

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:** 40 Minuten
- **Sozialform:** Gruppenarbeit zu 3-4 Personen
- **Hilfsmittel:**
 - Download-Link: [GnuPG-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

Vorarbeit

Laden Sie das für Ihren Computer passende Softwarepaket, wie beispielsweise *GnuPG* von der GNU-Webseite herunterunter herunter.

The screenshot shows a web browser window with the URL gnupg.org/download/index.html. At the top, there is a note: "GNUPG DISTRIBUTIONS ARE SIGNED. IT IS WISE AND MORE SECURE TO CHECK OUT FOR THEIR INTEGRITY." Below this, under "Remarks:", there is a list of several tools and their descriptions:

- *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 |

Installieren Sie die Software. Wählen Sie alle angebotenen Komponenten wie «Kleopatra» oder «PGA» zur Installation aus. • Nach der Installation starten Sie das Programm mit «GPA». • Wenn alles korrekt lief, sollten Sie nebenstehenden Bildschirmausschnitt haben

....

Solution

Lösung



Volkan Demir

From:
<https://wiki.bzz.ch/> - **BZZ - Modulwiki**



Permanent link:
<https://wiki.bzz.ch/modul/m183/learningunits/lu05/aufgaben/08?rev=1755854433>

Last update: **2025/08/22 11:20**