DİJİTAL GÜVENLİK SİSTEMLERİ VE PGP

S. Nalan TOPBAĞ nalan@turksis.com
Fatih ABLAK fatih@turksis.com

ŞİFRELEME VE ALGORİTMALARI

Şifreleme : Bir bilginin içeriğini başkalarının anlayamayacağı hale getirilmesidir.

Temelde bilgi güvenliği için şifreleme kullanılır. Bilginin güvenliği; başkası tarafından dinlenme, bilginin değiştirilmesi ve kimlik taklidi gibi tehditlerin ortadan kaldırılması ile sağlanır.

ŞİFRELEME VE ALGORİTMALARI

Sezar Şifresi:

0 1 2
012345678901234567890123 45
ABCDEFGHIJKLMNOPQRSTUVWXYZ

çözme yönü
şifreleme yönü NOPQRSTUVWXYZABCDEFGHIJKLM
|
n=13

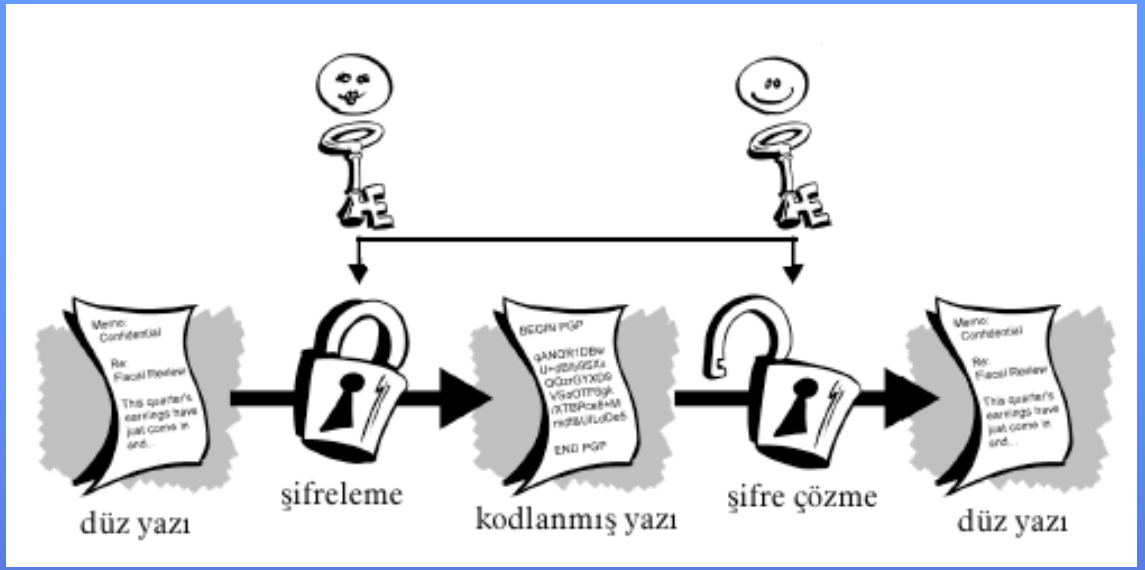
Açık Metin: "SEZAR SIFRESI"
Şifrelenmiş Metin: "FRMNE FVSERFV"

ŞİFRELEME VE ALGORİTMALARI

Şifrelemek ve deşifre etmek için kullanılan sayısal karakterler dizisine anahtar denilir. Kullanılan anahtar yapısına göre şifreleme algoritmaları iki çeşittir : Simetrik (Gizli) ve asimetrik (Açık).

Kullanılan algoritmanın gücü anahtarın yapısı ile doğru orantılıdır.

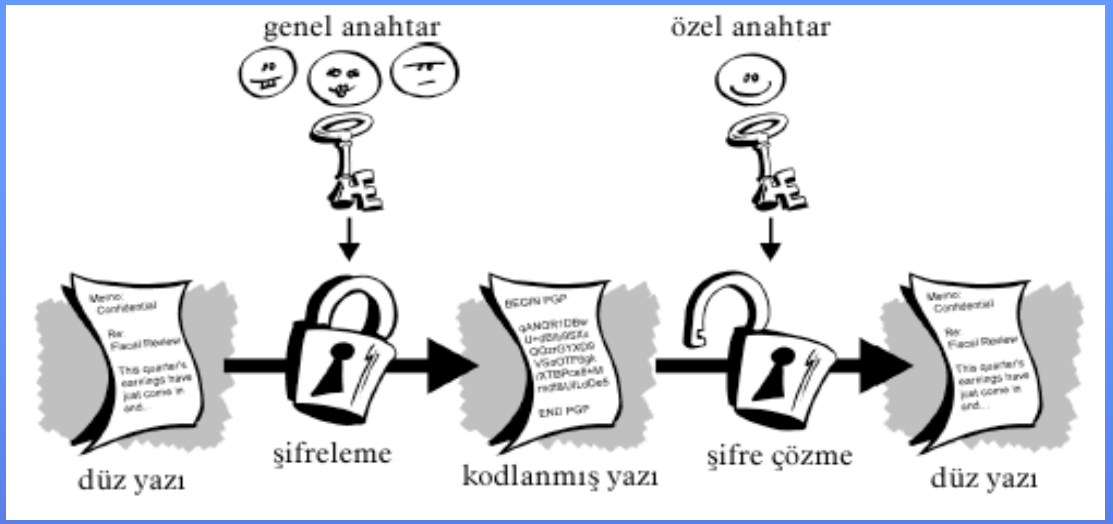
SİMETRİK ŞİFRELEME ALGORİTMALARI



Simetrik anahtar algoritmaları şifreleme ve deşifre işleminde aynı anahtar kullanılır. En çok kullanılan simetrik yöntemler :

- ✓ Des
- ✓ 3Des
- ✓ Dea

ASİMETRİK ŞİFRELEME ALGORİTMALARI



Asimetrik anahtar algoritmalarında şifreleme işleminde ve deşifre işleminde kullanılan anahtarlar farklı anahtarladır. En çok kullanılan yöntemler :

- ✓RSA
- ✓DSA

RSA

Şifreleme : $y = x^e \bmod n$

Deşifre : $x = y^d \bmod n$

$n = p*q$

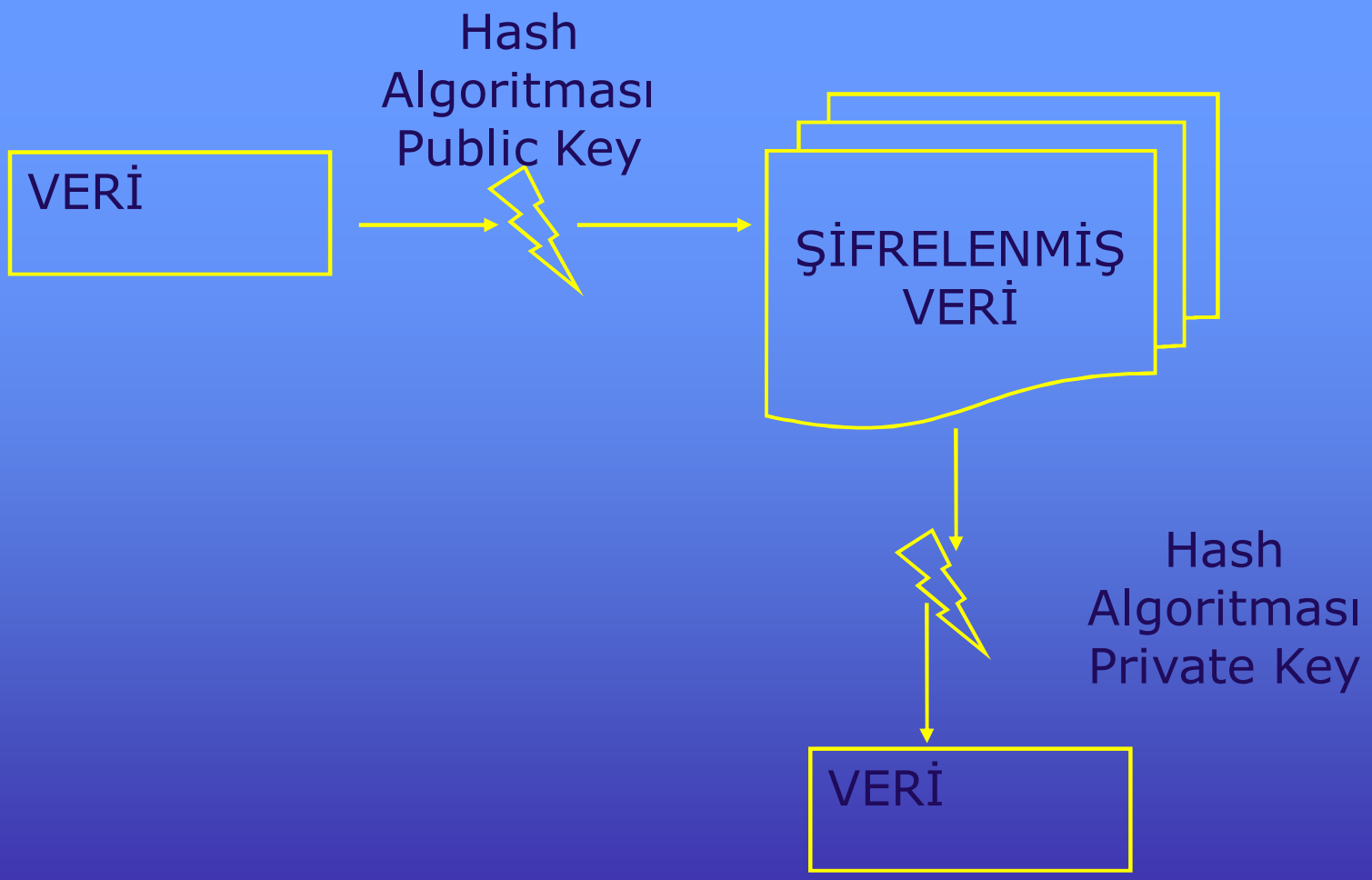
x : Açık metin e : Açık anahtar

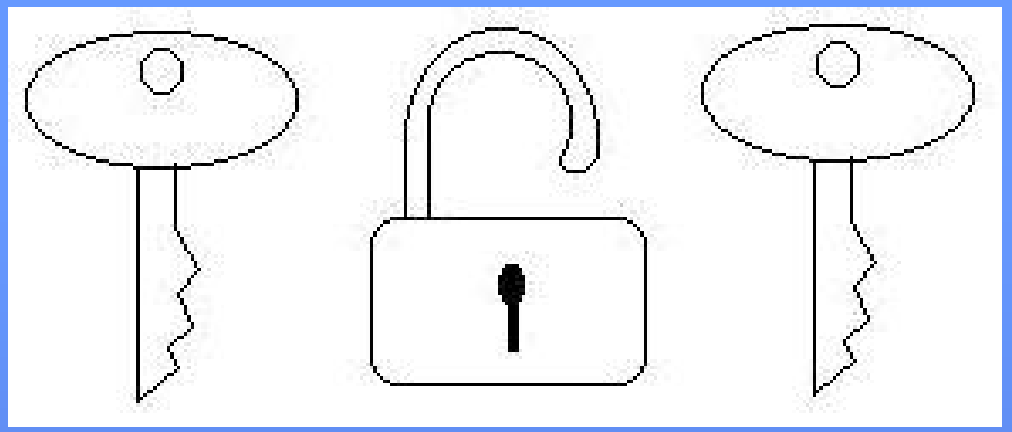
y : Şifreli metin d : Gizli anahtar

n : Açık modül p,q : Gizli asal sayılar

1- İki asal sayı seçilir (p,q)
2- Açık modül hesaplanır. (n = p*q)
3- Anahtar için ara değişken hesaplanır. (z = [p-1] * [q-1])
4- Açık anahtar hesaplanır. (e < z) ve gcd (z,e) = 1
5- Gizli anahtar hesaplanır. (d *e) mod z = 1

RSA


Hash
Algoritması
Public Key
VERİ
ŞİFRELENMİŞ
VERİ
Hash
Algoritması
Private Key
VERİ



P G P

(PRETTY GOOD PRIVACY)

PGP Nedir ?

PGP, yerine koyma ve kaydırma olarak çevirme çalıştığımız her iki kriptografik yöntemi de kullanan Halka Açık Anahtarla Şifreleme (Public Key Encryption) sistemidir.

Halka Açık Anahtar sisteminin en büyük avantajı, anahtarların alıcı ve verici arasında değiş tokuşu için güvenli bir kanala ihtiyaç duymamasıdır.

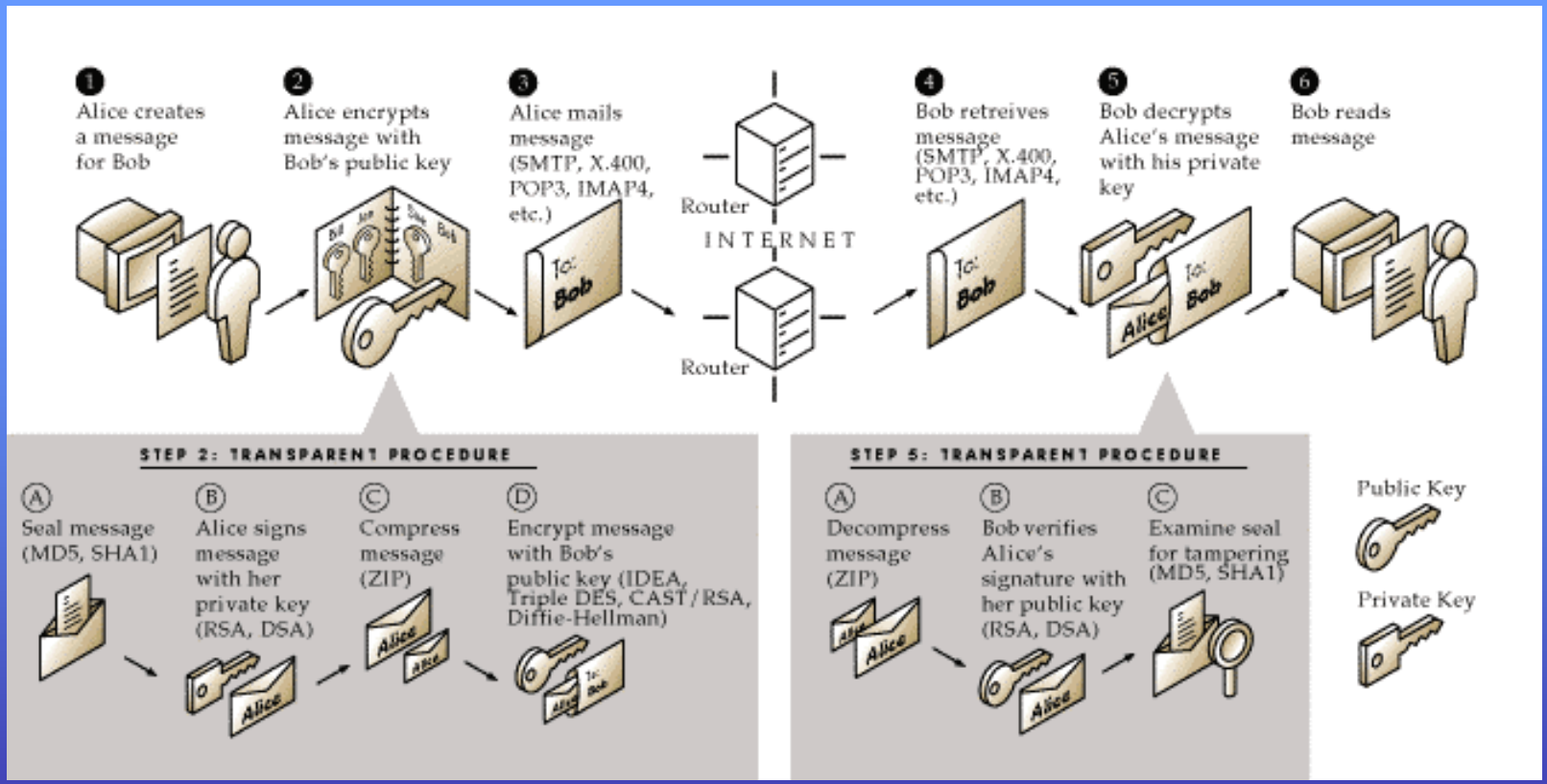
Bununla birlikte, bir kez kapatılan veya şifrelenen dosya,ancak ve ancak alıcısının özel anahtarı ile açılabilmekte veya deşifre edilebilmektedir.

PGP Nedir ?

Kişiye Özel Anahtar (Secret Key) : PGP tarafından "Passphrase" ile şifrelenir ve secring.skr dosyasında saklanır. Kişiye Özel Anahtar ile mesajlar şifrelenir, deşifrelenir veya dijital imza eklenebilir.

Halka Açık Anahtar (Public Key) : Gönderilen mesajı alacak kişinin halka açık anahtarı ile şifreleme işlemi ve alınan mesajın özgünlüğü dijital imzasından yararlanılarak kontrol edilir.

PGP ÇALIŞMA STİLİ



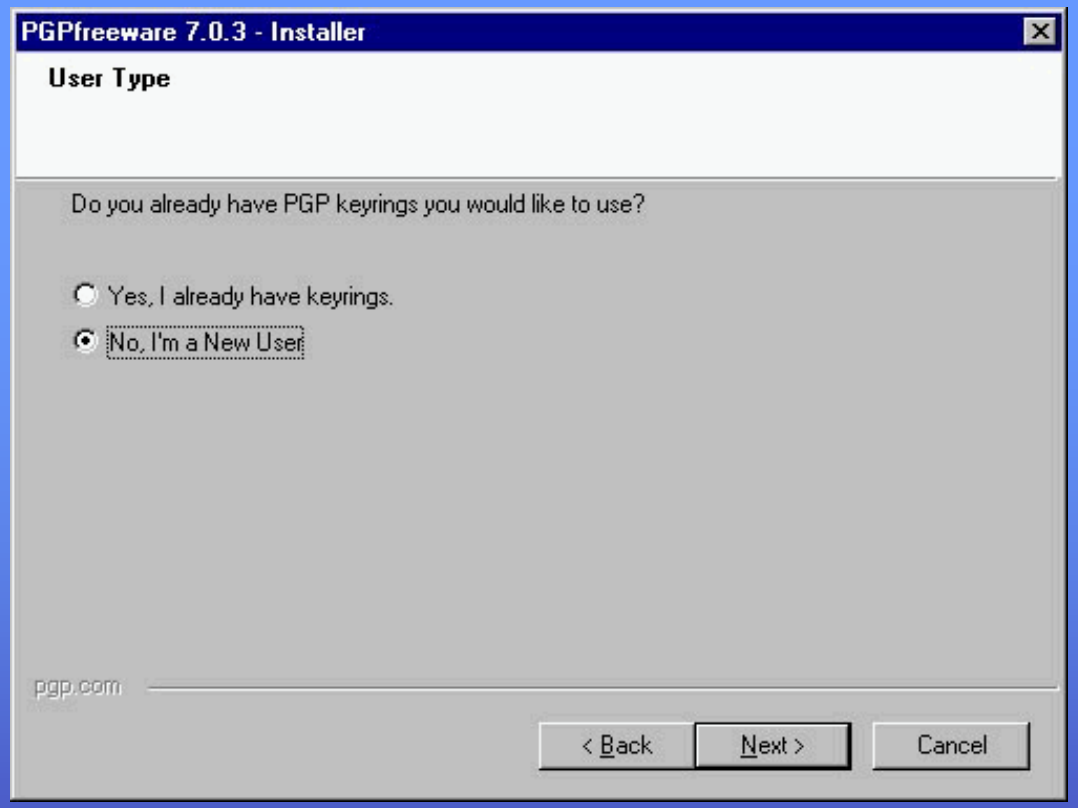
PGP YAPISI

PGP, halka açık anahtarın üretilmesi amacıyla RSA algoritmasından yararlanıyor. Dijital imza ile oluşturulan kontrol verileri RSA ile şifrelenmektedir.

Böylece güvenlik sağlanmış hem de zamandan kazanılmış olunuyor. Bütün metnin RSA ile şifrelenmesi çok zaman alacağından PGP bu amaçla IDEA yöntemini kullanıyor. IDEA ile şifreleme, aynı anahtarın birden fazla kullanılmaması halinde güvenlidir.

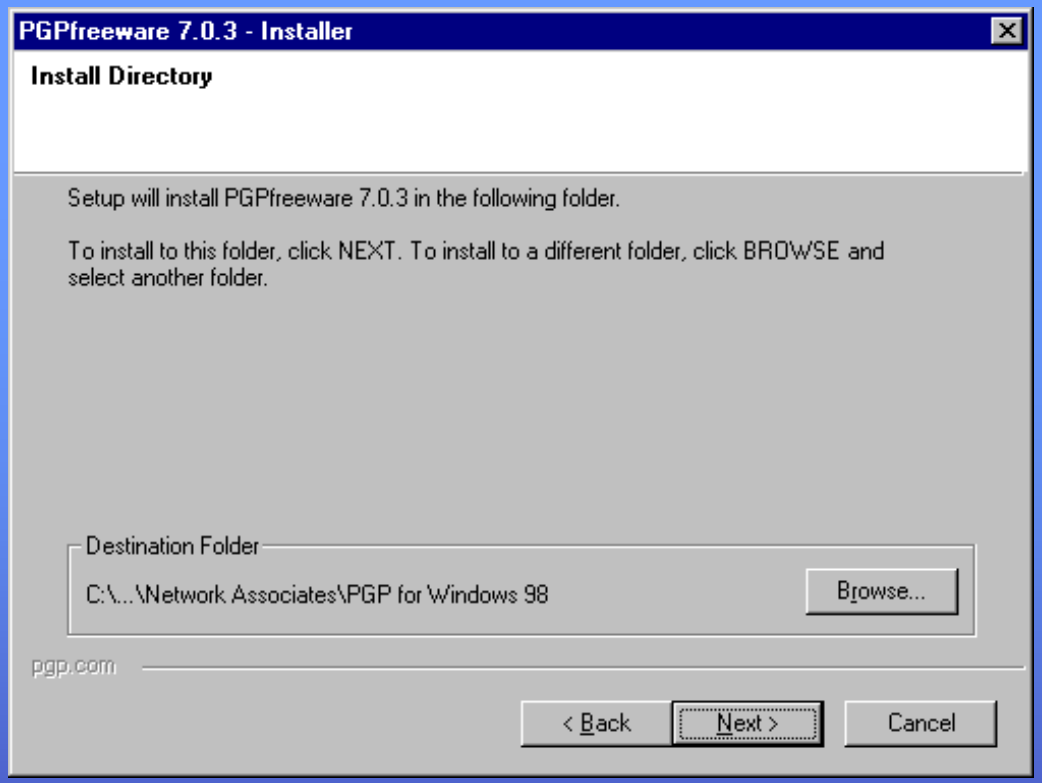
Bir çok kullanıcıya oldukça karmaşık gelebilecek bütün bu işlemlerin PGP tarafından tamamen otomatik olarak arka planda gerçekleştirildiğini ve kullanıcının sıkıştırma, bir defalık anahtar vs ile tek tek uğraşmasına gerek yoktur.

PGP KURULUMU



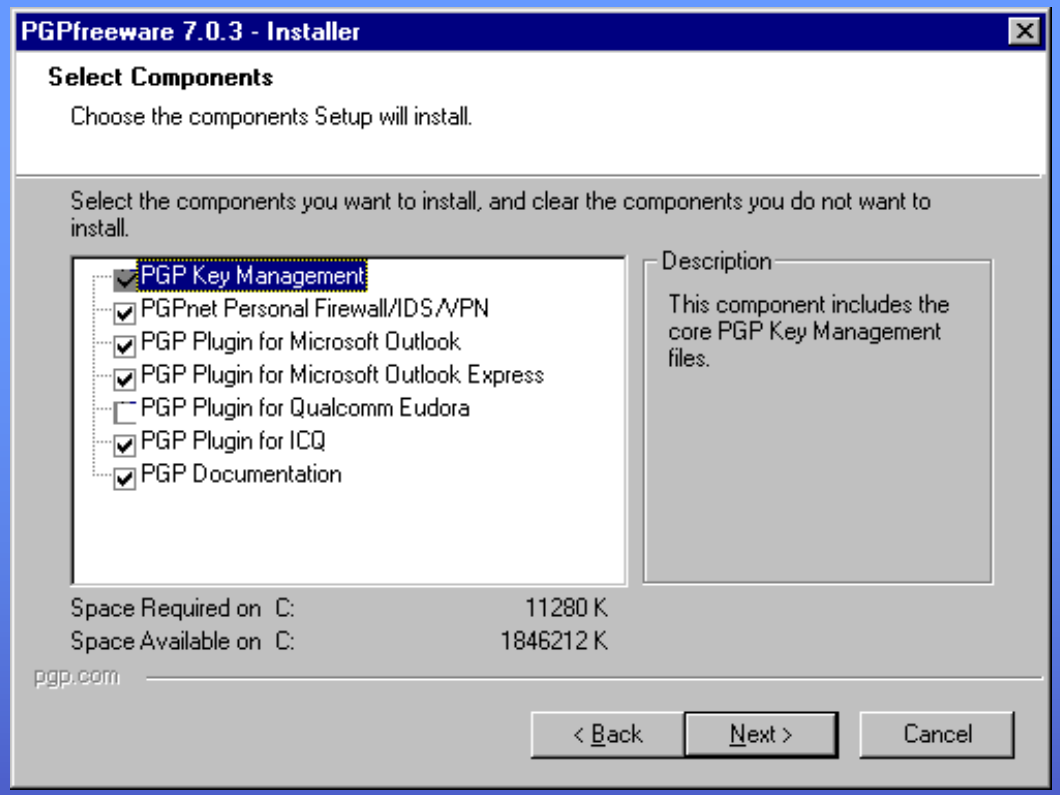
PGP Freeware 7.0.3 için yeni bir kurulum ya da yeni bir kullanıcı eklemedir.

PGP KURULUMU



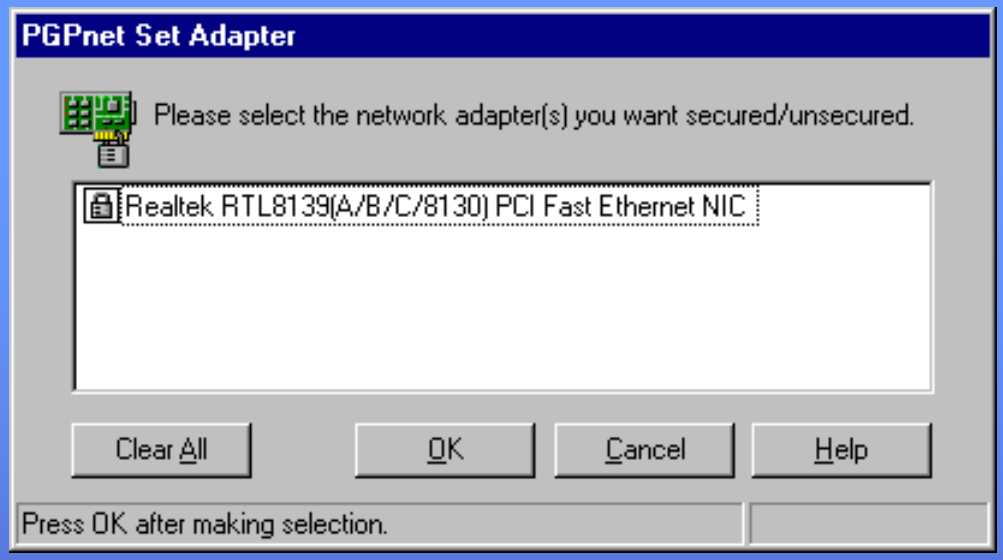
PGP kurulumu için gerekli dizinin seçilmesi ile kuruluma devam ederiz.

PGP KURULUMU



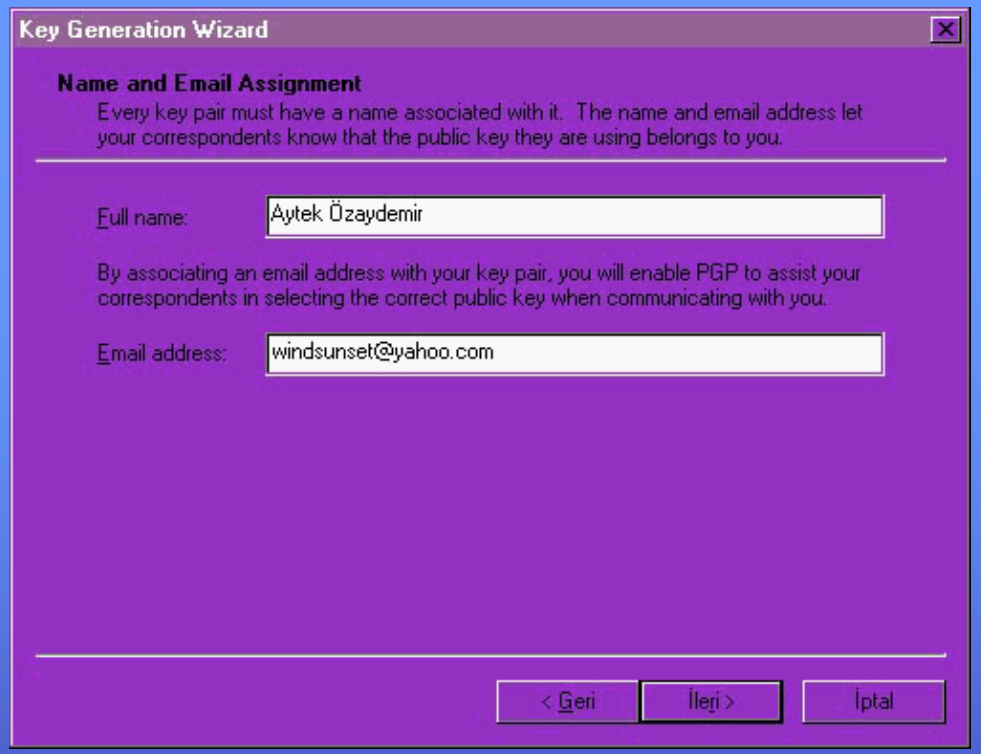
Bu pencerede PGP'yi diğer programlarla daha rahat kullanılmasını sağlayacak destek yazılımlarının yüklenmesi için, listeden bilgisayarda yüklü olan programlar'ın sol tarafındaki kutu işaretlenir.

PGP KURULUMU



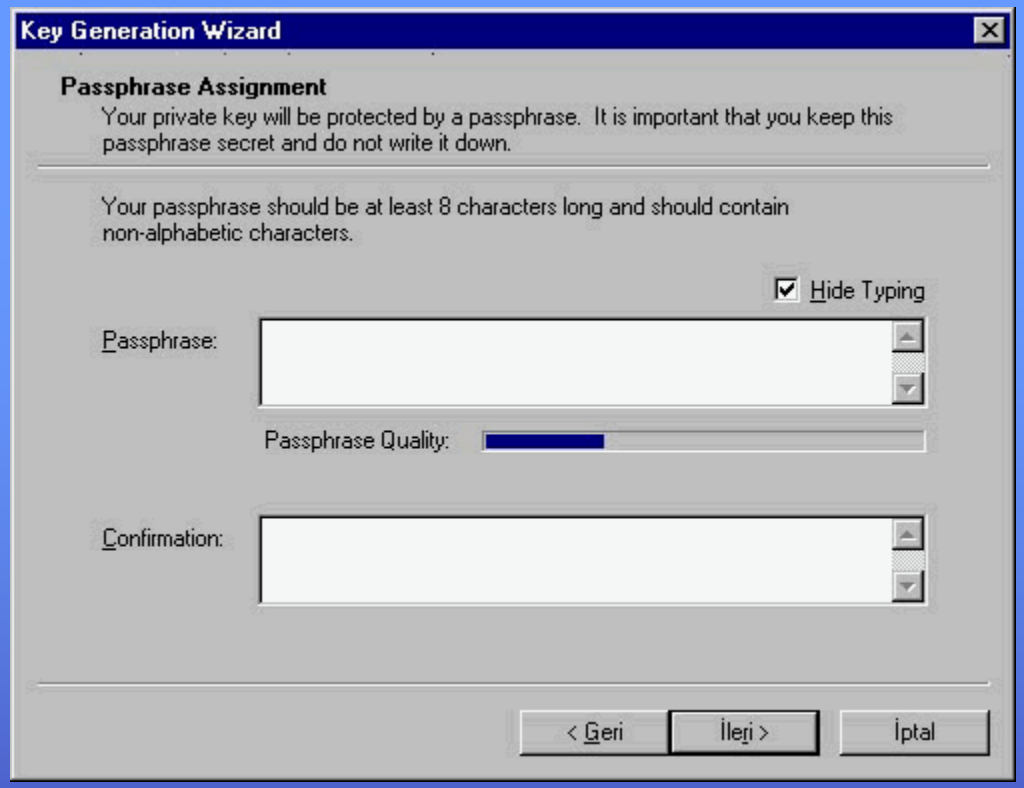
Son olarak PGP'nin güvenlik altına alması istenen ağ cihazları solundaki kutuya tıklanarak seçilir.

PGP KURULUMU



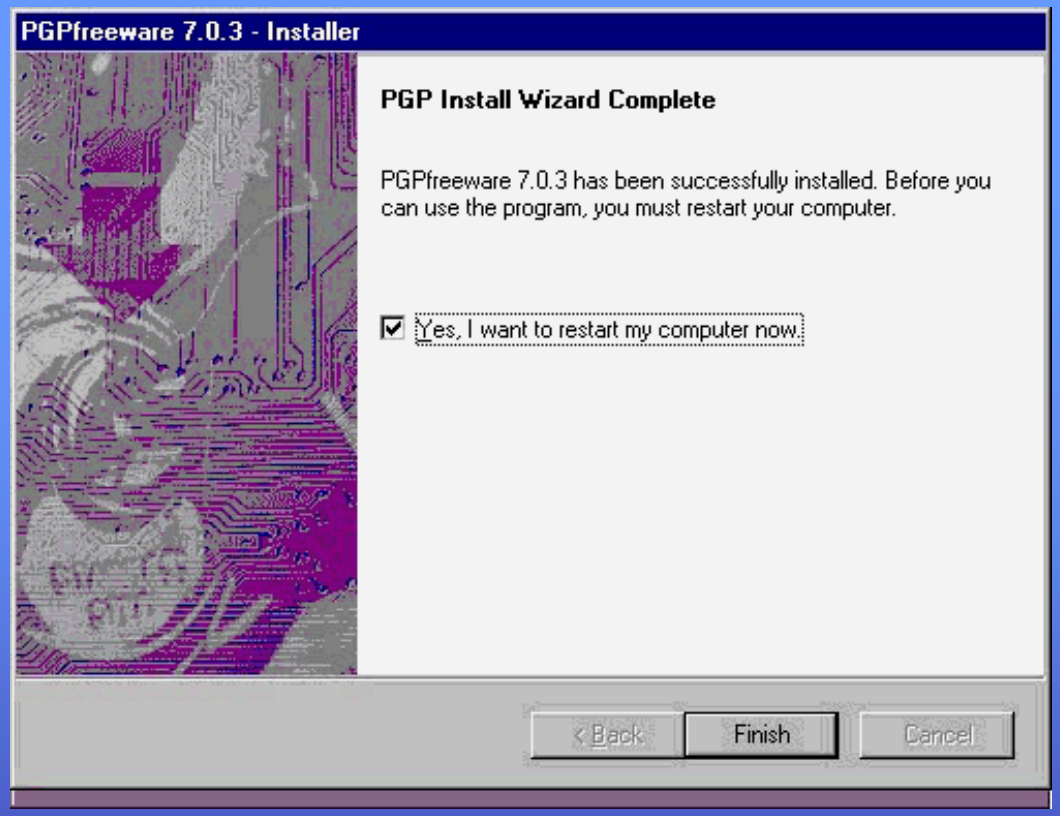
Gerçek ad ve e-mail adresinizi yazmanızla ileride başkalarının public key tanınmasına yardımcı olur.

PGP KURULUMU



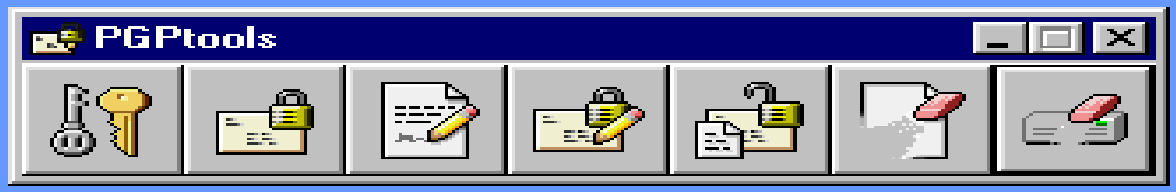
Passphrase kelimenizi yazarsınız.En az 8 karakterli olması ve içinde sayısal değerlerin bulunmasına dikkat edilmelidir.

PGP KURULUMU



PGP kurulumunu bilgisayarı yeniden başlatarak bitirebilirsiniz.

PGP KULLANIMI



İmzalama : PGP' de imzalama işlemi bir yazının veya dosyanın gerçekten sizden geldiğini doğrulamak için kullanılır.

Dosya İmzalama : Internet'te kurulum programları içine Trojan yerleştiren araçlar var. Normal yazıyı imzalamada olduğu gibi bir dosyayı imzaladıktan sonra dosyada değil tek bir byte bir bit değişse dahi imzanın geçersiz olduğu ve dosyanın imzalandıktan sonra değiştirildiği gösterilir. Dosya imzası dosya içinde olabileceği gibi dosya dışında .sig uzantılı ayrı bir dosya şeklinde olabilir.

PGP KULLANIMI

Otomatik Genel Anahtar Alma : Genel anahtarı elinizde olmayan biri size şifreli mesaj veya dosya gönderirse ve o kişinin anahtarını almak isterseniz PGP otomatik olarak sizin yerinize o anahtarı sunucuda arar ve getirir. Bu işlemi PGP' ye yaptırmak için **Options->Servers** sekmesinde "Verification" kutusunu işaretli hale getirin.

Ayrıca bu işlemi PGPKeys aracında **Server->Search** menüsünde kişinin adı, email adresi, id numarası gibi özelliklerini aratarak kendiniz de yapabilirsiniz.

PGP KULLANIMI

Alt Anahtar : Asıl anahtarın taşıdığı diğer imzaları ve imzalama yetkisini kaybetmeden birden fazla anahtar oluşturulmasıdır.

FingerPrint : PGP'de istediğiniz sayıda ve biçimde anahtar oluşturup kullanabilirsiniz. Bu anahtarların isim, e-mail adresi, anahtar türü ve boyutu, şifre gibi özellikleri aynı olabilir. Farklı anahtarların Key ID özelliği aynı olma olasılığı vardır fakat parmak izi dediğimiz Fingerprint'in farklı anahtarlarda aynı olması matematiksel olarak epsilon kadar düşük bir ihtimaldir.

DİJİTAL GÜVENLİK SİSTEMLERİ VE PGP

"Hiçbir insan zekası yoktur ki, doğru yöntemi kullanan başka bir insan zekasının çözemeyeceği bir şifre yaratabilsin."

Poe, Edgar, Alan

KATKILARINDAN DOLAYI

Sayın Prof. Doç. Dr. Mehmet TEKTAŞ ‘a
ve Tahsin ERTAN ‘a
Teşekkürü Borç Biliriz.....