GPG4Win ï Aufgaben Teil1

Hinweis: Eine Anleitung für die folgenden Aufgaben finden Sie in der Datei *M7_09_gpg4Win_Anleitung.*

Aufgabe 1: Starten Sie das Programm GPA (GNU Privacy Assistant) aus dem Paket Gpg4Win und erstellen Sie sich ein asymmetrisches Schlüsselpaar aus privatem und öffentlichem Schlüssel.

Aufgabe 2: Exportieren Sie Ihren öffentlichen Schlüssel und stellen Sie ihn den übrigen Kursteilnehmern zur Verfügung.

Aufgabe 3: Importieren Sie die öffentlichen Schlüssel der anderen Kursteilnehmer, mit denen Sie geheime Nachrichten austauschen möchten.

Aufgabe 4: Jetzt kann es losgehen!

a) Tauschen Sie einige geheime Nachrichten mit verschiedenen Kursteilnehmern aus. Vor dem Versenden muss die Nachricht also verschlüsselt werden. Der Empfänger muss sie anschließend auch wieder verschlüsseln.
b) Erstellen Sie ein kurzes Protokoll Ihres Nachrichtenaustausches, in dem steht, wer mit wem kommuniziert hat. Und welcher Schlüssel dabei jeweils verwendet wurde.

   Beispiel: Alice kommuniziert mit Bob:

   1. Alice schreibt eine Nachricht und verschlüsselt sie mit dem öffentlichen Schlüssel von Bob.
   2. Bob erhält die Nachricht von Alice und entschlüsselt sie mit é
   3. é
   4.

c) Simulieren Sie einen Angriff und versuchen Sie eine Nachricht zu lesen, die nicht für Sie bestimmt ist.

Aufgabe 5:

a) In der Datei *M7_09_gpg4Win_Anleitung* ist auch beschrieben, wie man eine Nachricht signieren und die Signatur anschließend überprüfen kann. Probieren Sie es aus, indem Sie mit ihrem Kommunikationspartner signierte Nachrichten austauschen.
b) Worin bestehen die Unterschiede zwischen dem Verschlüsseln und dem Signieren? Signieren und Verschlüsseln Sie auch einmal eine sehr lange Textdatei. Was fällt dabei auf?
c) Wer kann eine signierte Nachricht lesen? Stellen Sie sicher, dass nur der Empfänger, für den die Nachricht bestimmt ist, die Nachricht lesen kann.

Aufgabe 6:

a) Stellen Sie sich folgendes Szenario vor: Bob ist schwer verliebt in Alice. Nach langem Warten erhält er endlich eine Nachricht von Alice mit einer Einladung ins Kino. Bob hat allerdings auch Zoff mit seinem Mitschüler Cleo. Deshalb ist er sich nicht sicher, ob die Nachricht tatsächlich von Alice stammt oder ob Cleo ihn nur foppen will.

- Teilen Sie die Rollen von Alice, Bob und Cleo unter sich auf. Jeder benötigt einen eigenen Rechner.
- Simulieren Sie den Nachrichtenaustausch in den Varianten 1 bis 3 in beliebiger Reihenfolge, ohne dass Bob weiß, welche Variante gewählt wurde.
- Bob prüft jeweils die Signatur der Nachricht. Welche Meldungen werden jeweils ausgegeben? Welche Nachricht stammt tatsächlich von Alice?

Variante 1: Cleo schickt die Nachricht ohne Signatur.

Variante 2: Alice schickt die Nachricht ohne Signatur.

Variante 3: Alice schickt die Nachricht mit ihrer Signatur.

Variante 4: Cleo schickt die Nachricht mit seiner Signatur.

b) Gibt es für Cleo eine Möglichkeit Alice Signatur zu fälschen?