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

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 einen kleinen Präsentation, wie der Angriff auf die Caesarverschlüsselung funktioniert.

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 zurücksetzen 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. Eine Alternative ist die quelloffene Technik „keepass“, für die es Apps für nahezu alle Handys und Betriebssysteme gibt.

From:
http://cs-free.riecken.de/ - **Informatik 10**

Permanent link:
http://cs-free.riecken.de/doku.php?id=lesson:four&rev=1694415515

Last update: **2023/09/11 08:58**