L3 1. Verschlüsselung und Datensicherheit

1.3 Moderne Verschlüsselungsverfahren

Hinweis: Beachten Sie zur Bearbeitung der nachfolgenden Aufgabenstellungen

- das Video https://www.youtube.com/watch?v=4mbryW8fZrA
- den Informationstext *L3 1.3 Informationsmaterial Asymmetrische Verschlüsselung.docx*

1.3.1 Was ist symmetrische Verschlüsselung? Welchen Nachteil hat sie?

Wer eine Nachricht versendet, verschickt gleichzeitig auch eine Kopie des Schlüssels. Mit diesem Schlüssel entschlüsselt der Empfänger die Nachricht. Die Nachricht wird mit dem gleichen Schlüssel ver- und entschlüsselt. Wird eine Nachricht abgefangen, dann würde auch der Schlüssel abgefangen werden und die Verschlüsselung ist nutzlos.

1.3.2 Zur Verschlüsselung von Dateien steht eine Vielzahl an Open-Source-Software zur Verfügung. So bietet beispielsweise die Software *7-Zip* die Möglichkeit, einzelne Dateien oder Dateiordner zu verschlüsseln.
Die Software steht Ihnen in im Unterordner '7-ZipPortable' zur Verfügung.

1.3.2.1 Verschlüsseln Sie eine beliebige Datei und versenden Sie diese per E-Mail an einen Mitschüler/eine Mitschülerin Ihrer Klasse.
Einen Link zur Anleitung der Software *7-Zip* finden Sie unter folgendem Link:
https://praxistipps.chip.de/7-zip-archivdateien-mit-passwort-verschluesseln_27706

1.3.2.2 Begründen Sie, welches Verschlüsselungsverfahren bei der Software *7-Zip* zur Anwendung kommt.

Es handelt sich um ein symmetrisches Verschlüsselungsverfahren. Sie benötigen den Schlüssel, um den Container, in den Sie die Datei kopiert haben, zu verschlüsseln. Ihr Lehrer benötigt diesen Schlüssel ebenfalls, um den Container wieder zu entschlüsseln.

1.3.2.3 Empfehlen Sie Ihrem Lehrer eine weitere Software, mit der er seine Notenlisten verschlüsselt per E-Mail verschicken kann.

Zum Beispiel:

- VeraCrypt
- ProxyCrypt
- GNU Privacy Guard
- DiskCryptor

1.3.3 Wie läuft asymmetrische Ver- und Entschlüsselung ab? Was ist der Vorteil im Vergleich zur symmetrischen Verschlüsselung?

Bei der asymmetrischen Verschlüsselung existiert ein Schlüsselpaar:

- Öffentlicher Schlüssel (vgl. offenes Vorhängeschloss; zum Verschlüsseln)
- privater Schlüssel (vgl. Schlüssel; zum Entschlüsseln)

Es steht ein öffentlicher Schlüssel zur Verfügung. Mit diesem kann der Versender eine Nachricht verschlüsseln (vgl. Vorhängeschloss schließt sich). Diese Nachricht lässt sich mit privatem Schlüssel öffnen. Vorteil: Der private Schlüssel, der zum Entschlüsseln einer Nachricht benötigt wird, wird nie versendet. Abgefangen werden kann nur: der öffentliche Schlüssel, die verschlüsselte Nachricht.

1.3.4 Nennen Sie ein Beispiel für ein asymmetrisches Verschlüsselungsverfahren.

RSA-Verfahren

1.3.5 Überprüfen Sie für zwei Ihrer Apps, ob sie Ende-zu-Ende-Verschlüsselung anbieten und ob der Quellcode „Open-Source“ ist. Suchen Sie ggf. nach Alternativen.