Prof.Dr. Michael Anders
Studiengangsleiter Wirtschaftsingenieurwesen
Fachhochschule Wedel
Feldstraße 143
D 22880 Wedel

Wedel, den 04.03.14

Sehr geehrter Kommunikationspartner,

ich freue mich, dass Sie sich für den Schutz Ihrer elektronischen Kommunikation interessieren.

Unter der Webadresse http://www.youtube.com/watch?v=PR3XLeJDTQY oder http://www.fh-wedel.de/~an/crypto/videos/asymmetric_key_poem.ogv finden Sie ein dreiminütiges Video, das auf humorvolle Weise die Funktionsweise der asymmetrischen Kryptographie erläutert. Für den kompetenten Umgang mit dieser Verschlüsselungstechnik ist der im Video vermittelte Kenntnisstand ausreichend.

Es gibt zwei quelloffene Programme, Academic Signature und GnuPG, die auf komfortable Weise die starke, asymmetrische Verschlüsselung von Dateien für geschützten Transfer ermöglichen.

Beide Programme sind unter einer öffentlichen Lizenz frei verfügbar und wurden in Deutschland entwickelt. Kommerzielle Lösungen von in den USA ansässigen Softwareherstellern gelten unter Sicherheitsexperten nach den Enthüllungen des letzten Jahres nicht mehr als vertrauenswürdig.

Meine öffentlichen Schlüssel für die jeweiligen Programme finden Sie auf meiner Hochschulhomepage: http://www.fh-wedel.de/~an/crypto/academic_signature_key.html .

Beide Programme erstellen die Chiffre einer Datei im gleichen Ordner, in der auch die Originaldatei liegt. Die Programme benötigen lediglich die Angabe welche Datei zu verschlüsseln ist und für welchen öffentlichen Schlüssel. Alle anderen Angaben sind optional. Die für einen öffentlichen Schlüssel eines Kommunikationspartners chiffrierten Dateien, wie z.B. die Chiffre des Gutachtens zu einer Abschlussarbeit, können Sie dann ganz konventionell als Anhang einer unverschlüsselten E-Mail versenden. Zusätzliche vertrauliche Nachrichten können ebenfalls als verschlüsselte Dateien im Anhang einer lapidaren Klartextmail geschickt werden. Mit dem zugehörigen privaten Schlüssel kann der Empfänger dann auf seinem System die Chiffren in Klartext zurück wandeln.

Option 1:

Das Programm "**Academic Signature**"
Verschlüsselung mit elliptischer Kurven Kryptographie (ECC)
Verfügbar unter: http://www.fh-wedel.de/~an/crypto/Academic_signature_eng.html
auch zu finden über die Google Suche: > open source elliptic curve cryptography <
Auf der angegebenen Webseite finden Sie neben einer ausführlichen Anleitung auch Videotutorials zur Verwendung der Software.
Das Programm ist eine Eigenentwicklung und hat eine graphische Benutzeroberfläche.

Option 2:

Das Programm "**GnuPG**"
Verschlüsselung nach dem OpenPGP Standard mit dem RSA Verfahren
Verfügbar unter: http://www.gnupg.de/
auch zu finden über die Google Suche: > open source public key cryptography <
Auf der Website finden Sie Hinweise auf verschiedene graphische Benutzeroberflächen, die für das Programm entwickelt wurden.
Für GnuPG gibt es eine Vielzahl von "Plugins" für verschiedene Mailprogramme, die -richtig konfiguriert- die Verschlüsselung automatisch für die gesamte E-Mail inklusive Mailanhängen durchführen können. Bei korrekter Nutzung dieser Plugins kann auf die manuelle Verschlüsselung einzelner Dokumente verzichtet werden.

Ich verfüge über Schlüssel für beide Verschlüsselungsprogramme. Als Entscheidungshilfe für Ihre Wahl möchte ich Ihnen eine Einschätzung aus meiner persönlichen Sicht anfügen:

Academic Signature ist transparenter, nutzt ein moderneres Kryptosystem und das Programm kann mit sehr begrenzten Computerkenntnissen ohne fremde Hilfe installiert, konfiguriert und betrieben werden. Alle Optionen sind über Dialoge der graphischen Benutzeroberfläche einstellbar. Jede Ver-/Entschlüsselung oder ggf. Signatur ist manuell auszulösen. Man sollte allerdings die Grundzüge der asymmetrischen Kryptographie in der Tiefe kennen, wie sie in dem oben verlinkten Video dargestellt werden.

GnuPG ist verbreiteter, langjährig bewährt, allerdings ist der manuelle Betrieb etwas umständlich und nicht immer transparent. Mit Mailer Plugin und richtig -am besten durch einen Experten- konfiguriert kann der Betrieb sehr einfach sein und die gängigen Operationen passieren meist automatisch im Hintergrund auch ohne besonderes Verständnis auf Benutzerseite.

Ich würde mich sehr freuen, wenn Sie sich für geschützte elektronische Kommunikation mit mir entscheiden könnten.

Mit freundlichen Grüßen,

Prof.Dr. Michael Anders