

How it works

- Radio waves are electromagnetic radiation, like light, but with a lower frequency. All electromagnetic radiation travels at the speed of light, 3.0×10^8 m/s. Radio waves can travel short or long distances depending on the electrical power of the radio transmitter. The micro:bit's can travel about 70 meters in clear space. Look on the back of your micro:bit card, in the upper left corner. Can you find the radio's gold antenna? This is where the radio waves go in and out of the card.
- The micro:bit radio emits and receives radio waves with frequencies ranging from 2402 - 2486 megahertz; this range is called the radio's spectrum, and the micro:bit's is divided into 1 MHz wide bands called **channels**. There are **84** different radio channels, ranging from 0 to 83, on the micro:bit. Two or more micro:bits must share the same channel to communicate.
- Text messages are added to radio waves in digital modulation. Text messages are inserted into a **packet**, including additional information needed for routing and error checking.
- In addition to the micro:bit radio channels, there is also a software **group**. The group number is part of the message **packet** used to route the data, similar to TCP/IP packets used on The Internet. The group is one byte of the packet and ranges from **0 – 255**.
- For two radios to communicate, they must share **the same channel and group**.
- When a text message in readable characters is sent over the radio, it is called **cleartext**. It is vulnerable to eavesdropping by an unseen hacker listening on the same radio channel and group. This type of hacking is called a "man-in-the-middle attack."

What will you do?

1. Organize your team:
 - a. Work in a team with at least two others, each with an Nspire CX II calculator and micro:bit.
 - b. Your teacher will assign your team a radio channel number. Do not change the group number.
 - c. Each group member chooses a sender, receiver, or hacker role.
2. Send a text message:
 - The **receiver**
 - will advance to '**student_receiver.py**,' change the channel to your assigned number, and run the program **before** the sender has run theirs.
 - The **sender**
 - will advance to the '**student_sender.py**,' edit the message string, change the channel to your assigned number, and then run your program **after** the receiver and hacker have started theirs.
 - The **hacker**
 - will advance to '**student_hacker.py**,' change the channel to your assigned number, and run the program **before** the sender has run theirs.
 - After your team runs the activity, the sender should change their program to a different channel number (0-83) and also change their message. The sender should whisper the new channel to the receiver, who should then change their program to the same channel number. Don't tell the hacker; **keep it private!** Then, rerun the activity. Does the hacker get the new message? Can you explain why?

Code it

Sender role

```
1.1 1.2 2.1 1 - Cyber...ear RAD 10/11
from microbit_radio import *
# The secret channel and group must be the
# same as the receiver.

channel = 1
group = 1
message = "The gold is hidden in the cookie jar!"
clear_history()
print("\nmessage=",message)
tx(message,channel,group)
```

Receiver role

```
1.2 2.1 2.2 1 - Cyber...ear RAD 9/10
from microbit_radio import *
# The secret channel and group must be the
# same as the sender.

channel = 1
group = 1
clear_history()
message = rx(channel,group)
print("\nmessage=",message)
```

Hacker role

```
2.1 2.2 2.3 1 - Cyber...ear RAD 9/10
from microbit_radio import *
# The secret channel and group must be the
# same as the sender.

channel = 1
group = 1
clear_history()
message = rx(channel,group)
print("\nmessage=",message)
```

Go further

- Try a different role in your group.
- Include another group of students and make a large group text.
- Try the activity with the same channel number but a different group number.

Check your understanding

- The receiver must be listening before the sender transmits the message.
- A radio message can be sent on any combination of the micro:bit's 84 radio channels or 256 radio groups.
- For micro:bits to communicate, they must be on the same channel and group.
- Messages sent in cleartext over a known channel and group can be hacked.
- Using a secret channel or group can help to prevent hacking.

Help

- Check that everyone in the group is on the same channel and group numbers.
- Ensure the receiver and hacker run their programs and wait before the sender transmits the message.