

Welcome to

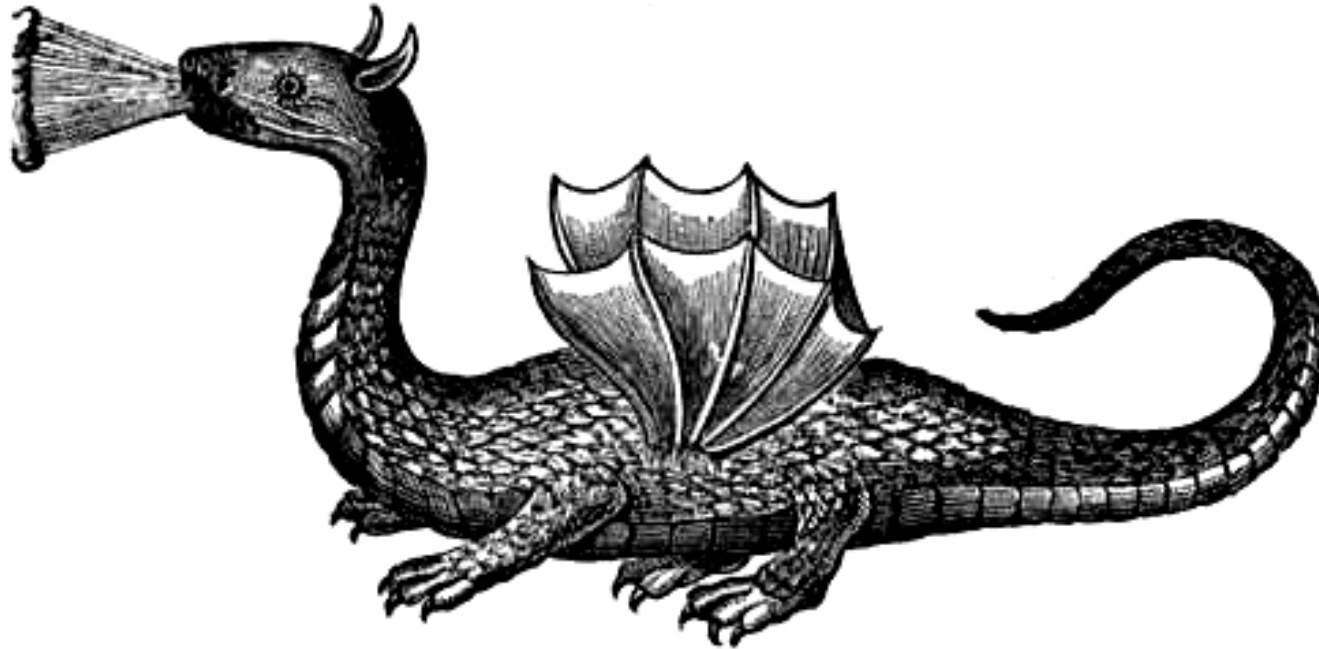
# Introduction PGP

Henrik Lund Kramshøj [hlik@kramse.org](mailto:hlik@kramse.org)



Cryptoparty PDF available [kramshoej@Github](https://github.com/kramshoej)

# Warning



This is just a taste of crypto - introduction

Dont feel secure until you have experience and understand the programs better.

BUT learn the tools before you need them

# PGP origins



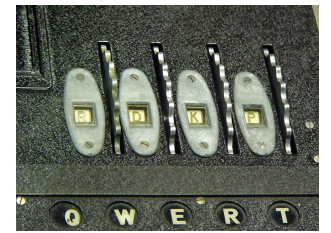
Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.[1]

... and dont forget:

Shortly after its release, PGP encryption found its way outside the United States, and in February 1993 Zimmermann became the formal target of a criminal investigation by the US Government for "munitions export without a license".

Source: [https://en.wikipedia.org/wiki/Pretty\\_Good\\_Privacy](https://en.wikipedia.org/wiki/Pretty_Good_Privacy)

# Definitions: PGP, GPG and OpenPGP



**PGP** and similar software follow the **OpenPGP standard (RFC 4880)** for encrypting and decrypting data

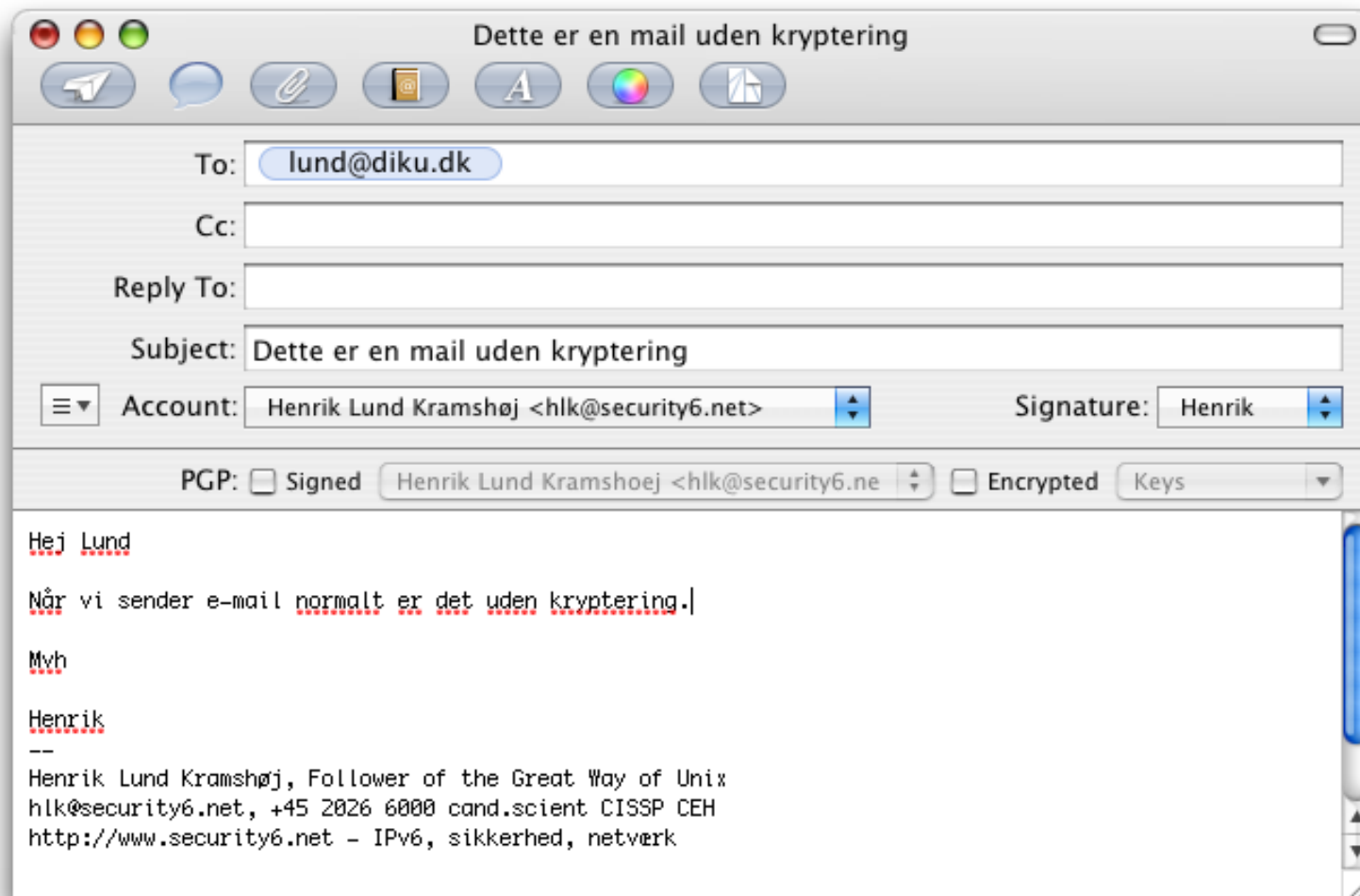
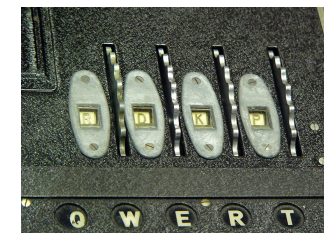
A popular compatible software is **GPG, Gnu Privacy Guard**

<https://gnupg.org/>

which is used in the GPG Suite for Mac OS X <https://gpgtools.org/>

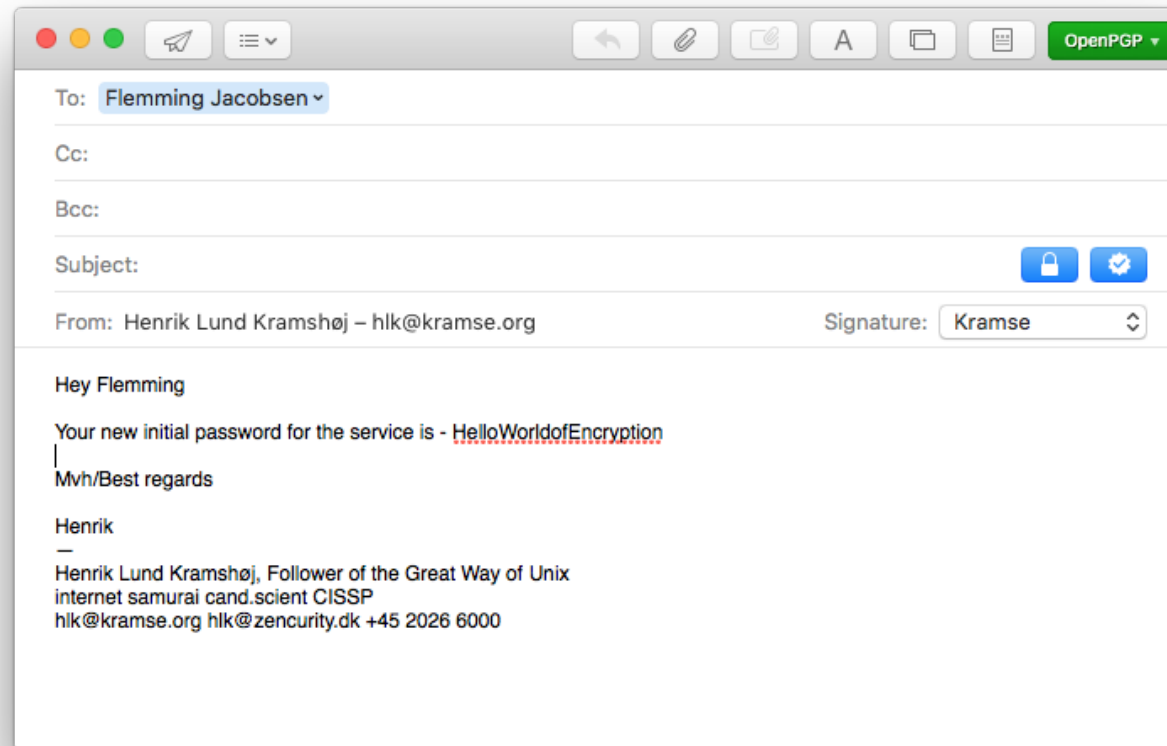
and Enigmail plugin for handling encrypted email in Thunderbird

# Email is insecure



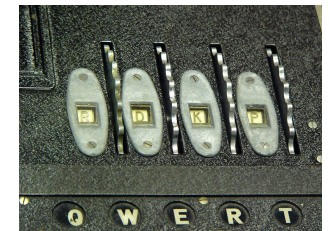
Email without encryption - is like a postcard

# Email with Encryption



Not harder to send encrypted

# Encrypted Email Source Data Sent



```
Source of
Content-Description: OpenPGP encrypted message
To: Flemming Jacobsen <fj@batmule.dk>

This is an OpenPGP/MIME encrypted message (RFC 2440 and 3156)
--Apple-Mail=_866E5C87-3EF1-461A-9D73-BDCE9C0E2E7A
Content-Transfer-Encoding: 7bit
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME Versions Identification

Version: 1

--Apple-Mail=_866E5C87-3EF1-461A-9D73-BDCE9C0E2E7A
Content-Transfer-Encoding: 7bit
Content-Disposition: inline;
    filename=encrypted.asc
Content-Type: application/octet-stream;
    name=encrypted.asc
Content-Description: OpenPGP encrypted message

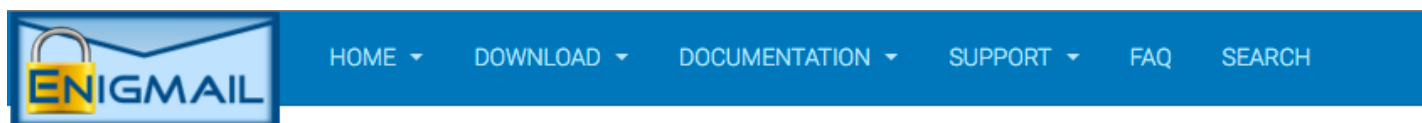
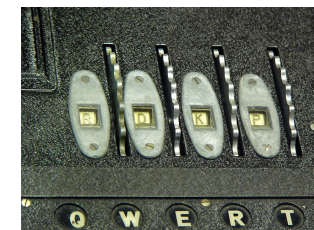
-----BEGIN PGP MESSAGE-----
Comment: GPGTools - http://gpgtools.org

hQIMA2dXkaUMkJaZAQ//aXzjPMGr89/1fc55Rbf1v0bjSw6IGgStEI4K8R20FNbP
0h0itcMCLXzEc/0LSRF4zrSpmUD0ihLFVEwUcFBjImTHCLeyni3MZpca1SkSWueX
nXqRLMG8fGUVtnw9MhU/vHdwqkTG3PKS9daK10tpJff2lbWRLCxGSPFD891gMi
y2SEyxy6Rh4xNE3UEU0LSUi0m0EBVRXMPPsIJARM55/YgyPAmEPQ8mjNnBwcEzEb
KJQWa/KZqQzM0Sr0ZkS77u0j5pEz2KcgUa/Z/S2NNl3n0LIic31fonrpSSUe876F
RijqPrR0VDJ6pIwd4TDCftRHIVMl09f6o73Ppqpd42/c+J61pxb/g3mexx30eps3
KLNL93Ag63wCtyj52VmWclg/ktixlPwqTGXA/nFQXSor8+3ye6zSnYXuoab6aqG5
ZvLVxsoBBrx2vRiGWHNMFLmteMw0BHmA+Klixlms0k4AwTd+20K50q0lNs0CMb+
ARL1osrbi9RaID0/h1y545FIevqr9cR9Zi1TyGysq0zKLJWsdHda1cvY9+bvdsLy
+swdnfPX/yQcy+Un9kS610sAJsmyetFckmaDa49WqbpwTpemim0W+GbC0mHyqN/n
P5C6u7T22oqf9BE0Cr9BPW3IpyVlaZVKjgxfL2u8Na5BnreSl9iG5/3ppkeSpxmF
AgwDBXNdeGcujkUBD/9Hfnt5W+zrFU+PiTM2VNC52oNtk7ntBvs9AfY3g4qrU+bK
z072Z/7vhJP7VVZE3sGlyKPHm37at1zW49R8C7HjkForWrZpAifR78NPisvPiXkS
62V5/ouTiqEcuEGcUNLi0h8GaoZY3fXo2Tmc90iaHudKseBY1x083Sxsxy8EwpsS
```

A secure encrypted Email cannot be opened by others



# Enigmail for Mozilla Thunderbird



## A simple interface for OpenPGP email security



### Why encrypt emails?

Do you want to send your digital letters as post cards? Probably not.

Sending unencrypted emails is like sending post cards – anyone and any system that process your mails can read its content. If you encrypt your emails, you put your message into an envelope that only the recipient of the email can open.

### What is Enigmail?

Enigmail is a seamlessly integrated security add-on for [Mozilla Thunderbird](#). It allows you to use OpenPGP to encrypt and digitally sign your emails and to decrypt and verify messages you receive.

Enigmail is [free software](#). It can be freely used, modified and distributed under the terms of the [Mozilla Public License](#).

### Start encrypting your emails today!

[Download Enigmail Now](#)

[Version 1.9.1](#) - [OpenPGP Signature](#) - [Previous Releases](#)

Source: <https://www.enigmail.net>