So funktioniert es

- Radiowellen sind elektromagnetische Wellen wie Licht, aber mit einer niedrigeren Frequenz. Alle elektromagnetische Strahlung bewegt sich mit Lichtgeschwindigkeit, 3,0 x 10^8 m/s. Radiowellen können kurze oder lange Strecken zurücklegen, je nach der elektrischen Leistung des Senders. Der *micro:bit* kann im freien Raum etwa 70 Meter weit agieren. Schauen Sie auf die Rückseite Ihrer micro:bit Karte in die obere linke Ecke. Hier finden Sie die goldene Antenne des Senders/Empfängers. Hier werden die Funkwellen in der Karte aufgenommen und von ihr abgegeben.
- Der *micro:bit* sendet und empfängt Radiowellen mit Frequenzen von 2402 bis 2486 Megahertz. Dieser Bereich wird als Spektrum des Radios bezeichnet. Der *micro*:bit ist in 1 MHz breite Bänder unterteilt, die **Kanäle** genannt werden. Auf dem *micro:bit* gibt es **84** verschiedene Funkkanäle, die von 0 bis 83 nummeriert sind. Um zu kommunizieren, müssen sich zwei oder mehr *micro:bits* denselben Kanal teilen.
- Textnachrichten werden den Funkwellen in digitaler Modulation hinzugefügt. Die Textnachrichten werden in ein **Paket** eingefügt, einschließlich zusätzlicher Informationen, die für die Weiterleitung und die Fehlerprüfung benötigt werden.
- Zusätzlich zu den *micro:bit* Funkkanälen gibt es auch eine **Softwaregruppe**. Die Gruppennummer ist Teil des **Nachrichtenpakets**, das für die Weiterleitung der Daten verwendet wird – ähnlich den TCP/IP-Paketen, die im Internet verwendet werden. Die Gruppe ist ein Byte des Pakets und reicht von **0 bis 255**.
- Damit zwei *micro:bits* miteinander kommunizieren können, müssen sie **denselben Kanal und dieselbe Gruppe** verwenden.
- Wenn eine Textnachricht in lesbaren Zeichen über Funk gesendet wird, wird sie als **Klartext** bezeichnet. Sie ist anfällig für das Abhören durch einen unsichtbaren Hacker, der denselben Funkkanal und dieselbe Gruppe abhört. Diese Art des Hackens wird als "Man-in-the-Middle-Angriff" bezeichnet.

Was werden Sie tun?

1. Organisieren Sie Ihr Team:
    a. Arbeiten Sie in einer Gruppe mit mindestens zwei weiteren Personen, die jeweils einen Nspire CX II CAS-Taschenrechner und einen *micro:bit* besitzen.
    b. Ihr Lehrer wird Ihrer Gruppe eine Funkkanalnummer zuweisen. Ändern Sie die Gruppennummer nicht.
    c. Jedes Gruppenmitglied wählt eine Rolle: Sender-, Empfänger- oder Hackerrolle.
    d. Öffnen Sie die Datei *CyberSecurity – Klartext.tns*

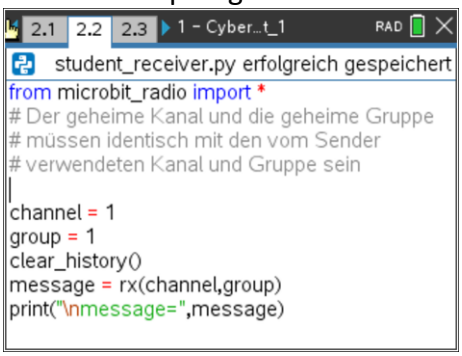
2. Senden Sie eine Textnachricht:
    - Der *Empfänger*
        - wählt die Dateiseite '**student_receiver.py**', ändert den Kanal auf die zugewiesene Nummer und startet das Programm, **bevor** der *Sender* sein Programm ausgeführt hat.
    - Der *Sender*
        - wählt die Dateiseite "**student_sender.py"**, ändert den Kanal auf die zugewiesene Nummer, bearbeitet die Nachrichtenzeichenfolge und führt dann sein Programm aus**, nachdem** der *Empfänger* und der *Hacker* ihre Programme gestartet haben.

- Der *Hacker*
  - wählt die Dateiseite "**student_hacker.py**", ändert den Kanal auf die zugewiesene Nummer und startet das Programm**, bevor** der *Sender* sein Programm ausgeführt hat.
- Nachdem Ihr Team die Aktivität durchgeführt hat, ändert der *Sender* sein Programm auf eine andere Kanalnummer (0-83) und eine separate Nachricht. Dann flüstert der *Sender* dem *Empfänger* den neuen Kanal zu. Aber sagen Sie es dem *Hacker* nicht; **behalten Sie die neue Kanalnummer für sich**! Führen Sie dann die Aktivität erneut durch. Erhält der *Hacker* die neue Nachricht? Können Sie erklären, warum?

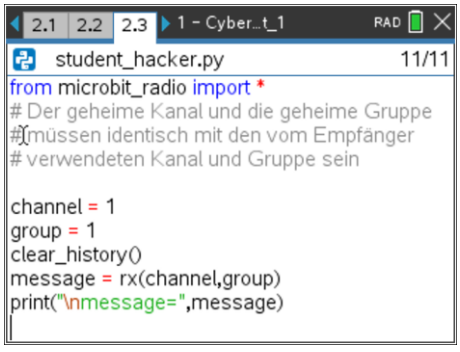
Die Programme

Rolle des Senders

Rolle des Empfängers



Rolle des Hackers



Weitere Übungen

- Probieren Sie eine andere Rolle in Ihrer Gruppe aus.
- Nehmen Sie eine weitere Gruppe von Schülern auf und erstellen Sie einen Großgruppentext.
- Versuchen Sie die Aktivität mit der gleichen Kanalnummer, aber einer anderen Gruppennummer.

Prüfen Sie Ihr Verständnis

- Der *Empfänger* muss zuhören, bevor der *Sender* die Nachricht sendet.
- Eine Funkmeldung kann auf einer beliebigen Kombination der 84 Funkkanäle oder 256 Funkgruppen des *micro:bit* gesendet werden.
- Damit mehrere *micro:bits* miteinander kommunizieren können, müssen sie sich auf demselben Kanal und in derselben Gruppe befinden.
- Nachrichten, die im Klartext über einen bekannten Kanal und eine bekannte Gruppe gesendet werden, können leicht gehackt werden.
- Die Verwendung eines geheimen Kanals oder einer geheimen Gruppe kann helfen, Hackerangriffe zu verhindern.

Hilfe

- Vergewissern Sie sich, dass alle Mitglieder der Gruppe den gleichen Kanal und die gleiche Gruppennummer haben.
- Stellen Sie sicher, dass der *Empfänger* und der *Hacker* ihre Programme gestartet haben und warten Sie, bis der *Sender* die Nachricht übertragen hat.