Praktikum zur „IT-Sicherheit“

Aufgabenblatt 1 – Lösungsskizze

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 GPG finden Sie z.B. 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 Installation**
  Windows Portable Versionen von GPG ermöglicht eine Nutzung ohne eine Installation auf dem Windows:

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

Praktikum zur „IT-Sicherheit“

Auswahl benutzter Kommandos/Optionen

```
--armor -a
--clearsign --clear-sign
--decrypt  -d
--edit-key with inputs "trust" "pref" "showpref"
--encrypt  -e
--export
--fingerprint
--full-gen-key
--import
--listkey
--listkeys  -k   --list-public-keys
--list-secret-keys   -K
--list-sig
--list-sigs
--output -o
--recipient -r
--sign-key
```

Unterstützende Tipps

- GPG erlaubt die Auswahl eines Keys aus dem Keyring mit minimaler Eingabe, z.B. nur anhand eines Vornames:

  ```
  # gpg –listkey fritz
  ```

- Automatische Kommandoerweiterung in der Shell (gilt das auch unter Windows und macOS):
  Eingabe eines Teilkommandos und dann mit der Tab Taste →| mögliche Kommandos vorschlagen lassen. Beispiel:

  `--list` →| →|

  schlägt `--listkey` und `--listkeys` vor.

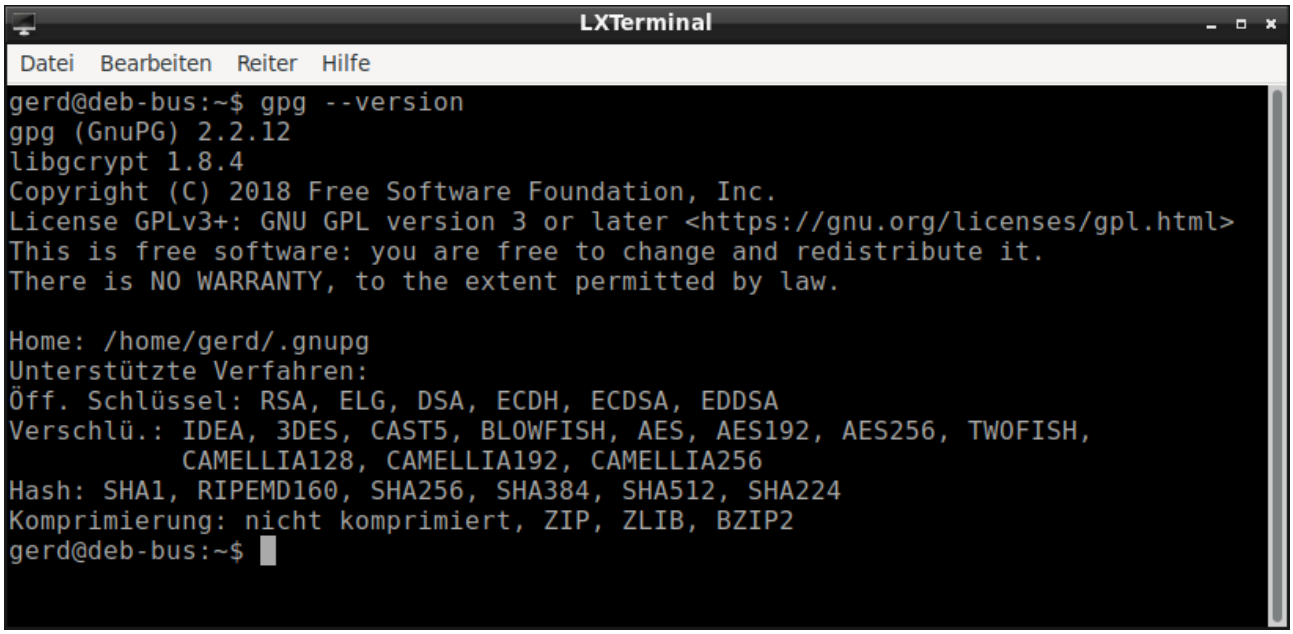
- Das Kommandofenster erlaubt häufig die letzten Befehle mit den Cursor-Tasten (hoch und runter) zurückzuholen und zu bearbeiten (die sog. Shell-History).

- Unter Linux wird für die Eingabe der Passphrase ein eigenes Fenster geöffnet.

Praktikum zur „IT-Sicherheit“

Installation des Umfelds:

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.wunderlich@smail.inf.h-brs.de.

Lösungshinweis:
`gpg --full-gen-key`

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

Lösungshinweis:
Der gesuchte Kommandozeilenschalter beinhaltet den folgenden Bestandteil: `list`

Praktikum zur „IT-Sicherheit“

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-Schlüssel-datenbank (GPG_keyserver) ein.

Lösungshinweise:
Die folgenden Kommandozeilen-Bestandteile werden beim Schlüsselexport benötigt und sollten daher in Ihrer Lösung vorkommen:
`--export`
`-a`

Für die Berechnung und Ausgabe des Fingerprints ist das folgende Flag erforderlich:
`--fingerprint`

Um die Konsolenausgabe eines Programms in eine Datei umzuleiten bzw. Zu schreiben kann in Linux-basierenden Betriebssystemen das Größer-Zeichen (>) gefolgt von einem Dateinamen verwendet werden.

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.

Lösungshinweis:
Einen SchlüsselImport ermöglicht GPG via
`--import`

Die Berechnung und Ausgabe des Hashwerts des Schlüssels erfolgt so wie in Teilaufgabe c).

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.
Lösungshinweis:
Zum Signieren eines öffentlichen Schlüssels steht folgender Schalter bereit:
`--sign-key`

Für die Signaturerzeugung wird der private Schlüssel des Unterzeichners benötigt. Dieser Schlüssel ist durch eine Passphrase geschützt (damit verschlüsselt gespeichert), die zur Signaturerzeugung eingegeben werden muss.
Der Export und Import des signierten öffentlichen Schlüssels erfolgt äquivalent zu den Teilaufgaben c) und d).
Zur Überprüfung Ihrer Aktionen können Sie das Flag `list-sigs` heran-

ziehen. Fehlt zu einer Signatur der öffentliche Schlüssel eines Signierenden in der Schlüsselliste, so wird zwar die Signatur des Schlüssels mit der Key-ID angezeigt, der Name des Signierenden dagegen nicht.

f) Verwalten Sie die importierten GPG-Schlüssel mit `--edit-key`. Geben Sie insbesondere an, wie weit Sie den importierten Schlüsseln vertrauen. Welche symmetrischen Krypto-Algorithmen sind voreingestellt?

Lösungshinweis:
Zur Festlegung des in einen Schlüssel entgegengebrachte Vertrauen wird das Schlüsselwort `trust` an geeigneter Stelle einzugeben sein.

Mit dem `edit-key`-Kommando `showpref` werden die zugrundeliegenden Krypto-Algorithmen ausführlich angezeigt. Hingegen zeigt `pref` nur die Abkürzungen der Algorithmennamen.

Aufgabe 1.2: GPG – Ver- und Entschlüsselung

(Einzelaufgabe mit Gruppenanteilen)

a) Erstellen Sie eine formatlose Textdatei (mit ein wenig Textinhalt in UTF-8) mit einem Editor Ihrer Wahl. Verschlüsseln Sie diese Textdatei mit Ihrem öffentlichen Schlüssel und (mindestens) mit einem weiteren importierten Schlüssel Ihrer Gruppenmitglieder.

Lösungshinweis:

Für die Lösung dieser Aufgabe werden Sie die nachfolgenden Kommando-Flags verwenden müssen:

```
-e
-a
-r
```

Bitte beachten Sie, dass die verschlüsselte Datei für zwei Empfänger (engl. ***r****ecipient*) verschlüsselt werden soll. Das entsprechende Flag kann im Gesamtbefehl auch mehr als nur einmal verwendet werden.

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

Lösungshinweis:
Für die Lösung dieser Aufgabe werden Sie die nachfolgenden Kommando-Flags verwenden müssen:

```
-d
-o
```

Bitte beachten Sie, dass bei diesem Befehl eine Umleitung der Konsolen-ausgabe mitte `>` nicht funktioniert. Stattdessen müssen Sie die Ausgabe (engl. ***o****utput*) über ein explizites Flag in eine Datei schreiben.

Praktikum zur „IT-Sicherheit“

Aufgabe 1.3: GPG – Signaturerzeugung und -verifikation

(Einzelaufgabe mit Gruppenanteilen)

a) Erstellen Sie eine neue Textdatei. Signieren Sie diese Datei so, dass das Ausgabeformat UTF-8 ist und sowohl der Dateiinhalt als auch die Signatur in der Ausgabedatei enthalten sind. Verifizieren Sie die Korrektheit Ihrer digitalen Signatur.

Lösungshinweis:

Für die gesuchten GPG-Kommandos werden Sie die folgenden Flags benötigen:

`--clearsign`

`--verify`

Aufgabe 1.4: GPG – Kombination von Verschlüsselung und Signatur

(Einzelaufgabe mit Gruppenanteilen)

a) Verwenden Sie eine beliebige Datei (z.B. Photos, die Sie von dieser Website laden können: https://unsplash.com/s/photos/security). Signieren und verschlüsseln Sie sie für Ihre Gruppenmitglieder. Tauschen Sie die erzeugte Datei mit Ihren Gruppenmitgliedern aus.

Lösungshinweis:

Kryptographische Operationen können auch kombiniert werden. In diesem Fall sollte der Schalter `-es` zum Ziel führen können.

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

Lösungshinweis:

Das bekommen Sie jetzt auch ganz ohne Hilfe hin!