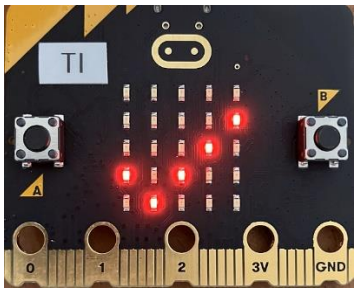
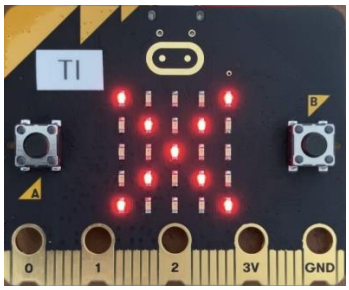
So funktioniert es

- Ein Kennwort wird auf einem Computer in einer Form gespeichert, die für Menschen nicht lesbar ist. Wenn ein Hacker Ihren Computer durchsucht, sieht er Ihr Kennwort nicht im Klartext. Stattdessen sieht er eine verschlüsselte Version, einen sogenannten Hash.
- Bei der Erstellung eines Kontos wird das Klartext-Passwort mit einer Hash-Funktion, z. B. SHA-256, verschlüsselt und für einen späteren Vergleich bei der Passwortauthentifizierung in einer Datei gespeichert. Der von SHA-256 erzeugte Hashwert ist 256 Bit lang.
- Bei der Passwortauthentifizierung wird das eingegebene Klartextpasswort gehasht und mit dem vom *micro:bit* abgerufenen gültigen Hash verglichen. Wenn die Hashes gleich sind, wird der Benutzer authentifiziert und erhält die Kontrolle über das angeschlossene Schloss.
- Bei der Fernsteuerung des Schlosses wird der Hash-Wert übertragen und kann abgehört werden. Wenn ein Hacker den Hash Ihres Kennworts erhält, kann er in einer Rainbow-Tabelle nach dem Hash suchen. Wird er gefunden, kann das mit diesem Hash verbundene Klartextkennwort ermittelt werden.
- Diese Anleitung unterstützt keine externen Komponenten wie eine Schatztruhe oder ein elektrisches Schloss, sondern simuliert das Aufknacken eines Schlosses durch entsprechende Symbole und akustische Signale auf dem *micro:bit*.

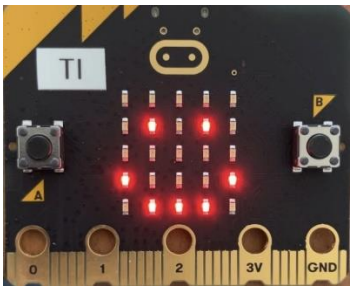
micro:bit Häckchen



micro:bit Kreuz



micro:bit smile



Was ist zu tun?

1. Legen Sie ein Passwort für Ihren *micro:bit* fest.
    a. **Wählen Sie eines der zehn gebräuchlichen Passwörter aus,** die in der Regenbogentabelle dieser Aktivität enthalten sind.

Passwort	*qwerty*	*111111*	*abc123*	*12345678*
123456	*Gast*	*123123*	*123456789*	*12345*

    b. Gehen Sie auf die Seite mit "*set_password.py*" und führen Sie das Programm aus, um das Passwort Ihrer Wahl auf Ihrem *micro:bit* zu setzen.
2. Üben Sie das Auf- und Abschließen der Schatztruhe
    a. Wechseln Sie auf die Seite mit "*authentication.py*" und führen Sie das Programm aus, um Ihr Passwort und die Authentifizierungsroutine zu testen. Dieses Programm vergleicht den auf dem *micro:bit* gespeicherten Hash mit dem Hash des eingegebenen Passworts. Wenn die beiden übereinstimmen, wird dem Benutzer der Zugang gewährt und es erscheint ein Häckchen-Symbol auf dem *micro:bit*.
    b. Drücken Sie [enter], um die Truhe wieder zu schließen. Dies wird mit einem Kreuz-(X)-Symbol auf dem *micro:bit* quittiert.

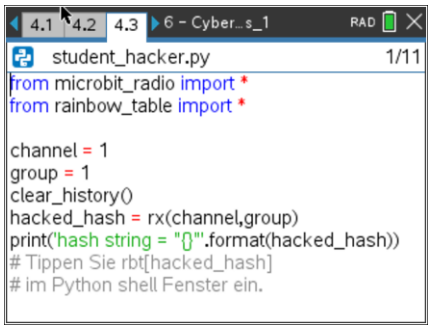
3. Fernanmeldung bei der Schatztruhe
   - Der *Empfänger*:
     - wechselt auf die Seite "*student_receiver.py*" auf und startet das Programm. Teilen Sie dem *Sender* Ihr Passwort mit, da er Ihre Schatztruhe aus der Ferne öffnen wird.
   - Der *Sender*
     - wechselt auf die Seite "student_sender.py" auf. Senden Sie das Passwort des *Empfängers*, da Sie dessen Schatztruhe aus der Ferne entsperren werden. Starten Sie Ihr Programm**, nachdem** der *Empfänger* und der *Hacker* ihre Programme gestartet haben.
   - Der *Hacker*
     - wechselt auf die Seite "student_hacker.py" und führt das Programm aus. Sie sollten den übertragenen Hash des Schatztruhen-Passworts des *Empfängers* erhalten. Nachdem Sie den gehackten Hash angezeigt bekommen haben, tippen Sie beim Shell Prompt >>> rbt[] ein. Bewegen Sie den Cursor in die eckige Klammer, drücken Sie die [var] Taste auf dem Taschenrechner und wählen Sie "hacked_hash". Ihre Python-Shell sollte wie folgt aussehen: >>>rbt[hacked_hash]; dieser Befehl gibt das Klartext-Passwort für den eingegebenen Hash zurück.
   - Sobald der *Hacker* das Klartext-Passwort des *Empfängers* kennt, sollte der *Empfänger* sein Programm erneut ausführen. Jetzt sollte der *Hacker* zum Programm "student_sender.py" wechseln, das Programm starten und den gehackten Hash eingeben. Haben Sie das Schloss geöffnet, ohne das geheime Kennwort des *Empfängers* zu erfahren?

Die Programme

Rolle des Senders

Rolle des Empfängers

Rolle des Hackers



Weitere Übungen

- Wechseln Sie in Ihrem Team die Rollen und versuchen Sie es erneut.
- Versuchen Sie ein neues Passwort, das nicht in der Regenbogentabelle enthalten ist.
- Versuchen Sie, das Passwort erneut einzugeben. Vergewissern Sie sich, dass auf dem Display des Taschenrechners *"file written and closed*" und auf dem Display des *micro:bit* ein "✓" angezeigt wird.
- Ändern Sie den Ton und die LED-Anzeigen, die während der Authentifizierung verwendet werden.

Prüfen Sie Ihr Verständnis

- Ein Hash ist eine eindeutige 256-Bit-Zeichenkette, die ein Klartextpasswort darstellt.
- Bei der Authentifizierung wird ein gespeicherter gültiger Hash eines Kennworts mit einem berechneten Hash eines eingegebenen Klartextkennworts verglichen. Wenn die beiden Hashes übereinstimmen, authentifiziert das System den Benutzer und gewährt ihm Zugang.
- Bei der Fernsteuerung des Schlosses wird der Passwort-Hash an den *Empfänger* gesendet, nicht das Klartext-Passwort.

Hilfe

- Vergewissern Sie sich, dass alle Teammitglieder die ihnen zugewiesene Gruppennummer verwenden.
- Stellen Sie sicher, dass der *Empfänger* und der *Hacker* ihre Programme ausführen und warten, bevor der *Sender* die Nachricht überträgt.
- *Empfänger* und *Hacker* können ihre Programme bei Bedarf durch Drücken der <esc> Taste jederzeit beenden.
- Stellen Sie sicher, dass die Passwörter auf jedem *micro:bit* erfolgreich gesetzt wurden.