Enigmail

Enigmail is a free Thunderbird extension, to encrypt and sign emails.

Cryptography and Signature

Enigmail works with **asymmetric cryptography**. Two keys are used (one public and one private). There is also symmetric cryptography where you just use one key, but which needs to be sent to the recipient via a secure channel, so that she can decrypt the message.
In asymmetric cryptography a **key pair** is used. Public and private key are created together at the same time using a special algorithm and they are strictly connected to each other. A message is encrypted with a public key and can only be decrypted with the companion private key. Similarly, a message is digitally signed with a private key and can only be verified with the companion public key.[1]
The public key can be thought of as an envelope. This envelope is only handed out by you. Letters you receive in this envelope will only ever be accessible to you, because only you own the private key to unlock it.[2]

Web of Trust vs. Public Key Infrastructure (PKI)

The Public Key Infrastructure system is hierarchical. Digital certificates are verified by Certifying Authorities whose role is to be a trusted third party that issues digital certificate. The trust model is based on a number of top instances (Certifying Authorities) who "all" parties trust.
Web of Trust is a decentralized alternative to the standard PKI system. In contrast to the latter, the Web of Trust works based on trust between users. Here, every user can certify other users public key.[3]
For example: Alice signs the key of Bob and, by that, implicitly trusts signatures created by Bob. Bob signs the key of Carl. Therefore Alice considers Carl's key as valid.[4]

Confidentiality, Integrity and Authenticity

The three terms stand for the classic security goals in IT. **Confidentiality** of information is protecting it from disclosure to unauthorized parties. **Integrity** refers to protecting information from being modified by unauthorized parties[5] and the **Authenticity** means to ensure a signature is indeed from author claiming to have created it.[6]

Inline PGP vs. PGP/MIME

With inline PGP all attachments are individually encrypted, while in PGP / MIME, the entire message is encrypted. PGP/MIME is the further development of inline PGP, thats why older versions of e-mail clients and apps on mobile clients sometimes have troubles to correctly displaying PGP/MIME encrypted messages.[7] To deal with that, Enigmail allows you to set the format explicitly e.g. to inline PGP if you can't communicate otherwise.[8]

---

1 Enigmail Wiki; url: https://enigmail.wiki/ [02.01.2015]
2 explanation from Ralph Wozelka [27.01.2016]
3 Eyas Al-Hajery: Trust Model in PGP and X.509 Standard PKI; url: https://www.giac.org/paper/gsec/625/trust-model-pgp-x509-standard-pki/101441 [02.01.2015]
4 https://de.wikipedia.org/wiki/Web_of_Trust [02.01.2015]
5 Terry Chia: Confidentiality, Integrity, Availability. The three components of the CIA Triad; IT Security Community Blog; url: http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/ [02.01.2015]
6 explanation from Ralph Wozelka [27.01.2016]
7 Stefan Deser, Rolf Meinecke u.a.: Die CryptoCD; http://www.vorratsdatenspeicherung.de/CD/CD_1.0/cryptocd/doku/macos/pgp_mime/pgp_mime.html [02.01.2015]
8 explanation from Ralph Wozelka [27.01.2016]