GNUPG

GnuPG is the GNU project's complete and free implementation of the OpenPGP standard as defined by RFC4880 (http://www.gnupg.org/)

GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories.

GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. Version 2 of GnuPG also provides support for S/MIME.

Electronic Mail Security

- GNU Privacy Guard (GnuPG)
  - a GPL Licensed alternative to the PGP suite of cryptographic software.
  - compliant with RFC 4880, which is the current IETF standards track specification of OpenPGP.
  - Current versions of PGP are interoperable with GnuPG and other OpenPGP-compliant systems.
  - a part of the Free Software Foundation's GNU software project, and has received major funding from the German government

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

GnuPG Demo

- **Creating GPG Keys**

  http://fedoraproject.org/wiki/Creating_GPG_Keys

  GnuPG Commands – Examples

  http://www.spywarewarrior.com/uiuc/gpg/gpg-com-4.htm

  Checking integrity of file downloaded

  Examine the following page to study md5sum or sha1sum:

  http://linuxsagas.digitaleagle.net/2012/05/11/checking-files-with-md5sum-or-sha1sum/

- **Origin and integrity of the file can be ensured by verifying its signature**

  Details can be found from

  https://www.torproject.org/docs/verifying-signatures.html.en

  One can perform these operations on a file and its signature downloaded from

  https://www.torproject.org/download/download-easy.html.en

Gnupg Örnekler

http://www.gnupg.org/gph/en/manual/x110.html

- GPG anahtarı (key) oluşturma:

  gpg --gen-key

- GPG Anahtarın basitleştirilmiş parmak izini görüntülemek

  gpg --fingerprint jqdoe@example.com

- GPG anahtarını, kamu anahtar sunucusuna (key server) aktarmak için

  gpg --keyserver hkp://subkeys.pgp.net --send-key KEYNAME

  Burada KEYNAME, anahtarın kimlik numarası (Başına 0x eklenecek; bu numarayı öğrenmek için önceki komudun çıktısına bakmak yeterli).

- Public ring (açık halka) üzerindeki anahtarları listelemek için

  gpg --list-keys

- Açık halka üzerine yeni bir açık anahtar (örneğin arkadaşınıza ait) eklemek için

- ***gpg --import blake.gpg***

Gnupg Örnekler

- GPG anahtarı ile doc dosyası için imza oluşturmak:

  gpg --output doc.sig --sign doc

- GPG anahtarı ile doc dosyasının imzasını doğrulamak:

  gpg --output doc --decrypt doc.sig

- GPG şifreleme işlemi:

  gpg --output doc.gpg --encrypt --recipient blake@cyb.org doc

  Burada alıcı blake@cyb.org ***; doc*** dosyası şifrelenecek; simetrik şifreleme için bir gizli anahtar belirlenecek ve bu gizli, oturuma özel anahtar, alıcının açık anahtarı ile şifrelenecek. Bu gizli anahtar ile dosya şifrelenecek.

- GPG deşifreleme işlemi (***blake@cyb.org*** tarafından yapılacak)

  gpg --output doc --decrypt doc.gpg

  blake@cyb.org, kapalı anahtarını koruyan passphrase anahtarını girecek ve deşifreleme sonucu ortaya çıkan kapalı anahtar ile yapılan deşifreleme işleminde oturum anahtarı ortaya çıkacak. Bu anahtar ile ***doc***.***gpg*** dosyası deşifrelenecek.

- Sadece simetrik şifreleme için izleyen komut çalıştırılıp, passphrase anahtarı sağlanacak. Bu anahtardan gizli anahtar üretilecek. Bu yöntem ağ üzerinden paylaşılmayacak, sistem üzerindeki dosyaları şifrelemek için kullanılabilir.

  gpg --output doc.gpg --symmetric doc

Enigmail: Thunderbird Addon

- Enigmail is a security extension to Mozilla Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

  Sending and receiving encrypted and digitally signed email is simple using Enigmail.

  https://www.enigmail.net/home/index.php

- Screenshoots

https://www.enigmail.net/documentation/screenshots.php

- Installation and Usage

https://addons.mozilla.org/en-US/thunderbird/addon/enigmail/

http://fedoraproject.org/wiki/Using_GPG_with_Thunderbird

Openssl

- OpenSSL is an open-source implementation of the SSL and TLS protocols.
- The core library, written in the C programming language, implements the basic cryptographic functions and provides various utility functions.
- Wrappers (for Java etc.) allowing the use of the OpenSSL library in a variety of computer languages are available.
- Versions are available for most Unix-like operating systems (including Solaris, Linux, Mac OS X and the various open source BSD operating systems), OpenVMS and Microsoft Windows.
- OpenSSL supports a number of different cryptographic algorithms:
  - **Ciphers**

    AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, Triple DES, GOST 28147-89
  - **Cryptographic hash functions**

    MD5, MD2, SHA-1, SHA-2, RIPEMD-160, MDC-2, GOST R 34.11-94
  - **Public-key cryptography**

    RSA, DSA, Diffie–Hellman key exchange, Elliptic curve, GOST R 34.10-2001

(Perfect forward secrecy is supported using elliptic curve Diffie-Hellman since version 1.0.)

Openssl Örnekleri

http://www.madboa.com/geek/openssl/

- ***rapor.pdf*** dosyasının SHA-1 özet fonksiyonu ile parmakizini/özetini oluşturmak:

  openssl dgst -sha1 rapor.pdf

- ***http://ftp.gnu.org/gnu/anubis/*** adresinden **anubis-4.0.tar.gz** dosyasını indirip, hash değerini hesaplayalım ve sha1sum dosyasındaki değer ile karşılaştıralım:

  openssl dgst -sha1 **anubis-4.0.tar.gz**

- Openssl in desteklediği algoritmaların listesi için:

  openssl ciphers -v

- Algoritmaların çalışma sürelerini test için. Örneğin AES testi:

  openssl speed aes

- RSA 2048-bit anahtar anahtarını yaratıp, ***anahtarim.pem*** dosyasına yerleştirmek için

  openssl genrsa -out anahtarim.pem 2048

Openssl Örnekleri

http://www.madboa.com/geek/openssl/

- ***rapor.pdf*** dosyasını AES 256-bit CBC blok mod işlemi ile şifrelemek için

  openssl enc -aes-256-cbc -in rapor.pdf -out rapor.pdf.enc

- ***rapor.pdf.enc*** dosyasını, önceki örnekte kullanılan gizli anahtar ile AES 256-bit CBC blok mod işlemi ile deşifrelemek için

  openssl enc -d -aes-256-cbc -in rapor.pdf.enc -out rapor.pdf

- RSA 2048-bit anahtar anahtarını yaratıp, ***anahtarım.pem*** dosyasına yerleştirmek için

  openssl genrsa -out anahtarim.pem 2048

- RSA 2048-bit açık anahtar anahtarını oluşturmak için

  openssl rsa -in anahtarım.pem -pubout

- Bu anahtarı dosyaya aktarmak için

  openssl rsa -in anahtarım.pem -pubout > acik.pem

Openssl Örnekleri

http://www.madboa.com/geek/openssl/

- ***rapor.txt*** dosyasını imzalamak için

  openssl dgst -sha1 -sign anahtarim.pem -out rapor.txt.sha1 rapor.txt

- ***rapor.txt*** dosyasını imzasını doğrulamak için

  openssl dgst -sha1   -verify acik.pem -signature rapor.txt.sha1 rapor.txt

- 3. güvenli şahış (Türkiye'de nitelik e-imza servis sağlayıcıları Turktrust, E-Güven, E-Tuğra ve Tübitak Kamu SM veya dünya çapında firmalar Verisign, Globalsign vb.) tarafından verilen ve imzalanan sertifikalar yerine kişinin bir web alanı için kendi kendini imzalayan sertifika oluşturma yöntemi: (How to create a self-signed SSL Certificate …)

  http://www.akadia.com/services/ssh_test_certificate.html