LU05.A08 - Asymmetrisch Ver- und Entschlüsseln

Lernziele

- Sie können ein asymmetrisches Schlüsselpaar generieren und verteilen.
- Sie können von Ihnen erstellte Nachrichten bzw. Medien korrekt verschlüsseln und versenden.
- Sie können an Sie gesendete Nachrichten bzw. Medien korrekt entschlüsseln.

Rahmenbedingungen

- **Zeitbudget:** 50 Minuten
- **Sozialform:** Gruppenarbeit zu 3-4 Personen
- **Hilfsmittel:**
  - Download-Link: GnuPGP-Download
- **Erwartetes Ergebnis:** Prozessbeschreibung inkl. Screenshot wie Nachrichten und Medien ver- und entschlüsselt worden sind, als PDF-Datei.

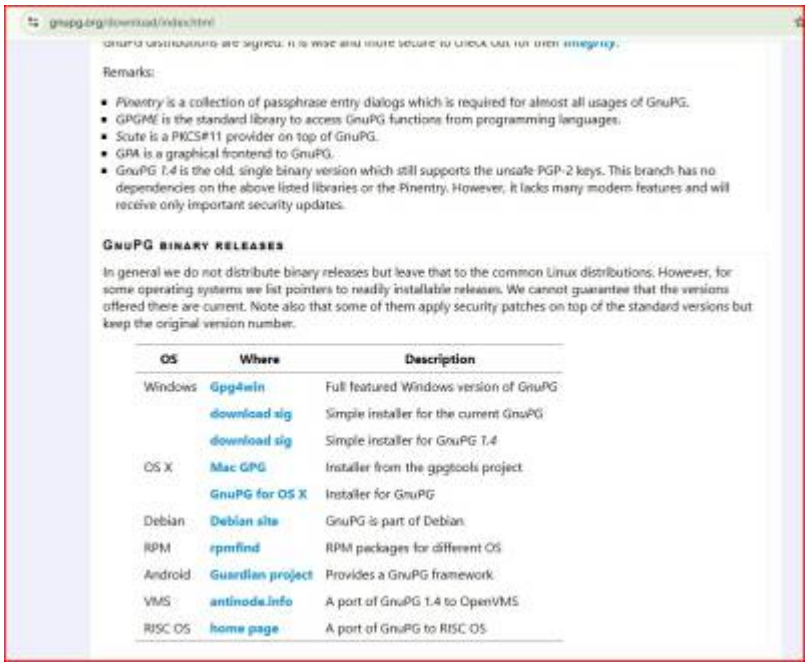
Ausgangslage

Die aktuellen Systeme wie Google oder WhatsApp bieten schon im Standard Verschlüsselungsmechanismen an, die das Lesen von Nachrichten von Unbefugten verunmöglichen sollen. Die vorliegende Aufgabe soll Ihnen den Prozessverlauf einer solchen **sicheren Kommunikation** verdeutlichen.

Arbeitsauftrag

Um Nachrichten verschlüsseln, und damit für Unberechtigte und unlesbar machen zu können, müssen wir ein Schlüsselpaar generieren. Hinweis: Es wird als *Best-Practise* angesehen diese zusätzlich zu sichern.

Vorarbeit: Gehen Sie auf die genannte Webseite, um die Installationsdatei zu finden, sie befindet sich ca. in der Mitte der Downloadseite. Laden Sie das für Ihren Computer passende Softwarepaket, wie beispielsweise *Gpg4win* oder *Mac GPG* von der GNU-Webseite und starten den Installationsprozess durch Doppelklick der Datei *gpg4win-4.4.1.exe*. Installieren Sie diese App.



Remarks:

- *Pinentry* is a collection of passphrase entry dialogs which is required for almost all usages of GnuPG.
- GPGME is the standard library to access GnuPG functions from programming languages.
- Scute is a PKCS#11 provider on top of GnuPG.
- GPA is a graphical frontend to GnuPG.
- GnuPG *1.4* is the old, single binary version which still supports the unsafe PGP-2 keys. This branch has no dependencies on the above listed libraries or the Pinentry. However, it lacks many modern features and will receive only important security updates.

GnuPG binary releases

In general we do not distribute binary releases but leave that to the common Linux distributions. However, for some operating systems we list pointers to readily installable releases. We cannot guarantee that the versions offered there are current. Note also that some of them apply security patches on top of the standard versions but keep the original version number.

OS	Where	Description
Windows	Gpg4win	Full featured Windows version of GnuPG
	download sig	Simple installer for the current GnuPG
	download sig	Simple installer for GnuPG *1.4*
OS X	Mac GPG	Installer from the gpgtools project
	GnuPG for OS X	Installer for GnuPG
Debian	Debian site	GnuPG is part of Debian
RPM	rpmfind	RPM packages for different OS
Android	Guardian project	Provides a GnuPG framework
VMS	antinode.info	A port of GnuPG 1.4 to OpenVMS
RISC OS	home page	A port of GnuPG to RISC OS

1. Erstellen Sie ein Schlüsselpaar und tauschen diese mit Ihren Peer-Parnern aus.
2. Verschlüsseln Sie Nachrichten und senden diese an Ihre Peerpartner. Diese sollen versuchen Ihre Nachricht zu entschlüsseln.
3. Jede Peer-Parner sollte mindestens eine Nachricht Ver- und entschlüsselt haben.
4. Notieren Sie Ihre Beobachtungen durch Beschreibungen und Screenshots.
5. Versuchen Sie nun auch Medien wie Bilder oder kleine Videos zu verschlüsseln, zu versenden und zu entschlüsseln.
6. Notieren abschliessend Ihr Fazit auf da. 1/4 Din A4 Seite. Beachten Sie, dass Ihre *Arbeitsprotokoll* einer aussen stehenden Person verständlich sein sollte.

Video-Tutorial für Installation und Anwendung

Videotutorial zur Installation und Anwendung
