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: GnuPGP-Download
- **Erwartetes Ergebnis:** Prozessbeschreibung inkl. Screenshot wie Nachrichten und Medien ver- und entschlüsselt worden sind, als PDF-Datei.

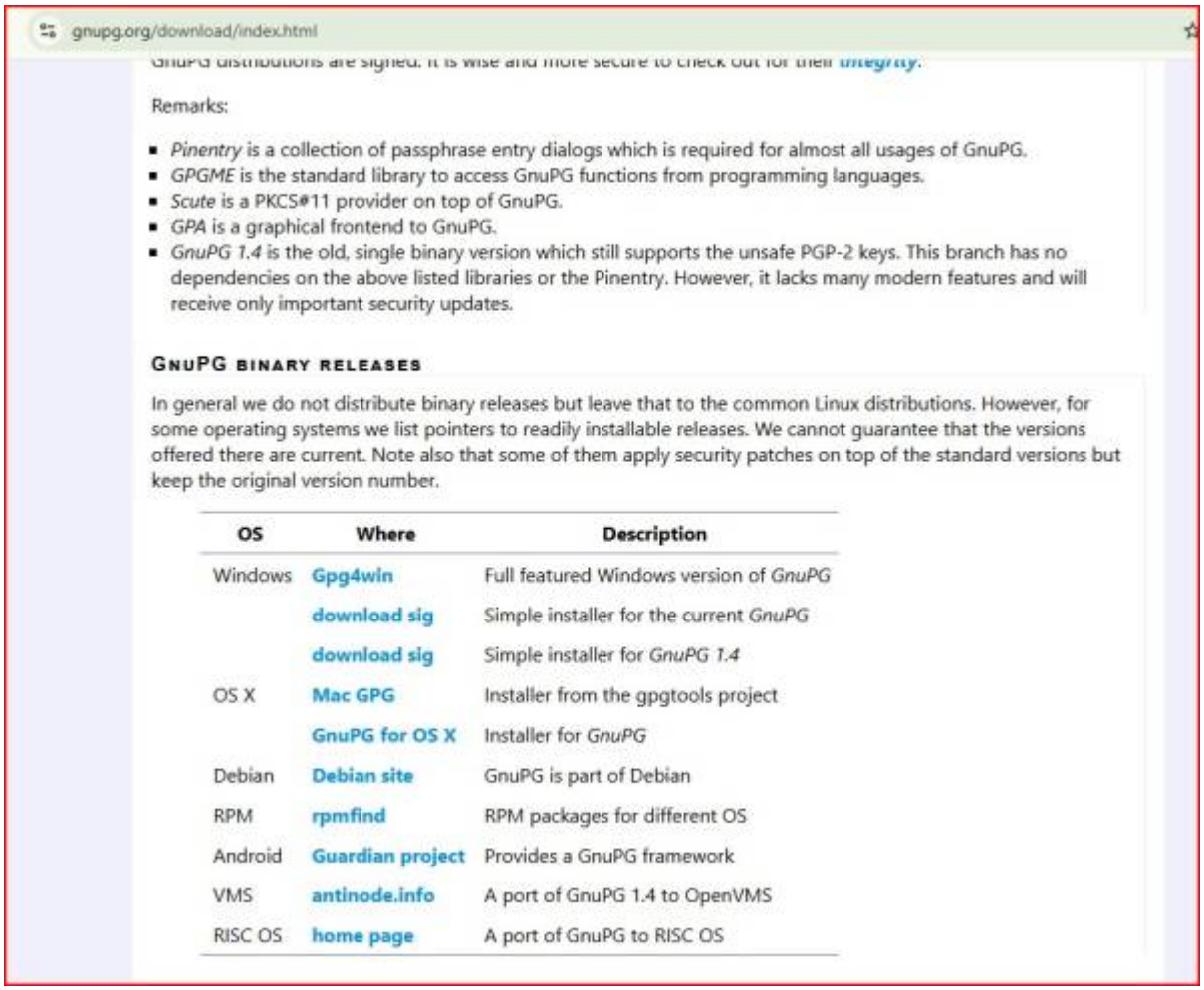
Ausgangslage

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

Vorarbeit

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



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
