi bittikten sonra anahtarı imzalayarak onu geçerli hale getirebilirsiniz. Anahtar doğrulaması genel anahtar kriptografisinin zayıf karnı olduğundan, bir anahtarı imzalamadan önce anahtarın parmak izini *daima* anahtarın sahibi ile haberleşerek doğrulatmalı ve bu konuda çok çok dikkatli olmalısınız.

```
$ gpg --sign-key farukesk@comu.edu.tr
```

2.4. Bir anahtarın silinmesi

```
$ gpg --delete-key anh–kiml
```

Sisteme dahil edilmiş *anh–kiml* anahtar akimlikli kullanıcının genel anahtarını siler. Bu kullanıcının özel anahtarı da sistemde mevcutsa ilk önce bunun silinmesi gerekir.

3. Belgelerin Şifrelenmesi ve Şifresinin Çözülmesi

Genel ve gizli anahtarların her biri belgelerin şifrelenmesi ve şifrelerinin çözülmesinde kendilerine özel rollere sahiptir. Bir genel anahtar açık güvence olmak niyetinde olabilir. İlgili kişi bir belgeyi bir genel anahtar kullanarak şifrelediğinde belge kasaya konmuş, kasa kapatılmış ve anahtar defalarca döndürülerek kilitlenmiştir. Karşılığı olan gizli anahtarın rolü ise kasayı yeniden açmak ve belgeyi almaktır. Başka bir deyişle, bir genel anahtarla şifrelenmiş bir belge, sadece bu genel anahtarın karşılığı olan gizli anahtarı bulunduran kişi tarafından okunabilir.

Belgelerin şifrelenmesi ve şifrelerinin çözülmesi süreci bu düşünce modeli ile basitleşmiştir. Murat'a göndereceğiniz bir mesajı şifrelemek isterseniz, onu Murat'ın genel anahtarını kullanarak şifrelersiniz ve Murat'da onu kendi özel anahtarını kullanarak çözüp okur. Eğer, Murat size bir şifreli mesaj göndermek isterse, mesajı sizin genel anahtarınızı kullanarak şifreler ve siz bu mesajı kendi özel anahtarınızla çözüp okursunuz.

Bu iki işlem için önemli bir ortak nokta vardır. Eğer sistemde birden fazla özel anahtar yüklüyse işlemin hangi kullanıcı olarak yapıldığını belirtmek gerekir. Belirtilmezse, işlemi yapan kullanıcı öntanımlı kullanıcıdır. Belirtme işlemi bir seçenektir **`-u kullanici_adi`** şeklinde yapılır.

3.1. Şifreleme

Bir belgeyi şifrelemek için `--encrypt` komut satırı seçeneği kullanılır. Elinizde şifreli belge göndermek istediğiniz alıcıların genel anahtarları olmalıdır. Yazılım, şifrelenecek belgenin girdi olarak verilmesini bekler; eğer verilmezse standart girdiyi okur. Şifrelenmiş belge ya standart çıktıya konur ya da `--output` seçeneği verilmişse onun argümanı olarak belirtilen dosyaya konur. Belge şifrelemeye ek olarak güvenliği arttırmak için sıkıştırılır.

```
$ gpg --output belge.gpg --encrypt --recipient anh–kiml belge
```

`--recipient` komut satırı seçeneği her alıcı için bir kere kullanılır ve argüman olarak belgeyi şifrelemekte kullanılacak genel anahtarı alır. Şifreli belge sadece alıcıların genel anahtarlarının karşılığı olan özel anahtarlarla çözülebilir. Özellikle, kendiniz şifrelediğiniz bir belgenin şifresini çözebilmeyi istiyorsanız, kendi genel anahtarınızı da alıcılar listesine eklemelisiniz (ya da belgeyi imzalamalısınız, imzalama genel anahtarınızı devreye sokar).

Bu komut ile *anh–kiml* anahtar kimlikli alıcının genel anahtarı bu komutun girildiği sistemde mevcutken, *anh–kiml* anahtar kimlikli alıcının özel anahtarını kullanarak açabileceği şifrelenmiş ve sıkıştırılmış veriyi **gpg** uzantılı bir dosyaya yazar. Ayrıca, herhangi birisinin şifrelediğiniz bu verinin kendisi tarafından gönderildiğini iddia etme riskini ortadan kaldırmak için bu veriyi kendi özel anahtarınızla imzalamalısınız. Bu işin tamamını aşağıdaki komut ile yapabilirsiniz, bu komut çıktısını `asc` uzantılı bir dosyaya yazar:

```
$ gpg -u gönderen -r alıcı --armor --sign --encrypt belge
```

Bilgi

`-u` seçeneğini kullanmazsanız, veri sistemdeki öntanımlı özel anahtar ile imzalanır. Eğer sistemde birden fazla özel anahtar varsa, *gönderen* yerine bu anahtarlardan kullanmak istediğinizin anahtar kimliğini yazarak, imzalama işlemini gerçekleştirebilirsiniz. Hatırlayacağınız gibi, anahtar kimliklerini görmek için *gpg —list–keys* çıktısından faydalanabilirsiniz.

Örnek 1.

```
$ gpg --output cikti_dosyasi --export farukesk
```

Bu komut *farukesk* isimli kullanıcının ortak anahtarını ikili biçimde `cikti_dosyasi` isimli dosyaya yazar.

Örnek 2.

```
$ echo "Merhaba, bu mesajı zyariz gonderdi :)" | gpg -u farukesk -r meren -ea | ¬
mail meren@comu.edu.tr
```

Bu komut "*Merhaba, bu mesajı zyariz gonderdi :)*" mesajını *farukesk* kullanıcısı olarak ascii kipte *meren* kullanıcısı için şifreler, çıktısını da <meren (at) comu.edu.tr> adresine postalar.

3.2. Şifre Çözme

Bir mesajın şifresini çözmek için `--decrypt` komut satırı seçeneği kullanılır. Bunun için mesajın şifrelendiği genel anahtarın karşılığı olan gizli anahtara ihtiyacınız vardır. Şifreleme işlemine benzer olarak şifresi çözülecek belge girdi olarak alınır ve çözülmüş belge çıktılanır.

```
$ gpg --output belge --decrypt belge.gpg
```

Genel anahtarınıza sahip birisinin, onu kullanarak yalnızca sizin açmanız için şifrelediği veriyi deşifre etmenizi sağlar. Seçeneksiz kullanımda çıktısını standart çıktıya yazar. **`--output belge`** seçeneği eklenirse çıktı `belge` dosyasına yazılır. Bu komut `belge.gpg` isimli dosya içerisindeki şifreli veriyi özel anahtarınızın parolasını istedikten sonra deşifreler ve çıktıyı `belge` dosyasına yazar.

3.3. Simetrik Şifre ile Şifreleme

Belgeler genel anahtar kriptografisi kullanılmadan da şifrelenebilir. Bunun yerine belgeyi şifrelemekte simetrik şifre de kullanabilirsiniz. Simetrik şifreyi sürmede kullanılan anahtar, belge şifrelenirken belirtilen paroladan

üretilir ve iyi bir güvenlik için bu parola gizli anahtarınızı korumakta kullandığınız anahtar parolası olmamalıdır. Simetrik şifreleme başkaları ile haberleşirken parolaya ihtiyaç duyulmadığında belge güvenliğini sağlamak için elverişlidir. Bir belgeyi simetrik şifre ile şifrelemek için `--symmetric` komut satırı seçeneği kullanılır.

```
$ gpg --output belge.gpg --symmetric belge
Anahtar parolasını girin:
```

4. İmzalama ve Doğrulama

Bir sayısal imza bir belgeyi onaylamak ve tarih damgası vurmak için kullanılır. Bir belge herhangi bir şekilde imzalamanın ardından değiştirilirse, imzanın doğrulanması başarısız olur. Bir sayısal imza, bir elyazısı imzanın kullanım amacına ek olarak değişikliğe dirençlilik gibi bir yararı da beraberinde sunar. Örneğin, GnuPG kaynak paketi imzalı dağıtılır; paketlendikten sonra kaynak kodu değişikliğe uğramışsa, imza doğrulaması başarısız olacaktır.

İmzaların oluşturulması ve doğrulanmasında genel/gizli anahtar çifti ile şifreleme ve şifre çözmeden farklı bir işlem uygulanır. Bir imza, imzalayanın gizli anahtarı kullanılarak oluşturulur. İmzanın doğrulaması ise karşılığı olan genel anahtar kullanılarak yapılır. Örneğin, Murat yazdığı son makaleyi gönderirken kendi gizli anahtarı ile ürettiği imza ile imzalamalıdır. Dergi editörü makalenin üzerindeki imzanın Murat'a ait olup olmadığını ve Murat'ın makalesinde değişiklik olup olmadığını Murat'ın genel anahtarını kullanarak anlayabilir. Sayısal imzaların kullanımının bir önemi de uzlaşma için gizli anahtarın açıklanması gerektiğinden yapılan sayısal imzanın yalanlanmasındaki zorluktur.

4.1. İmzalama

`--sign` komut satırı seçeneği sayısal imzaları üretmekte kullanılır. İmzalanacak belge girdi olarak alınır ve imzalı belge çıktılanır.

```
$ gpg --output makale.sig --sign makale
```

Bu komut veriyi imzalar ve sıkıştırır. Çıktı `sig` uzantılı okunamaz bir dosyadır. Komuta eklenecek **`--clearsign`** parametresi, çıktının okunabilir bir `asc` uzantılı dosyaya saklanmasını sağlar.

Örnek 3.

```
$ gpg -u gönderen -r alıcı --armor --sign --encrypt veri
```

Bu komut *veri* dosyasındaki veriyi şifreler, imzalar ve çıktısını *veri.asc* dosyasına ASCII biçimde yazar.

4.2. Doğrulama

Bir imzalı belge aldığınızda hem imzayı denetleyebilir hem de imzayı denetleyip özgün belgeyi açabilirsiniz. İmza denetimi için `--verify` komut satırı seçeneği kullanılır. İmzayı doğrulayıp belgeyi açmak için ise `--decrypt` seeneği kullanılır. Doğrulanacak ve açılacak imzalı belge girdi olarak alınır ve açılan belge çıktılanır.

```
$ gpg --output belge --decrypt belge.sig
```

4.3. Açık imzalı belgeler

Sayısal imzaların genellikle kullanıldığı yerlerden bazıları da eposta iletileri ve haber gruplarına gönderilen postalardır. Bu tür metinler imzalanırken sıkıştırılmaları istenmez. `--clearsign` komut satırı seçeneği kullanılarak metin ASCII zırhlı bir imza ile sarmalanır, ancak bu takdirde metnin değiştirilememesi sağlanır.

```
$ gpg --clearsign belge
```

4.4. Ayrık imzalar

Bir imzalı belgenin kullanışlılığı sınırlıdır. İmzalı belgeden orjinal belgeyi elde etmek isteyen kullanıcılar, belge açık imzalı olsa bile, imzalı belgeyi düzenlemek zorundadır. Bu nedenle, bir belgeyi imzalamak için üçüncü bir yol bulunmuştur. Bu imzalama türünde ayrı bir dosya olarak bir ayrık imza oluşturulur. Bir ayrık imza `--detach-sig` komut satırı seçeneği kullanılarak oluşturulur.

```
$ gpg --output belge.sig --detach-sig belge
```

İmzayı doğrulamak için belge ve ayrık imza birlikte kullanılır. İmzayı denetlemekte `--verify` seçeneği kullanılır.

```
4 gpg --verify belge.sig belge
```

5. Kavramlar

GnuPG ***simetrik şifreler***, ***genel anahtarlı şifreler*** ve ***tek yönlü haşlama :–)*** gibi çeşitli kriptografik kavramlar kullanır. Bu kavramları çok iyi bilmeden de GnuPG kullanabilirsiniz ancak, onları biraz bile anlamak GnuPG'yi akıllıca kullanmak için gereklidir.

Bu kısımda GnuPG'de kullanılmış olan kriptografik kavramlar ele alınmıştır. Başka kitaplarda bu konular daha ayrıntılıdır. Bu öğretiyi izleyebileceğiniz iyi bir kitap Bruce Schneier[B4]'in "Applied Cryptography"[B5] kitabıdır.

5.1. Simetrik Şifreler

Simetrik şifre, hem şifreleme hem de şifre çözme için aynı anahtarın kullanıldığı bir şifredir. Haberleşirken bir simetrik şifreyi kullanan iki taraf, anahtarın diğer tarafta mevcut olduğunu varsayar. Bu varsayımdan hareketle gönderici bir mesajı anahtarı kullanarak şifreler ve onu alıcıya gönderir. Alıcı da bu gönderinin şifresini anahtarı kullanarak çözer. Bir örnek olarak, German Enigma bir simetrik şifredir ve günlük kullanılan anahtarlar kod kitabında dağıtılmıştır. Her gün gönderen ya da alan radyo operatörü günün anahtarını bulmak için kod kitabının kendindeki kopyasından yararlanır. Gün içindeki radyo trafiği günün anahtarı kullanılarak şifrelenir ve şifresi çözülür. Simetrik şifrenin günümüzdeki örnekleri arasında 3DES, Blowfish ve IDEA sayılabilir.

İyi bir şifre güvenliğin tamamını anahtara yükler, algoritmaya değil. Başka bir deyişle, hangi şifrenin kullanıldığını bilse bile bu şifrenin saldırgana hiçbir yardımı olmamalıdır. Sadece algoritmanın ne olduğu bilgisine gereksinimi olan anahtarı ele geçirir. GnuPG içinde kullanılan şifreler bu özelliğe sahiptir.

Güvenliğin tamamının anahtarda olmasından dolayı, anahtarın tahmin edilmesinin güçlüğü önemli bir faktördür. Başka bir deyişle, olası anahtarların kümesinin, vs. *anahtar uzayı*nın çok geniş olması gerekir. Los Alamos'dayken, Richard Feynman kasa açma yeteneği ile ümlüydü. İşin esrarını arttırmak için yanında içinde eski bir steteskop da bulunan bir alet çantası taşırdı. Gerçekte, doğru birleşimlerin sayısını zekice yöntemlerle düşürerek doğru birleşimi bulmak için bunları denemek yolunu kullanırdı. Başka bir deyişle, anahtar uzayını küçültürdü.

İngiltere II. Dünya Savaşı sırasında anahtarları keşfetmek için makina kullandı. Alman radyosu German Enigma çok geniş bir anahtar uzayı kullanıyordu, ama İngiltere de Bombes adını verdikleri bir makina ile deneyerek günün anahtarını bazan buluyordu.[2] Bazan günün anahtarı birkaç saat içinde bulunabilirken bazan bu hiç mümkün olmuyordu. Bombes genel amaçlı bir hesap makinası değildi, ama günümüz hesap makinalarının öncülerinden biriydi.

Bugün, bilgisayarlar anahtarları çok çabuk tahmin edebilmesi anahtar uzunluğunun günümüz kriptosistemleri için önemini arttırmaktadır. DES şifresi 56 bitlik bir anahtar kullanır. Bu da 2^{56} yani 72,057,594,037,927,936 tane

olası anahtar demektir. Bu büyük bir miktarmış gibi görünse de günümüzdeki sıradan bir bilgisayar günlerle ifade edilen bir sürede tüm anahtar uzayını tarayabilmektedir. Bu işe hasredilmiş bir bilgisayarla ise birkaç saat sürmektedir. Diğer yandan daha yakın zamanlarda 3DES, Blowfish, IDEA gibi 128 bitlik anahtarlar kullanan şifreler tasarlanmıştır. Bunlarla çok daha fazla sayıda, 2^{128} tane anahtar üretilebilir. Bu öyle büyük bir sayıdır ki, dünyadaki tüm bilgisayarlar birarada çalışıp tüm anahtar uzayını taramaları evrenin yaratılmasından zamanımıza kadar geçen süreden fazlasına ihtiyaç duyacaktır.

5.2. Genel Anahtarlı Şifreler

Simetrik şifrelerle igili asıl sorun onların güvenlikleri ile değil, anahtar değişimi ile ilgilidir. Güvenli haberleşme için gönderici ve alıcı anahtarlarını değiş–tokuş ederler de, bu değiş–tokuşun yapıldığı haberleşme kanalı ne kadar güvenlidir? İşte bu noktada saldırganın işi kolaydır, anahtarın yolunu kesmeye çalışacak sonra da anahtar uzayındaki tüm anahtarları deneyecektir. Bir diğer sorun da gerekli anahtarların sayısı ile ilgilidir. Haberleşmek isteyen `n` kişi varsa haberleşme gizliliğine ihtiyaç duyan kişilerin her çifti için `n(n-1)/2` anahtar gerekecektir. Bu küçük bir grup için sorun değildir ama bu grup çok kısa sürede çok büyük bir grup haline gelir.

Genel anahtarlı şifreleme ile anahtar değişimi sorunu tamamen ortadan kalkmaktadır. Bir genel anahtarlı şifre mesajların gönderilmesi sırasında bir anahtar çifti kullanır. Başka iki anahtarı da mesajı alan taraf kullanır. Anahtarlardan biri *genel anahtar*dır ve herkese verilebilir, diğeri ise *gizli anahtar*dır ve anahtarın sahibi tarafından herkesten gizlenir. Bir gönderici göndereceği mesajı alıcının genel anahtarı ile şifreler ve alıcı da bu mesajı kendi gizli anahtarı ile çözer.

Bu protokol simetrik şifrelerin doğasında olan anahtar değişimi sorununun çözümüdür. Gönderici ve alıcının diğerinden bir anahtar kabul etmeye ihtiyacı yoktur. Gizli haberleşmenin yapılmasından çok önce gönderici alıcının genel anahtarının bir kopyasını zaten almış olur. Diğer yandan aynı genel anahtarın kopyalarını alıcı ile gizlilik gerektiren iletişim gerçekleştirmek isteyen herkes tarafından kullanılabilir. Bu durumda `n` kişi için sadece `n` anahtar çifti gerekir.

Genel anahtarlı şifreleme tuzak kapılı tek yönlü işlev (one–way trapdoor function) üzerine inşa edilmiştir. Bir tek yönlü işlevin hesaplanması kolay olduğu halde tersinin hesaplanması çok zordur. Örneğin asal sayıların çarpımlarından oluşan bir sayıyı elde etmek kolaydır ancak böyle bir sayıyı asal çarpanlarına ayırmak daha zordur. İşte tuzak kapılı tek yönlü işlevde böyle birşeydir ancak onun bir tuzak kapısı vardır yani bilginin bazı parçaları bilinir, böylece tersini hesaplamak kolaylaşır. Örneğin iki asal sayının çarpımından oluşan bir sayıyı asal çarpanlarına ayırmak, çarpanlarından biri bilindiğinde çok kolay olur. Bir genel anahtarlı şifre asal sayıların çarpımları üzerine kurulur. Bir genel anahtar iki çok büyük asal sayının çarpımıdır ve şifreleme algoritması mesajı şifrelerken bu birleşimi kullanır. Şifreyi çözen algoritmanın asal çarpanları bilmesi gerekir. Gizli anahtar bu çarpanlardan birini içeriyorsa şifrenin çözülmesi kolay olur ancak çarpanlardan biri bile bilinmiyorsa çözüm çok çok zor olur.

İyi bir simetrik şifredeki gibi iyi bir genel anahtarlı şifre de güvenlik ihtiyaçlarının tamamını anahtara yükler. Burada da anahtarın uzunluğu sistemin güvenilirliğinin ölçüsüdür. Ancak bir simetrik şifreleme anahtarının uzunluğu ile bir genel anahtarlı şifreleme anahtarının uzunluğu arasındaki göreli bir ilişkiyle güvenilirlik derecesini ilişkilendirmek bir ölçü değildir. Bir deneme yanılmalı saldırıda 80 bitlik anahtarlı bir simetrik şifreyi oluşturan anahtarı bulmak için saldırgan 2^{80} anahtarı tek tek deneyecektir. Bir genel anahtarlı şifre üzerine böyle bir saldırı yapıldığında saldırgan, 512 bitle kodlanmış (155 haneli bir sayı) birleşiminin çarpanlarını bulmaya çalışacaktır. Saldırganın iş yükü temel olarak saldırdığı şifreye bağlıdır. Simetrik şifreler için günümüzde 128 bit yeterli olurken, günümüzdeki çarpanlara ayırma teknolojisi gözönüne alındığında, genel anahtarlarda 1024 bitin yeterli olacağı anlaşılmaktadır.

5.3. Melez Şifreler

Genel anahtarlı şifreler her derdin devası değildir. Birçok simetrik şifre güvenlik noktasından bakıldığında

daha sağlamdır, genel anahtarlı şifreleme ve şifre çözme işlemi ise simetrik sistemlerdeki aynı tür işlemlerle karşılaştırıldığında daha masraflıdır. Buna rağmen genel anahtarlı şifreleme simetrik şifreleme anahtarlarının dağıtımı için faydalı bir araçtır ve bu, melez şifreleme sistemlerinin nasıl çalıştığı hakkında bir fikir verir.

Bir melez şifre hem simetrik şifreyi hem de genel anahtarlı şifreyi kullanır. Bu mekanizma, bir simetrik şifreyi paylaştırmakta bir genel anahtarlı şifreyi kullanır. Simetrik şifreyi taşıyan mesaj genel anahtarla şifrelendikten sonra alıcısına gönderilir. Simetrik anahtar paylaşımının güvenliği için gönderilen her mesaj için farklı simetrik anahtar kullanılır. Bu nedenle, bazan ona oturum anahtarı dendiği de olur.

Hem PGP hem de GnuPG melez şifreleri kullanmaktadır. Oturum anahtarı, genel anahtarlı şifre kullanılarak şifrelenir ve gönderilecek mesaj da simetrik şifre ile şifrelenerek her ikisi otomatik olarak bir paket içinde birleştirilir. Alıcı gizli anahtarını kullanarak oturum anahtarının şifresini çözer ve elde ettiği oturum anahtarı ile mesajın şifresini çözer.

Bir melez şifre, kullandığı genel anahtarlı veya simetrik şifreden daha sağlam değildir. Bunlardan zayıf olanı kadar zayıftır. PGP ve GnuPG için genel anahtarlı şifre çiftin daha zayıf olanıdır. Bereket versin ki, yine de, eğer bir saldırgan oturum anahtarını ele geçirirse sadece bu oturum anahtarı ile şifrelenmiş mesajı okuyabilecektir. Başka bir mesajı okumak için benzer işlemleri yeniden yapmak zorundadır, çünkü oturum anahtarı her mesaja özeldir.

5.4. Sayısal İmzalar

Bir hash işlevi, girdisini bir sonlu sayılar kümesi içindeki bir değerle eşleştiren bir işlevdir. Genel olarak bu küme doğal sayılar aralığıdır. Basit bir hash işlevi x'lerin tamsayılardan oluştuğu $f(x) = 0$ eşitliği ile ifade edilir. Daha ilginç bir hash işlevi ise $f(x) = x \bmod 37$ dir. İşlevdeki x'in değeri, x'in 37 ile bölünmesinden kalandır.

Bir belgenin sayısal imzası belgeye bir hash işlevinin uygulanmasının sonucudur. Kullanım amacına uygun olarak, bir hash işlevi iki önemli özelliğinin sağlanmasını gerektirir. İlki, aynı değere haşlanan iki belgenin bulunması zor olmalıdır. İkincisi ise, verilen bir hash değerini sağlayan bir belgenin bulunması zor olmalıdır.

Bazı genel anahtarlı şifreler[3] belgeleri imzalamakta kullanılabilir. İmzacı belgeyi kendi gizli anahtarı ile şifreler. İmzayı kontrol etmek ve belgeyi görmek isteyen biri basitçe imzacının genel anahtarını kullanarak belgenin şifresini çözer. Bu algoritma, iyi bir hash işlevinin gerektirdiği iki özelliği sağlar, fakat pratikte, bu algoritma kullanışlılık bakımından çok yavaştır.

Bir alternatif de, bu iki önemli özelliği sağlamak üzere tasarlanmış hash işlevleri kullanmaktır. SHA ve MD5 bu algoritma için örnek olarak verilebilir. Bu algoritma kullanıldığında, bir belge onunla hash'lenerek imzalanmıştır ve hash değeri de imzadır. Bir başka kişi imzayı, belgenin ondaki kopyasını ayrıca hash'leyerek ve bu hash değerini orjinal belgenin hash değeri ile karşılaştırarak kontrol eder. Bu iki değer aynıysa belgeler de birbirinin aynıdır.

Şüphesiz, şimdiki sorun imza denetimi ile etkileşecek bir saldırgana izin vermeksizin sayısal imzalarda hash işlevinin kullanılmasıdır. Belge ve imza şifrelenmeksizin gönderilirse, bir saldırgan belgeyi değiştirebilir ve alıcının bilgisi dışında değişmiş belgeye uygun bir imza üretebilir. Eğer sadece belge şifrelenmişse, saldırgan imzayı tahrif ederek imza denetiminin başarısız olmasına sebep olabilir. Bir üçüncü seçenek de belgenin ve imzanın bir melez genel anahtarlı şifreleme kullanarak şifrelenmesidir. İmzalayan, kendi gizli anahtarını kullanır, diğer herkes belgeyi ve imzayı kontrol etmek için onun genel anahtarını kullanır. Buradan sesler iyi geliyor da, etkisi yok. Eğer bu algoritma gerçekten belgeyi güvenilir kılıyorsa, belgenin tahrif edilmesine karşı da güvenilir olacaktır ve imzaya gerek kalmayacaktır. Yine de bir takım sorunlar hala vardır; imza ve belgenin ikisini birden tahrif edilmekten koruyamaz. Bu algoritmada, simetrik şifrenin oturum anahtarı imzalayanın gizli anahtarı kullanılarak şifrelenir. Başkaları oturum anahtarını elde etmek için genel anahtarı kullanabilir. Bu sebeple, saldırgan için oturum anahtarını elde etmek kolaydır ve onu kullanarak yerine koyduğu belgeleri ve imzaları şifreleyip göndericinin ismiyle başkalarına gönderebilir.

Çalışan bir algoritma sadece imzayı şifrelemek için bir genel anahtar algoritmasının kullanıldığı algoritmadır. Hash değeri imzalayanın gizli anahtarı kullanılarak şifrelendiğinden herhangi biri genel anahtarı kullanarak imzayı kontrol edebilir. İmzalı belge herhangi bir algoritma kullanılarak gönderilebilir, belge genel amaçlı ise hiçbir şifreleme de yapılmayabilir. Belge değişikliğe uğrarsa, imza denetimi başarısız olacaktır, ancak bu, imza denetiminin tam olarak neyi yakalayacağının varsayıldığı ile ilgilidir. Sayısal İmza Standardı (DSA – Digital Signature Standard) tam da yukarıda anlatıldığı gibi çalışan bir genel anahtarlı imza algortimasıdır. DSA, GnuPG tarafından kullanılan birincil imzalama algoritmasıdır.

Belge ile ilgili görüş ve önerilerinizi lütfen iletmekten çekinmeyiniz. GNUPG, açık anahtarlı kriptografi teknikleri üzerine temellenmiş bir uygulamadır. Açık anahtarlı kriptografi hakkında daha geniş bilgiyi http://zion.comu.edu.tr/~evreniz/belgeler/pkc/pkc.html adresinden temin edebilirsiniz.

6. Yasal Açıklamalar

6.1. Telif Hakkı ve Lisans

6.2. Feragatname

Bu belgedeki bilgilerin kullanımından doğacak sorumluluklar, ve olası zararlardan belge yazarı sorumlu tutulamaz. Bu belgedeki bilgileri uygulama sorumluluğu uygulayana aittir.

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

GNU Free Documentation License

Version 1.2, November 2002

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. Secondarily, 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 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.

(1) 3. seçenek imzalamak için kullanılamayan bir tür ElGamal anahtar çifti üretir.

(B4) http://www.counterpane.com/schneier.html

(B5) http://www.counterpane.com/applied.html

(2) II. Dünya Savaşı sırasında İngiltere kıyılarında karaya oturan bir Alman denizaltısında daktilo makinasına benzer bir makina buldular. Bu makinanın günün anahtarını üreten makina olduğunu keşfettiler ve bu makinaya Bombes adını verdiler.

(3) Şifre, gerek genel anahtarın gerekse gizli anahtarın şifreleme algoritması tarafından genel anahtar olarak kullanılabilmesi özelliğine sahip olmalıdır. RSA bu algoritmaya uygunken ElGamal uygun değildir.

Bu dosya (gpg–kullanimi.pdf), belgenin XML biçiminin TEXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

23 Ocak 2007