

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 verschlüsselt und entschlüsselt worden sind, als PDF-Datei.

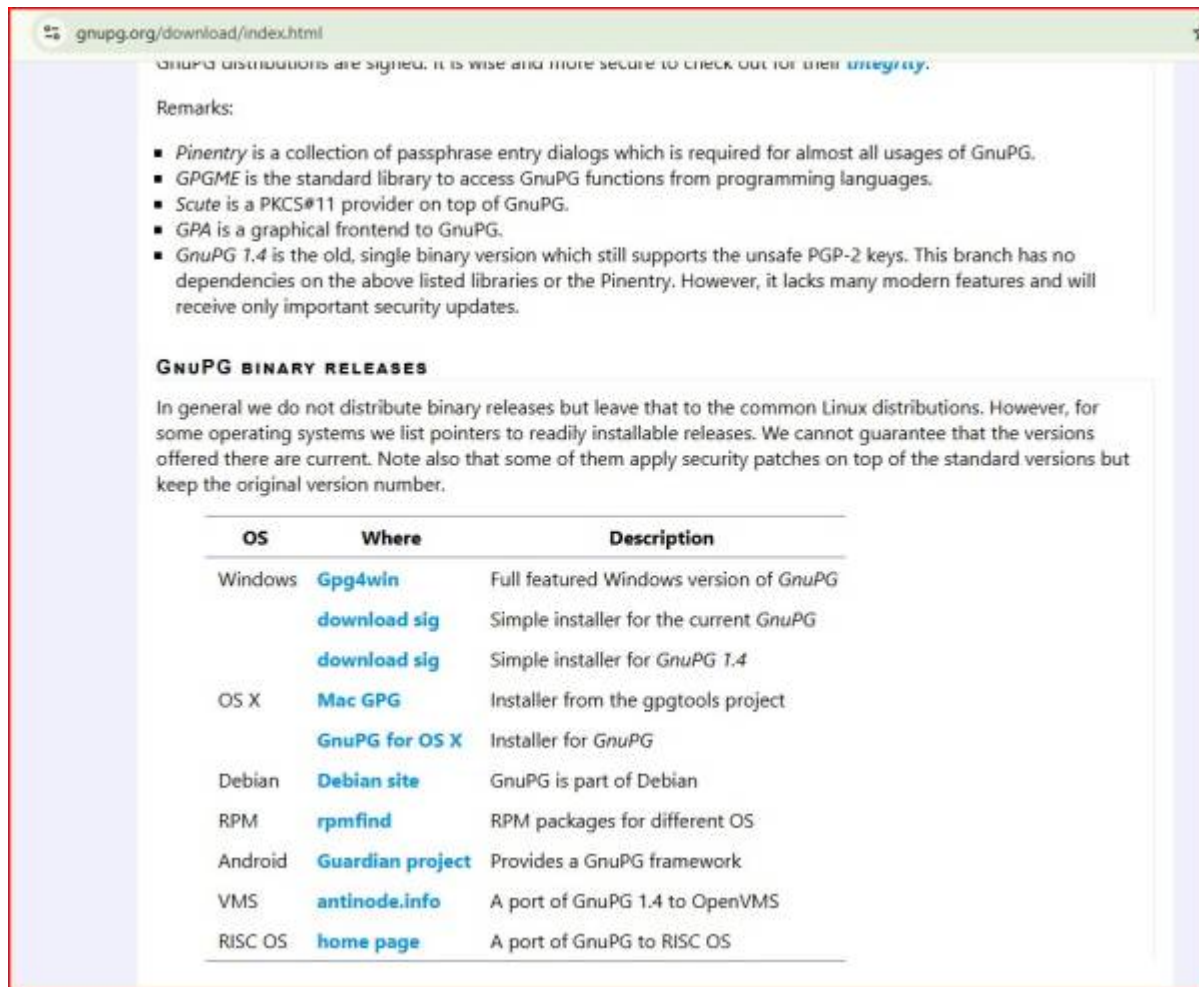
Ausgangslage

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 herunter.

The screenshot shows the GnuPG download page. At the top, it says "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 tools: Pinentry, GPGME, Scute, GPA, and GnuPG 1.4. Further down, the section "GNUPG BINARY RELEASES" explains that they generally do not distribute binary releases but provide pointers to readily installable releases for various operating systems. A table follows, listing the OS, where to find the release, and a description of each release.

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