

Pretty Good Privacy

Mailverschlüsselung mit



Geschichte

- PGP von Phil Zimmermann 1991 entwickelt
- 1995 Veröffentlichung des Quellcodes als Buch
- 1998 Standardisierung
- danach Entwicklung von GnuPG und vielen weiteren Tools zum Verschlüsseln und Entschlüsseln

Anwendungen

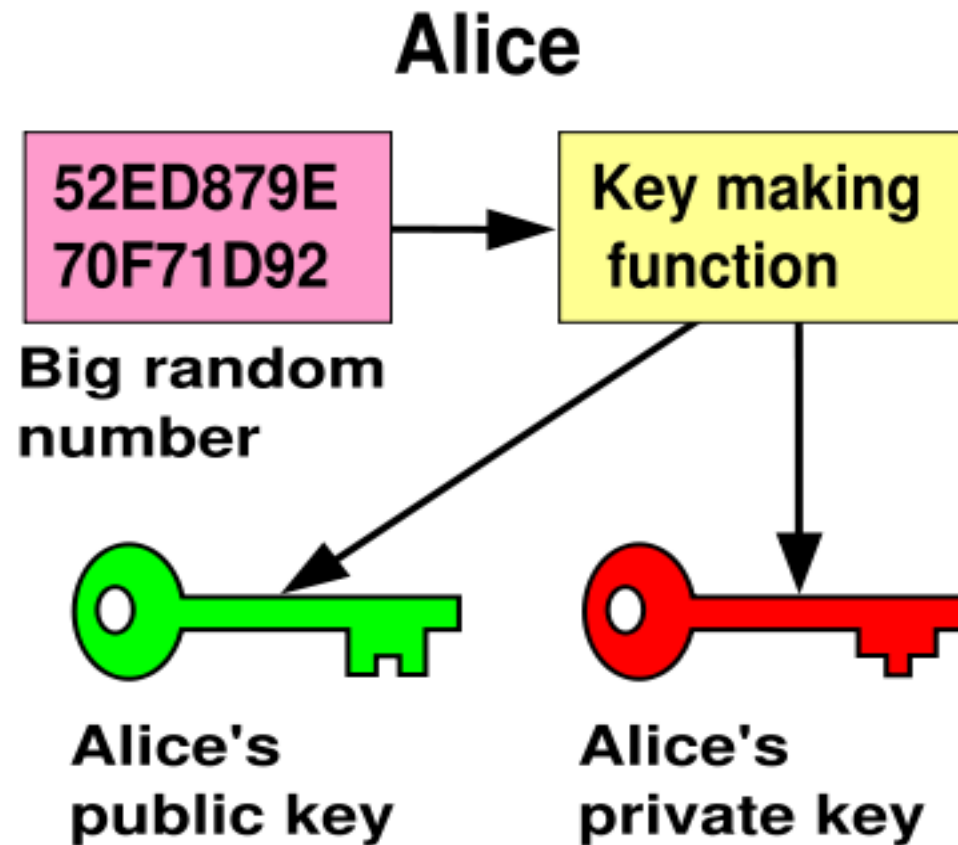
- Verschlüsseln und Signieren von:
 - Emails
 - Dateien
 - Chat

Verschlüsselung

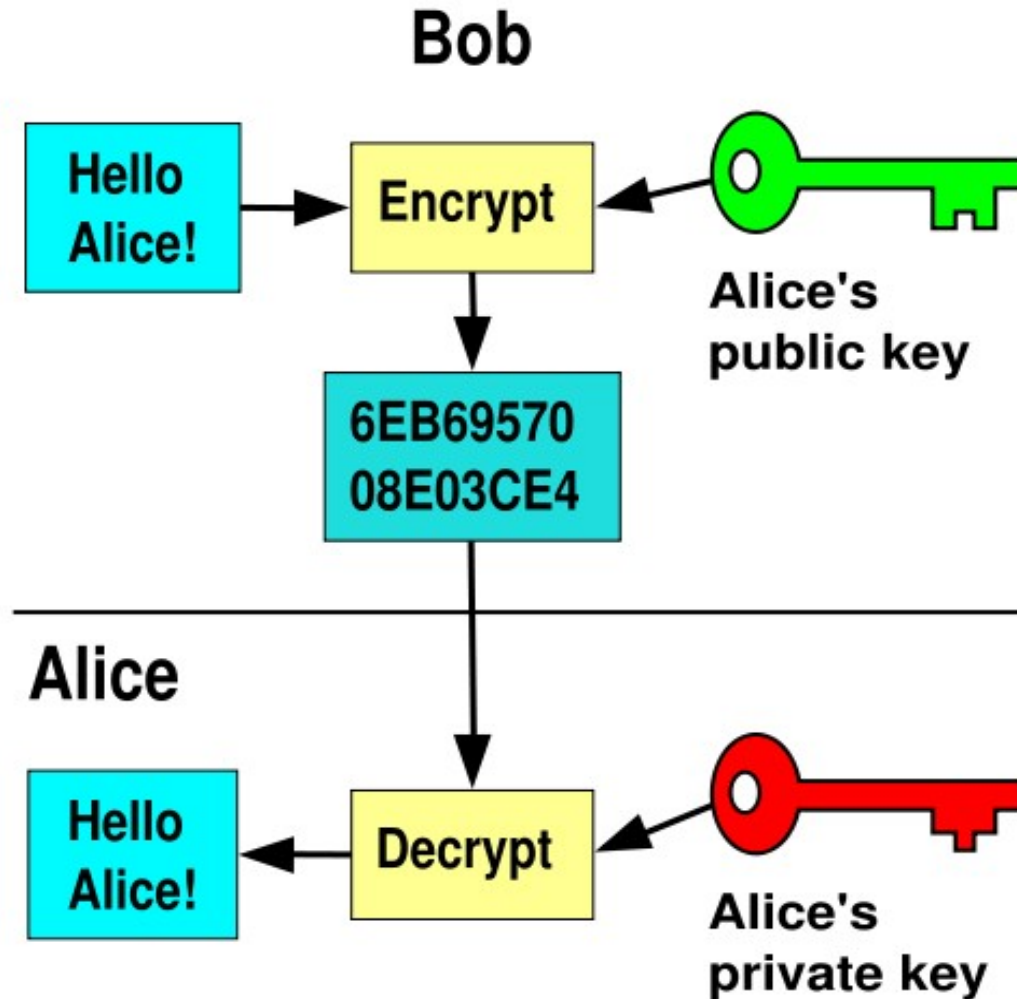
- hybrides Kryptosystem
- asymmetrische und symmetrische Verschlüsselung
- Algorithmen aus den 70er Jahren
- public/private Key



Schlüssel generieren



Ver- & Entschlüsselung public / private Key



Signieren

- Prüfsumme des Inhalts wird mit privatem Schlüssel verschlüsselt
- Entschlüsselung mit öffentlichem Schlüssel
- Vergleich der Prüfsumme mit eigener

Echtheit der Schlüssel

- Echtheit der Schlüssel muss überprüft werden (Key-Signing-Partys)
- Öffentliche Schlüssel können signiert werden (“web of trust”)

Software

- Viele Mailclients mit Plugin (Thunderbird,....)
- Schlüsselverwaltungssoftware (Seahorse,...)
- Texteditor (gedit,...)

Weg zum verschlüsselten Mail

- GnuPG installieren
- evtl. zusätzliche Software installieren (Schlüsselverwaltung, Plugins für Mailprogramme, Filebrowser, etc..)
- Eigenes Schlüsselpaar generieren
- öffentlichen Schlüssel verteilen
- andere öffentliche Schlüssel “signen”
- Mail schreiben und mit öffentlichem Schlüssel des Empfängers verschlüsseln