Praktikum zur „IT-Sicherheit“

Aufgabenblatt 1

Kryptographie mit GNU-PG

In den nachfolgenden Aufgaben wenden Sie mit GNU Privacy Guard (GPG) eine freie Software zum Verschlüsseln und Signieren von Dateien an. Sie arbeiten mit gpg von der Kommandozeile. Geben Sie bei allen Teilaufgaben in Ihrer Lösung die verwendeten Kommandozeilenaufrufe von gpg an.

Hinweise: Mit gpg –h erhalten Sie eine Kurzübersicht über die gebräuchlichsten Befehle von gpg. Für häufig genutzte Sub-Kommandos gibt es eine äquivalente Kurz- und Langform, beispielsweise:

-s, --sign [Datei] Eine Unterschrift erzeugen

Alternativ nutzen Sie das Tutorial, das Handbuch oder die man-Pages von gpg für die Auswahl der Aufrufparameter von gpg.

Generelle Hinweise zum Aufgabenblatt:

- Dokumentieren Sie die Lösungen Ihrer bearbeiteten Aufgaben für das Praktikumsgespräch und Ihre Unterlagen. Es ist sinnvoll, dies elektronisch zu tun, um auch Snapshots bzw. Ausgaben von der Kommandozeile einfach einbinden zu können.

Hinweise zur Vorbereitung: Informationen zu GNU-PG (GPG) finden Sie beispielsweise unter

Tutorial, Handbuch

http://www.online-tutorials.net/security/gnupg-gpg-tutorial/tutorials-t-69-124.html

http://www.gnupg.org/documentation/manuals/gnupg.pdf (Kapitel 4)

Allgemeine Information und Download

http://www.gnupg.org/

http://de.wikipedia.org/wiki/GNU_Privacy_Guard

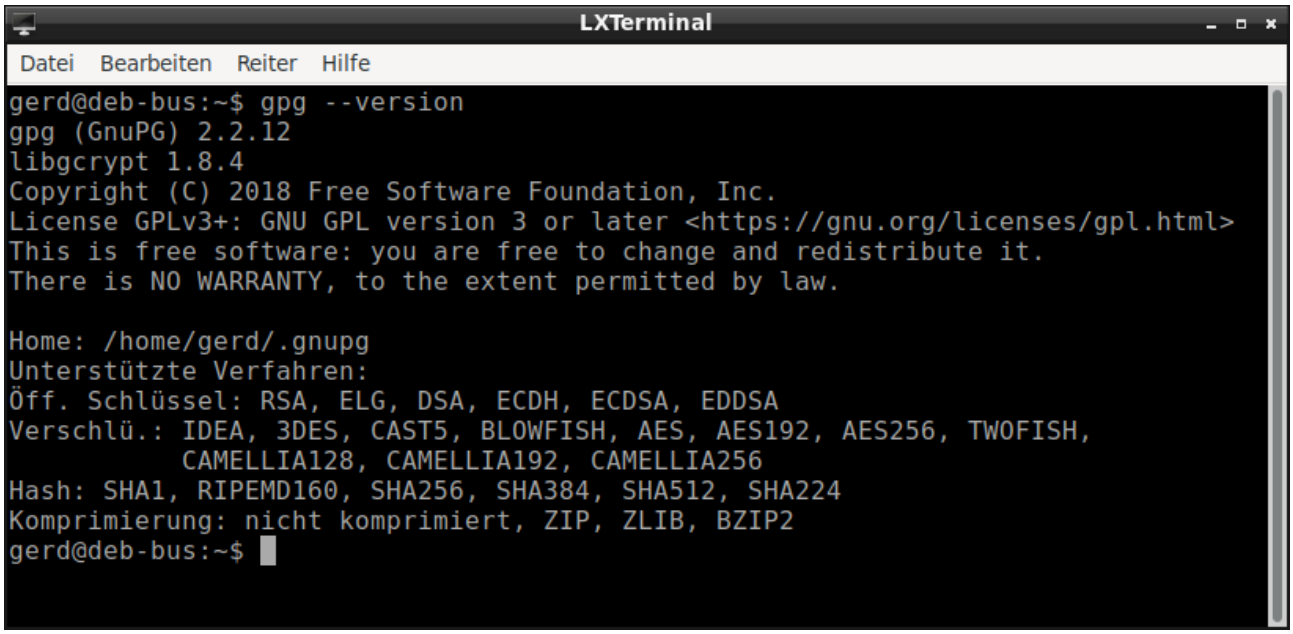
Windows Portable Version von GPG ermöglicht eine Nutzung ohne eine Installation auf dem Windows:

https://portableapps.com/apps/security/gpg-plugin-portable

Installation des Umfelds:

Praktikum zur „IT-Sicherheit“

Installieren Sie gpg in der Kommandozeilenversion auf Ihrem Rechner. Unter Windows können Sie auch eine portable Version verwenden, die nicht auf Ihrem Rechner sondern auf einem Datenträger installiert werden kann . Öffnen Sie ein Terminalfenster auf Ihrem Rechner und führen Sie darauf gpg zur Lösung der Aufgaben aus. Zur Überprüfung, ob die Installation auf Ihrem System erfolgreich war, sollte der Aufruf von „gpg --version“ die Versionsnummer Ihrer GPG-Installation in der Konsole anzeigen, wie z.B. im folgenden Screenshot zu sehen:



Aufgabe 1.1: GPG – Schlüsselmanagement

(Einzelaufgabe mit Gruppenanteilen)

a) Generieren Sie einen persönlichen GPG-Schlüssel mit dem Kommandozeilen-Aufruf „gpg --full-gen-key“. Verwenden Sie die Default-Einstellungen beim Schlüsseltyp: „RSA und RSA“.
Wenn Sie bei der Schlüsselgenerierung danach gefragt werden, geben Sie bitte Ihre Hochschul-email-Adresse an der Hochschule Bonn-Rhein-Sieg an, z.B. willi.winzig@h-brs.de.

b) Lassen Sie sich alle Schlüssel in Ihrem GPG-Schlüsselbund anzeigen. Was sind die privaten Schlüssel?

c) Exportieren Sie Ihren öffentlichen GPG-Schlüssel als ASCII-Datei. Geben Sie den Fingerprint Ihres öffentlichen GPG-Schlüssels aus. Stellen Sie diese Datei und den zugehörigen Fingerprint in LEA in die GPG-Schlüsseldatenbank (GPG_keyserver) ein.

d) Holen Sie bereits eingestellte Schlüssel Ihrer Gruppenmitglieder aus der GPG-Datenbank. (Sollte bereits ein Eintrag im Feld „signierter PublicKey“ vorliegen, so holen Sie sich diese Datei.) Verifizieren Sie den Fingerprint der importierten Schlüssel.

e) Nach erfolgreicher Verifikation signieren Sie den jeweiligen Schlüssel Ihrer Gruppenmitglieder. Anschließend exportieren Sie den signierten öffentlichen Schlüssel Ihres Gruppenmitglieds als ASCII-Datei und stellen ihn in dem Feld „signierter PublicKey“ der GPG-Schlüsseldatenbank Ihres Gruppenmitglieds ein.

f) Verwalten Sie die importierten GPG-Schlüssel mit gpg (Sub-Kommando: --edit-key). Geben Sie insbesondere an, wie weit Sie den importierten Schlüsseln vertrauen. Welche symmetrischen Kryptoalgorithmen sind voreingestellt?

Aufgabe 1.2: GPG – Ver- und Entschlüsselung

(Einzelaufgabe mit Gruppenanteilen)

a) Erstellen Sie eine formatlose Textdatei (mit ein wenig Textinhalt) mit einem Editor Ihrer Wahl. Verschlüsseln Sie diese Textdatei mit Ihrem öffentlichen Schlüssel und (mindestens) mit einem weiteren importierten Schlüssel Ihrer Gruppenmitglieder.

b) Tauschen Sie diese verschlüsselte Datei mit Ihren Gruppenmitgliedern aus. Entschlüsseln Sie Dateien, die Sie von Ihren Gruppenmitgliedern erhalten haben.

Aufgabe 1.3: GPG – Signaturerzeugung und -verifikation

(Einzelaufgabe mit Gruppenanteilen)

a) Erstellen Sie eine neue Textdatei. Signieren Sie diese Datei so, dass das Ausgabeformat ASCII ist und sowohl der Dateiinhalt als auch die Signatur in der Ausgabedatei enthalten sind. Verifizieren Sie die Korrektheit Ihrer digitalen Signatur.

Aufgabe 1.4: GPG – Kombination von Verschlüsselung und Signatur

(Einzelaufgabe mit Gruppenanteilen)

a) Verwenden Sie eine beliebige Datei. Signieren und verschlüsseln Sie sie für Ihre Gruppenmitglieder. Tauschen Sie die erzeugte Datei mit Ihren Gruppenmitgliedern aus.

b) Entschlüsseln und verifizieren Sie die Dateien, die Sie von Ihren Gruppenmitgliedern erhalten haben.

Praktikum zur „IT-Sicherheit“

Was sie für das Fachgespräch im Praktikumstermin für eine erfolgreiche Abnahme können müssen

1. Einfache Fragen zur Aufgabe des Tools gpg beantworten können
2. Das Tool gpg in einem Textfenster auf Ihrem Rechner bedienen und über BigBlueButton zeigen können.
3. Die geübten Funktionen von gpg an vorgegeben Dateien durchführen können.

Vorbereitung für den Abnahmetermin

1. Präsentation in BBB-Räumen üben.
    - Siehe LEA (BBB-Räume zur Team-Kollaboration).
    - Funktion der Webcam prüfen
    - Funktion des Mikrofons prüfen
    - Mit einem Teammitglied eine Präsentation üben.
2. Studierendenausweis und Lichtbildausweis zur Kontrolle bereit halten
3. Eine LEA Session für die Lehrveranstaltung 2021 WS – IT-Sicherheit öffnen.
4. Gpg Arbeitsumfeld auf Ihrem eigenen Präsentationsrechner verfügbar haben mit Ihrem gpg-Schlüssel, der aktuell in der Datenbank im LEA-Kurs steht.

Praktikum zur „IT-Sicherheit“

Erste Fragen im Praktikum

1. Einfache Fragen zur Aufgabe des Tools gpg beantworten können
   Was kann man mit Textdateien in gpg machen?
   - Was braucht man um einem Kommilitonen eine Datei verschlüsselt zu senden? Was braucht der Kommilitone um die Datei zu entschlüsseln?
   - Was ist ein Schlüsselring?
   - Wozu benötigt man einen Fingerprint?
   - Wie sollte man öffentliche Schlüssel austauschen?

2. Das Tool gpg in einem Textfenster auf Ihrem Rechner bedienen und über BigBlueButton zeigen können.
   - Schlüssel auflisten lassen
   - Wo ist der Fingerprint

3. Die geübten Funktionen von gpg an vorgegeben Dateien durchführen können.
   - Schlüssel zum Import zusenden
   - Signierte Datei verifizieren lassen