

TdI 2015 – Workshop CryptoParty

Vorbereitung: Laden Sie das Paket

https://ddi.ifi.lmu.de/t di/2015/upload/workshop-cryptoparty/CryptoPaket.zip/at_download/file herunter. Standardmäßig wird es im home/downloads-Ordner gespeichert.

Entpacken Sie es mit rechter Maustaste und „extract here“.

Aufgabe 1 (Manuell mit JavaScript)

1. Öffnen und lesen Sie die für BOB gedacht verschlüsselte Nachricht in „CryptoPaket\Nachricht an BOB.txt“. Viel werden Sie nicht damit anfangen können.
2. Gehen Sie zum Entschlüsseln auf die Seite <http://encrypt.alexanderjank.de/> oder nutzen Sie die Offline-Version in „CryptoPaket\JavaScript\index.htm“. Dort müssen Sie a) mit copy und paste den Nachrichtentext eingeben und b) Bobs privaten Schlüssel hochladen, der sich in „CryptoPaket\Schluessel\BOB **PRIVATE** (0x402EEE97).asc“ befindet. In Wirklichkeit würde Bob seinen privaten Schlüssel natürlich nie zu einem Server hochladen.
(Das Passwort für die Schlüssel ist leer, einfach nichts eingeben.)
3. Verschlüsseln Sie eine eigene Nachricht *an* Bob. Benutzen Sie dazu die gleiche Seite. Zum Verschlüsseln brauchen Sie einen anderen Schlüssel, nämlich den öffentlichen Schlüssel von Bob, „CryptoPaket\Schluessel\BOB **PUBLIC** (0x402EEE97).asc“. Entschlüsseln Sie den verschlüsselten Text wieder mit Bobs privatem Schlüssel.
4. Welche Informationen sind im Schlüssel BOB PUBLIC gespeichert? Lassen Sie den Schlüssel auf der Webseite analysieren.
5. Schreiben Sie eine verschlüsselte Nachricht an Alice (mit ALICE PUBLIC verschlüsselt) und entschlüsseln Sie sie (mit ALICE PRIVATE).

Aufgabe 2 (Manuelles Versenden)

Verschlüsseln Sie eine Nachricht an Alice oder Bob (mit ALICE PUBLIC oder BOB PUBLIC). Kopieren Sie das verschlüsselte Ergebnis und senden Sie es von ihrer eigenen Mailadresse aus an alice@herr-rau.de oder bob@herr-rau.de. Wichtig: Benutzen Sie dazu reines Textformat und nicht HTML. Und Vorsicht: Ihre Nachricht wird – mit etwas Verzögerung – entschlüsselt und veröffentlicht unter <http://herr-rau.de/blogs/t di> und <http://twitter.com/fortbildungInfo>, damit Sie überprüfen können, dass die Verschlüsselung gelungen ist.

Das manuelle Ver- und Entschlüsseln mit JavaScript ist umständlich. Leichter geht das mit dem Firefox- und Chrome-Plugin „Mailvelope“, zumindest wenn Sie Ihre E-Mails von einem Browser aus senden.

Aufgabe 3 (Firefox-Plugin)

1. Installation des Plugins

Öffnen Sie den Browser Firefox und installieren Sie das Mailvelope-Plugin, das Sie im Web finden oder im Ordner „CryptoPaket\Addons\mailvelope.firefox.xpi“. (Siehe eigene Datei.)

2. Import der öffentlichen Schlüssel

Importieren Sie in Mailvelope zumindest die öffentlichen Schlüssel von Bob und Alice (ALICE und BOB PUBLIC).

3. Mail an Bob und Alice

Senden Sie eine verschlüsselte Mail von Ihrem eigenen E-Mail-Provider aus an alice@herr-rau.de oder bob@herr-rau.de. Benutzen Sie dazu reines Textformat und nicht HTML. Sie können auch eine Nachricht an thomas.rau@ifi.lmu.de verschlüsseln, wenn Sie den Schlüssel importieren.

Genug von Bob und Alice. Sie wollen endlich auch selber verschlüsselte Mails empfangen können.

Aufgabe 4 (optional: Schlüsselerzeugung für eigene Adresse)

Erzeugen Sie mit dem Mailvelope-Plugin ein eigenes Schlüsselpaar für ihre eigene Adresse. (Die Schlüssel werden in einem Unterordner Ihres Firefox-Profiles gespeichert.) Nutzen Sie Mailvelope, um die Schlüssel in Ihr Linux-Verzeichnis zu exportieren, damit Sie den privaten für zu Hause haben (falls Sie sich da keinen neuen anlegen wollen) und den öffentlichen anderen weitergeben können (durch Upload oder Mitsenden als Anhang).

Am komfortabelsten geht das Arbeiten mit Verschlüsselung, wenn Sie Thunderbird nutzen. Sie brauchen dazu Thunderbird, die Verschlüsselungssoftware GnuPG (unter Linux bereits installiert, unter Windows Gpg4win verwenden <http://www.gpg4win.de/>) und das Thunderbird-Addon „Enigmail“.

Aufgabe 5: (Thunderbird-Addon)

1. Installation des Plugins

Öffnen Sie den Thunderbird. Ein Konto für die E-Mail-Adresse tdi###@imap.cip.ifi.lmu.de ist bereits vorkonfiguriert. Installieren Sie das Enigmail-Plugin, das Sie im Web finden oder im Ordner „CryptoPaket\Addons\enigmail-1.8.2-tb+sm.xpi“. (Siehe eigene Datei.)

2. Erzeugen Sie ein Schlüsselpaar (für die Adresse tdi###@imap.cip.ifi.lmu.de)

Wenn Ihnen das Addon das nicht selbst vorschlägt, geschieht das über den Menüpunkt „Enigmail/Schlüssel verwalten.../Erzeugen“. Unter Linux dauert das Generieren von 4096 bit langen Schlüsseln aber recht lange, zum Testen tut es auch ein kürzer Schlüssel.

3. Veröffentlichen des public key

Senden Sie eine unverschlüsselte E-Mail an die Person neben Ihnen, und hängen Sie Ihren public key an die Mail an.

4. Warten auf Antwort (und selber antworten)

Wenn Sie eine solche Mail erhalten, fügen Sie den Schlüssel zu Ihrem Enigmail hinzu. Ab jetzt können Sie an diese Person eine *verschlüsselte* Mail schicken. Im Workshop nehmen wahrscheinlich folgende Benutzer teil:

tdi002, tdi003, tdi005, tdi006, tdi008, tdi013, tdi014, tdi016, tdi017, tdi020, tdi025, tdi026, tdi027, tdi030, tdi033, tdi035, tdi036, tdi037, tdi038, tdi039, tdi046, tdi047, tdi049, tdi051, tdi054, tdi059, tdi061, tdi063 (jeweils [@imap.cip.ifi.lmu.de](mailto:###@imap.cip.ifi.lmu.de)).

Sie können natürlich auch für Ihre eigene Adresse Schlüssel erzeugen. Mit Mailvelope, oder Sie können in Thunderbird Ihr eigenes IMAP-Konto importieren. Beachten Sie jeweils: Wenn Sie Ihr Schlüsselpaar zu Hause verwenden wollen, müssen Sie es auf einem USB-Stick mitnehmen. Und wenn Sie auf Sicherheit bedacht sind, müssen Sie Ihren Schlüssel sorgfältig vom Linux-System löschen.