

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:** 45 Minuten
- **Sozialform:** Gruppenarbeit zu 3-4 Personen
- **Hilfsmittel:**
 - Download-Link: [GnuPG-Download](#)
- **Erwartetes Ergebnis:** Prozessbeschreibung inkl. Screenshot wie Nachrichten und Medien verschlüsselt 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.

The screenshot shows the GnuPG.org download index page. At the top, there's a note about PGPME being the standard library for GnuPG. Below it, a section titled "Remarks" lists several graphical frontends: Pinenut, GPGME, Scute, GPG4Win, and GPG4ME. A note states that GPG4ME 7.4 is an old, single-binary version that still supports unsafe PGP-2 keys. The "GNUPG BINARY RELEASES" section follows, with a note that binary releases are not distributed but pointers to common Linux distributions are provided. It lists binary releases for Windows, OS X, Debian, RPM, Android, VMS, and RISC OS, each with a link to its respective download page.

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 7.4
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	rpmlint	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](#)



Volkan Demir

From:

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

Permanent link:

<https://wiki.bzz.ch/modul/m183/learningunits/lu05/aufgaben/08>

Last update: **2025/09/02 07:06**

