Verschlüsselung

Warum verschlüsseln?

Du hast dir in der letzten Stunde ein Verfahren zum Übertragen von Farben und einfachen Grafiken überlegt. Für die Übertragung von Daten gibt es seit langem Codierungen - vor allem in der Schifffahrt. Hier findet teilweise immer noch das

Morsealphabet

seine Anwendung. Dieses Verfahren wurde auch sehr lange zum Telegrafieren genutzt. Es gibt auch Webseiten zur Codierung / Decodierung von Morsecode, die du zur Unterstützung nutzen kannst.

Aufgabe 1 (Partnerarbeit) - Eine vorgebene Nachricht übertragen
Übertrage folgenden Satz per Morsezeichen über eine längere Distanz an deine(n) Partner/in:

Still ruht der See.

Diese Aufgabe dient allein der Übung! Du musst dir einen geeigneten Übertragungsweg überlegen. Das kann beim Morsen sehr vielfältig sein.

Aufgabe 2 (Partnerarbeit) - Eine selbst erfundene Nachricht übertragen
Überlege dir einen kurzen Satz aus drei kurzen Worten. Übertrage diesen an eine(n) zufällige/n Partner/in.

- Warum funktioniert das?
- Welche Problematik kann das mit sich bringen?

Transportverschlüsselung

Caesarverschlüsselung als ein symmetrisches Verschlüsselungsverfahren

Bei einer bekannten Codierung können Daten sehr leicht auf dem Transportweg abgehört werden. So könnten Morsezeichen, die nachts per Licht übertragen werden z.B. von Feinden sehr leicht mitgehört werden. Man kann die Daten durch eine Verschlüsselung schützen. Eine sehr einfache (und unsichere Methode) zur Verschlüsselung ist die

Caesar-Verschlüsselung

.

Aufgabe 3 (Partnerarbeit) - Mit der Caesar-Verschlüsselung üben

Erledigt zusammen die Aufgaben in dem Material zur

Caesar-Verschlüsselung

. Eine große Hilfe kann dabei eine Textverarbeitung sein, mit der ihr Klaralphabet und Geheimalphabet wie im Material untereinanderschreibt. Die Größe der Verschiebung dürft ihr selbst bestimmen.

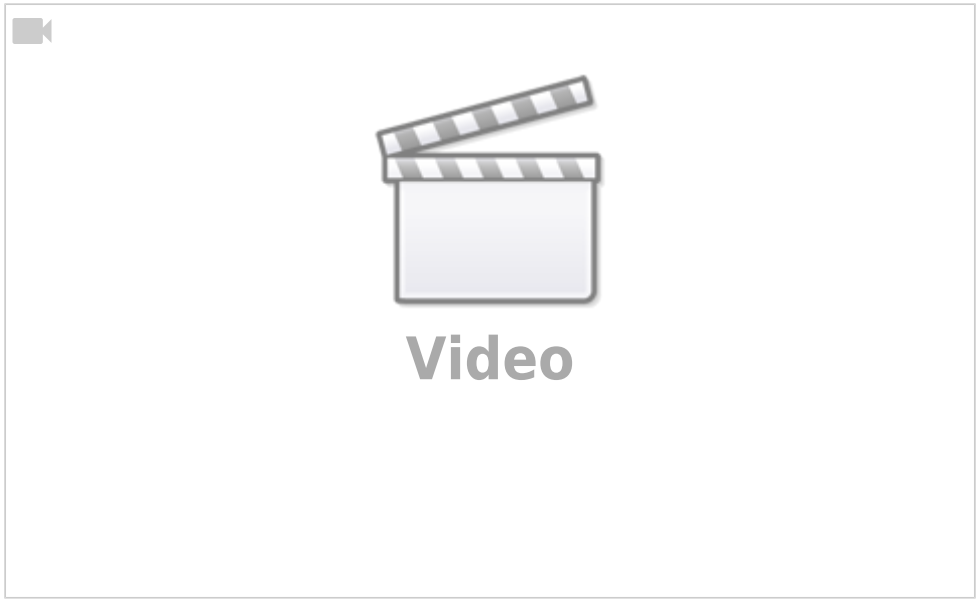
Aufgabe 4 (Partnerarbeit) - Verschlüsselte Nachrichten morsen
Überlege dir einen kurzen Satz aus drei kurzen Worten. Übertrage diesen diesmal verschlüsselt an deine(n) Partner/in. Es ist sehr wichtig, dass du diesem die von dir gewählte Verschiebung mitteilst.

Die Caesarverschlüsselung ist sehr leicht zu knacken. Diese Material zeigt, wie es geht.

Aufgabe 5 (Gruppenarbeit - Angriffsprinzip auf die Caesarverschlüsselung erklären
Erlärt mit einer kleinen Präsentation, wie der Angriff auf die Caesarverschlüsselung funktioniert.

Die asymmetrische Verschlüsselung

Schaue dir dieses Video an:



Aufgabe 6 (Partnerarbeit) - Fragen zum Video beantworten

1. Was ist das Problem an der symmetrischen Verschlüsselung?
2. Was ist der Unterschied zwischen einem öffentlichen und einem privaten Schlüssel?
3. Wann verschlüsselt man mit dem öffentlichen und wann mit dem privaten Schlüssel?
4. Warum stellt die asymmetrische Verschlüsselung einen sicheren Weg zur Übertragung eines symmetrischen Schlüssels dar?

Sonderfall: Passwörter sicher speichern

Du hast in der Onlinewelt oft mit Passwörtern zu tun. Menschen sind faul und neigen dazu, das gleiche Passwort für unterschiedliche Dienste zu verwenden. Wenn ein Passwort „fällt“, fallen dann alle Accounts, die mit dem gleichen Passwort geschützt sind.

Besonders übel:
Oft kann man sein Passwort über eine Passwort-Vergessen-Funktion zurücksetzen. Man bekommt dann einen Link an die hinterlegte E-Mailadresse geschickt, mit dem man sein Passwort wiederherstellen kann. Hat aber nun der Angreifer Zugang zu diesem E-Mailkonto, kann er sich sogar trotz ggf. unterschiedlicher Passwörter Zugang auf alle Dienste verschaffen, bei denen die E-Mailadresse hinterlegt ist.

Abhilfe können Passwort-Manager schaffen. Das sind Apps, die lokal auf deinem Handy laufen und sehr komplexe Passwörter generieren, auf die man mit einem Hauptschlüssel Zugriff hat. Du entsperrst verschlüsselte Passwortdaten mit deinem Hauptpasswort oder anderen Methoden (z.B. FaceID), musst dir also nur ein Passwort merken und bist trotzdem sicher im Netz unterwegs.

Es gibt proprietäre Passwortmanager, die über die Cloud funktionieren. Die sind sehr komfortabel und funktionieren über Gerätegrenzen hinweg. Dummerweise liegen deine Daten dann bei dem Anbieter, der auch die Art der Verschlüsselung bestimmt. Eine Alternative ist die quelloffene Technik „keepass“, für die es Apps für nahezu alle Handys und Betriebssysteme gibt. Diese können verschlüsselte Passwortdatenbanken erzeugen, die du recht bedenkenlos über einen Cloudanbieter (meist Google, iCloud) synchronisieren kannst.

- keepass2android - für Android-/Googlehandys
- keepassium - für iOS-/Applehandys

Achtung!
Wenn du das Passwort deines Passwortmanagers vergisst oder der Zugang über z.B. FaceID nicht mehr klappt, hast du ein echtes Problem! Du musst dir etwas überlegen, wie du da wieder herankommst.

Gleiches gilt für den Fall, dass du deine Passwortdatenbank verlierst! Mache unbedingt Sicherungskopien!

Aufgabe 7: Einen Passwortmanager nutzen
Suche im Playstore nach „keepass2android“, wenn du ein Androidhandy hast. Suche im Appstore nach „keepassium“, wenn du ein Apple-Handy hast.

- Installiere die dazugehörige App.
- Lege eine neue Datenbank „Informatikunterricht“ an
- Sichere diese Datenbank mit einem starken Passwort
- Erinnere Herr Riecken daran, dass er für dieses Wiki die Selbstregistrierung anschaltet
- Logge dich aus dem Wiki aus
- Registriere dich mit deiner Schul-E-Mailadresse, deinem Namen und einem sicheren Passwort
- Hinterlege diese Daten in deiner Keepass-Datenbank

Dein von dir gewähltes Passwort ist der private Schlüssel zu deiner Passwortdatenbank. Wir nutzen freie Versionen von Passwortmanagern. Diese sind meist um Komfortfunktionen beschnitten. Die Bezahlversionen erkennen z.B. beim Surfen eine Passworteingabeaufforderung, fragen nach dem Masterpasswort und loggen dich dann automatisch ein, ohne dass du das Passwort noch vorher kopieren musst.