# Ablaufplan Workshop Hacking als Beruf

|  |  |  |  |
| --- | --- | --- | --- |
| **9:00 - 9:15** | **Begrüßung** | **Vorstellungsrunde** und Vorstellung des dEIn Labors | 15 Min |
| **9:15 - 9:55** | **Input** | **“Hacken als Berufsfeld”** (Folien)  - Einleitung über die Begriffe: Hacken, Daten, Berufsfelder  - Datenschutz und Gefahren  - Grundlagen von Hacken als Beruf  - Präsentation der Berufsfelder  - Video Quanten-Kryptographie-Forscherin  - Ziele im Praktischen Teil | 30 - 40 Min |
| **9:55 - 10:40** | **Erste Workshop-einheit**  **Stufe 1** | **Calliope-Tresor**  (verfügt über 4 kapazitive Pins {0,1,2,3})  - Das Passwort ist eine vierstellige Folge von Pins, z.B. (0,1,3,0).  Ein Programm zur Überprüfung der Passworteingabe ist bereits auf jedem Calliope vorinstalliert  **Aufgabe**:: Das Passwort soll „von Hand“ erraten werden, indem die Pins der Reihe nach ausprobiert werden. Bei korrekter Eingabe nach Berührung eines Pins leuchtet die Kontroll-RGB-LED grün. Außerdem wird die entsprechende Zahl im LED-Panel visualisiert (bei „Pin 3 an 2. Stelle“ leuchtet die LED in Zeile 3 und Spalte 2). Es wird auf das Berühren der nächsten Pin gewartet. Bei falscher Eingabe leuchtet die RGB-LED rot und das Programm wird abgebrochen; das Raten beginnt von neuem.  **Frage**: Wie oft rätst du bis zur Lösung? Wie oft müsstest du im schlimmsten Fall raten? | 45 Min |
| **10:40 - 11:10** | **Pause** |  | 30 Min |
| **11:00 - 12:50** | **Zweite Workshop-einheit**  **Stufe 2**  **Stufe 3**  **Stufe 4** | **Passwortschutz und -prüfung mit Python**  Stufe 2: Einführung in Python (For-Schleifen und Bedingte Anweisungen).  Stufe 3: Das Passwort ist ein vierstelliger Zahlencode in einer geschützten Datei. Mit *check()* wird eine Zeichenkette mit dem echten Passwort in der Datei verglichen. Ausgabe: True für „korrekt“, sonst False.  Stufe 4: Das Passwort ist eine vierstellige Zeichenkette. in einer geschützten Datei. Wie muss *check()* aufgerufen werden?  **Frage**: Wie viele Vergleiche sind im ungünstigsten Fall bei vierstelligen Passwörtern nötig (a. bei Zahlen, b. bei Wörtern) Wie viele Vergleiche bei fünstelligen PW (a/b)?. | 110 min |
| **12:50 13:15** | **Abschluss** | *Ausblick auf „Verschlüsselung“*: Sicherheit muss so groß sein (Worst Case muss so viele Schritte umfassen), dass der Brute-Force-Ansatz keine Chance mehr hat (z.B. Laufzeit 3 Mio Jahre) |  |
| **13:30 - 15:00** | **Dritte Workshop-einheit:**  **Optionale Ausbau-stufe**  **Stufe 5**  **ab Klasse 10 (oder bei mehr-tägigen Workshops)** | **Von Brute-Force-Methoden zu Intelligentem Raten**  **Stufe 5a (Wörterbuchalgorithmus)**: Nimm ein Wörterbuch zu Hilfe, dessen Wörter in einer Vorstufe unseres Dekodierungs-programms als erste mit dem zu ratenden PW verglichen werden.  **Stufe 5b (Soziales Profil):** Berücksichtige Informationen über die Person, die sich das Passwort ausgedacht hat (Profile können aus dem Netz stammen oder frei erfunden werden und enthalten Infos zu Hobbies, Namen der Kinder, Freunde, Haustiere, …) und ergänze das Wörterbuch um diese Wörter.  **Frage**: Wenn beides nicht hilft, das Passwort zu raten, was könnte man noch tun, um schneller zur Ziel zu komjmen? (gängige Buchstabenkombinationen im Deutschen zuerst prüfen; Wörter aus dem Wörterbuch kombinieren; am Ende immer: Brute Force)  **Lernziele**- Erkenntnis „Das Internet weiß viel über mich“. Vorstellung davon, wie ein Passwort besser nicht aussehen sollte (keine Namen von Freunden, Haustieren, keine gängigen Wörter). Besser: Kombi mit Zahlen und Sonderzeichen | 90 min |