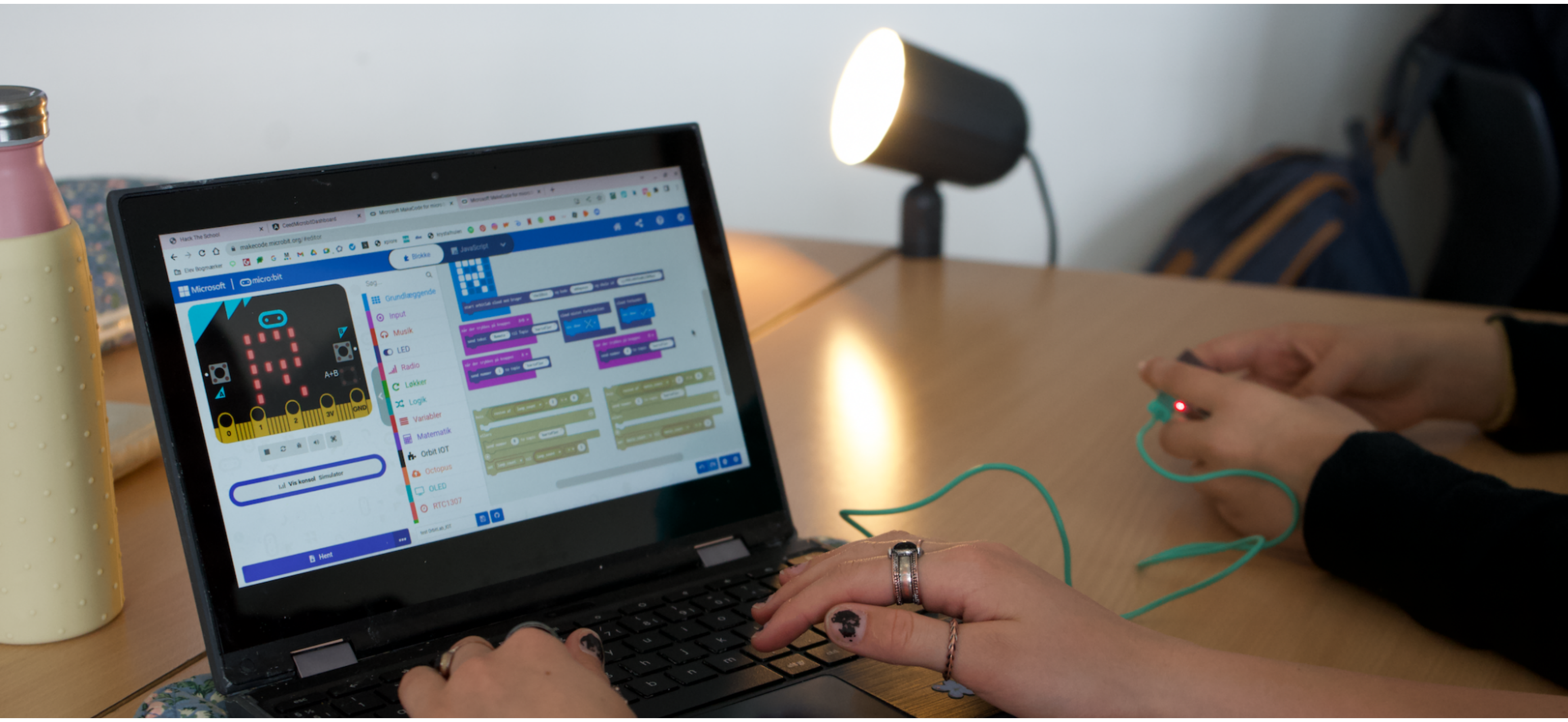
CEED Project | Aarhus University

TEACHER'S GUIDE

Pranking with IoT: Hack or be hacked?

A guide to facilitate a course in lower secondary school about the technical and societal aspects on Internet of Things



Indholdsfortegnelse

Introduction to the teacher guide

Brief course description

Pranking with IoT is a course that gives students the opportunity to gain first-hand experience with the Internet of Things and with hacking.

Using the IoT kit, students set up their own system to turn on/off a device such as a lamp, fan or speaker through the Internet. Once their IoT system is set up and tested, the students will hack their classmates' IoT systems, and/or devices in the teacher's room.

An integral part of the course is the discussions and reflections on the societal and ethical aspects of IoT and hacking.

The starting narrative of the course

The course starts with a message from a fictional 9th grad student who has been experimenting with hacking devices at the school. The student has discovered a way to hack the devices in the teachers' room in order to prank the teachers and invite other students to do the same in their schools.

The course framing

Target group: 7th–9th grade (ages 13–15 years)

Time spent: 7–8 lessons (We recommend these be scheduled in two half-day blocks)

Organization: Students should work on the tasks in groups of 2-3 students

The course assignments

The course encompasses student assignments which the hacker has developed to give the students the opportunity to learn step-by-step how to hack the teacher's room.

Assignment 1 contains activities for the students to set up their own IoT kit, program and test it, and finally to see how data from all the students' kits is collected on the dashboard. Part one does not include hacking assignments, but is intended to give students the knowledge and hands-on experience with IoT that will later enable them to hack.

Assignment 2 contains assignments for the students to hack each other's IoT devices and unmask each other's channel names. The students then learn to program Micro:bits so as to protect themselves against hacking by others.

Assignment 3 contains an assignment for students to hack various IoT devices implanted in the teacher's room

Assignment 1-3: Every stage of the course includes questions to frame class discussions and reflections on the ethical and societal impact of IoT and hacking.

Course resources

Online-materials

Below mentioned online-materials is used in the course:

- Website with teaching materials
    - Teacher guide (this document)
    - Student assignments
    - Slide presentation for teaching template
    - Programs as hex-filer for MakeCode
        - Microbit Hex Files (Assignment 1A/3A)
        - Crypto Hex Files (Assignment 2B)
- ORBIT Cloud Dashboard
- MakeCode

The slide presentation is a template to use in the classroom. It contains presentations and guidance for each assignment, as well as questions for class discussion as an integral part of the teaching.

Equipment required for the course (or borrowed from Aarhus University)

The course requires the following equipment for each IoT kit:

- 2 micro:bits
- 2 IoT boards (+ connection to the Internet/school network)
- 2 power banks
- 1 relay
- 1 resistor
- 1 micro-USB cable

Beside the equipment you will need access to view the data collection on the ORBIT Cloud dashboard. You can enter the dashboard website with a username and password from Aarhus University. Just write an email to vielandt@cc.au.dk (Ane Vielandt) and you will receive the needed information.

Equipment required in the school

- Computers
- Electrical devices (220V) (lamps, fans, speakers, etc.)

Course prerequisites

Familiarity - Micro:bit og MakeCode

The course requires students to have previous experience with Micro:bits and programming in Makecode for Micro:bit.

It is also an advantage for students to have experience with radio communication (Bluetooth) to send and receive information between Micro:bits.

Network

The IoT kit requires internet access. If it is not possible to connect to the school wifi, it will be necessary to set up another network for the students to gain internet access.

In order for the IoT boards to connect to the Internet, you will need a username, password and school ID from Aarhus University. The students need to insert this information in the programs in Makecode for Micro:bit. The information will be sent to you if you write an email to vielandt@cc.au.dk (Ane Vielandt).

To ensure the connection can be made, networks may need to be set up in both the classroom and the staffroom.

The two predefined programs for Makecode contain code blocks that enable the students to see whether the IoT boards are connected to the network. The displays on the Micro:bits will show an ╳ if there is no wifi connection and a “T” (for transmitter) or a “R” (for receiver) if the wifi connection is established. Be patient – it can take a little time for the IoT boards to connect to the wifi.

Alternative versions of the course

We recommend that teachers complete all the course assignments with the students to achieve the best learning outcomes, that is, for the students to gain knowledge and competencies in all the learning objectives (Full course). However, it is also possible for teachers to choose two different versions with fewer selected assignments. The table below shows the alternative versions to choose between, each of which has a specific learning focus from the programme. Please note that the introductory text message from the hacker does not make sense if students are not going to hack the teacher's room.

Version 1 **(3-4 lessons)**	**Version 2** **(2-3 lessons)**
Content	
Course introduction ● ONLY the introduction to hacking and types of hackers (slide 5-13) Assembling the IoT kits Assignment 1 - How does IoT work? ● 1A - IoT programming and testing ● 1B - IoT data collection Assignment 2 - Hack or be hacked? ● 2A - Hack your classmates **In this version the students only hack each other's IoT systems - not the teacher's room**	Assembling the IoT kits Assignment 1 - How does IoT work? ● 1A - IoT programming and testing ● 1B - IoT data collection
Specific learning focus	
The learning objectives for version 1 are almost identical with the objectives for the full course (see next page) The learning objectives on understanding and using encryption are not included in this version	The learning objectives for version 2 focuses on the technical aspects of IoT ● How does IoT work? ● Strength and weaknesses in IoT

Learning objectives

The learning objectives are defined by the experimental Danish school subject technology comprehension, a three-year pilot project trialed in Danish schools by the Danish Education Ministry. This course focuses on two of the four main competence areas of the project: computational empowerment and technological capability.

Digital myndiggørelse

- Students will learn to critically reflect on the impact of digital artifacts for the individual, community, and society
- Students will gain knowledge about the significance and impact of digital artifacts for the individual, community, and society
- Students will gain knowledge about the opportunities of acting in regard to the impact of digital artifacts for society

Technological skills

- Students will be able to read and understand programs written in a text-based programming language and will be able to use such a language to systematically modify and construct programs based on a specific problem

Færdigheds- og vidensmålene fra faget konkretiseres i nedenstående læringsmål.

General learning goals

1. Students will gain an understanding of the working of data flow in an Internet of Things system
2. Students will reflect on the impact of the Internet of Things for individuals and for society
3. Students will reflect on what hacking is, and will gain knowledge of various types of hackers
4. Students will reflect on the societal implications of hacking IoT systems
5. Students will be able to understand and use simple encryption to protect an IoT system against hacking

Course introduction

Specific learning goals

- To reflect on what hacking is, and gain knowledge of various types of hackers

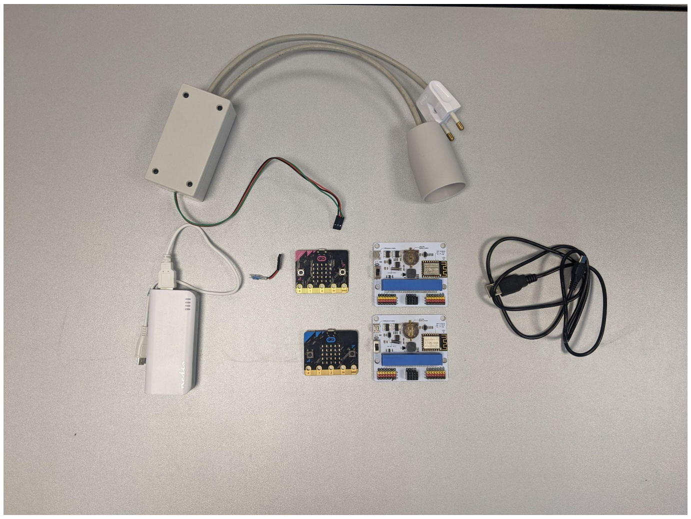
Activities (20 minutes)

1. Start by showing and reading the text message from the hacker (slide 3). The message is from a fictional student in 9th grade at the school who has discovered how to hack the teachers' room. The message is a frame and storyline for the course. The hacker has created the assignments as a guide so the students can try out IoT hacking for themselves.

2. Class discussion based on the following questions: (slide 4)
    a. What is a hacker?
    b. What kinds of hacking are there?
    c. Can hacking be used for good causes? What kind of good causes?
    d. Have you ever been hacked?

3. Show the slides 5-13 on hacking and on kinds of hackers from the teaching presentation. This will give them an introduction to hacking and the kinds of hacking that take place.

Assemble the IoT-kits



Learning objective

- To be able to set up the hardware in an IoT system in order to control devices through the Internet

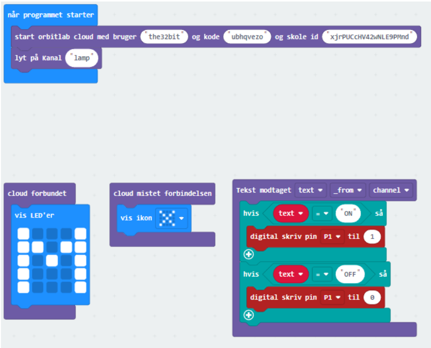
Activities (20 minutes)

1. Give every pair of students an IoT kit and an IoT device. Let them use the pictures in the student assignment or on slide 14-18. Alternatively, you can assemble the IoT kits with the students.

2. Introduce the students to the concepts: transmitter–receiver and relay

Assignment I - How does IoT work?

Assignment IA - IoT programming and testing



```
når programmet starter
  start orbitlab cloud med bruger "the32bit" og kode "ubhqvezo" og skole id "xjrPUCcHV42wNLE9PMnd"
  lyt på Kanal "lamp"

cloud forbundet
  vis LED'er

cloud mistet forbindelsen
  vis ikon

Tekst modtaget text _from channel
  hvis text = "ON" så
    digital skriv pin P1 til 1
  hvis text = "OFF" så
    digital skriv pin P1 til 0
```

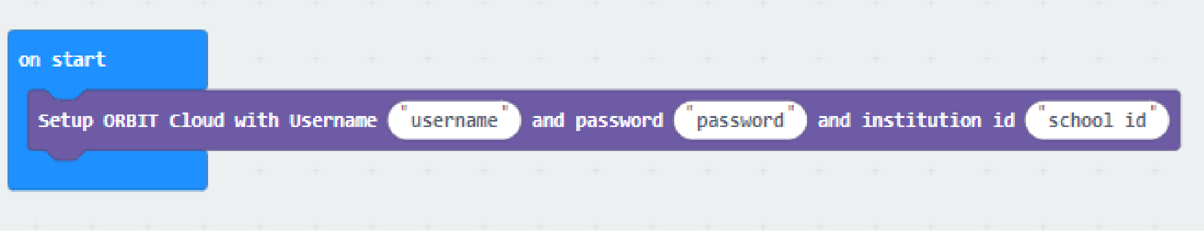
Learning objective

- To be able to program an IoT system in order to control devices through the Internet

Activities (45 minutes)

1. The students should download the programs for the transmitter micro:bit and receiver micro:bit from the website. They should import these programs into Makecode for Micro:bits. It can be a good idea to review the programs with the students to be sure they understand the function of the various code blocks in the programs. (slide 19-20).

   Important: Hand out username, password and school ID for the students to write into the code block as seen below (more information - see resources)

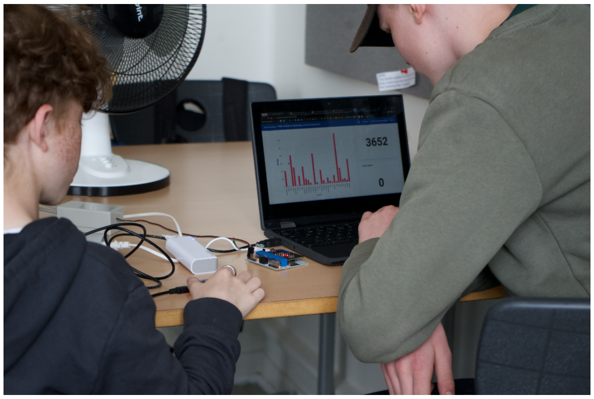


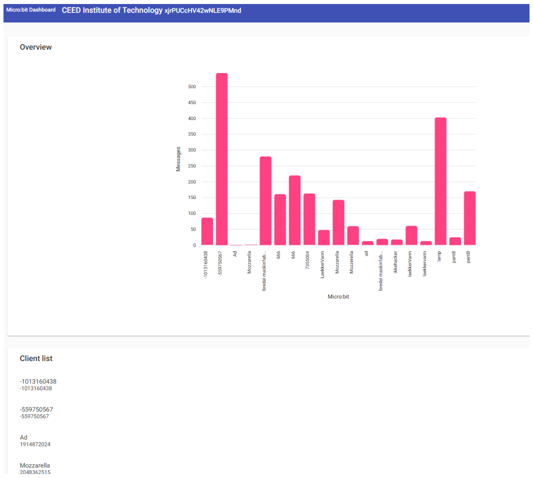
```
on start
  Setup ORBIT Cloud with Username "username" and password "password" and institution id "school id"
```

2. The students should now download the two programs to the transmitter micro:bit and the receive micro:bit. They should download the file "receiver.hex" to the receiver micro:bit, and the file "transmitter.hex" to the transmitter micro:bit.

3. The students should test whether they can turn their IoT device on and off with their transmitter.

Assignment 1B - IoT data collection




Micro:bit Dashboard CEED Institute of Technology xjrPUCcHV42wNLE9PMnd

Overview

Client list

-1013160438
-1013160438

-559750567
-559750567

Ad
1914872024

Mozzarella
2048362515

Learning objectives

- To read and interpret the data flow in an IoT system
- To be able to explain how an IoT system works
- To reflect on the significance and impact that an IoT system can have for individuals and society

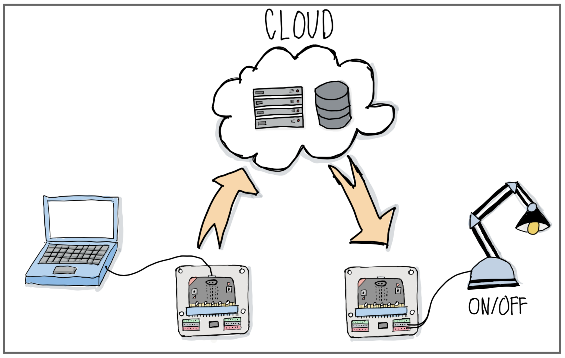
Activities (45 minutes)

1. Introduce the students to the ORBIT Cloud dashboard. They will require a username and password from you (more information - see resources). (Slide 21-22)
   - All student groups should use the channel name "lamp." This is predefined in both the receiver and the transmitter program. All student groups are therefore sending data to the dashboard on the channel "lamp."
   - The bar chart shows the sum of all the messages sent to the dashboard every time the students turn their IoT devices on and off.
   - If the students click on a channel name (below the bar chart), they will be able to see that the texts ON and OFF are sent every time they turn their IoT device on and off

2. The students should now change their channel name both in the receiver and the transmitter program. Each student pair should now have their own channel for sending data to the dashboard. To do this, they will need to change the name in the code block "channel name" and then download the programs again to the two Micro:bits. (slide 23)

- Important! Student pairs should not tell others their new channel name.
- It may be a good idea to tell the students to choose simple channel names that are easy for everyone to spell. (Avoiding tricky channel names that might prevent successful hacking)
- Have the student pairs check out how the data collection on their new channels changes on the dashboard.

3. Class discussion (slide 24)
   - Ask the students to explain how the Internet of Things works. They can use the illustration below as a starting point.



The Internet of Things describes devices that are connected to the Internet. Data is sent and received via built-in sensors. In this course, data is sent from the Micro:bit transmitter to a network server. The server then forwards the data to the Micro:bit receiver, which causes the IoT device to turn on and off.

- Ask the students to reflect on what IoT can, or should, be used for.

  Examples of IoT in use
  - A refrigerator connected to the internet that sends a message if the temperature gets too high/low
  - A washing machine connected to the internet that automatically turns on when power is cheapest
  - An electric car charger connected to the internet that only charges when the price of electricity is below a certain level

Assignment 2 - Hack or be hacked?

Assignment 2A - Hack your classmates

Learning objectives

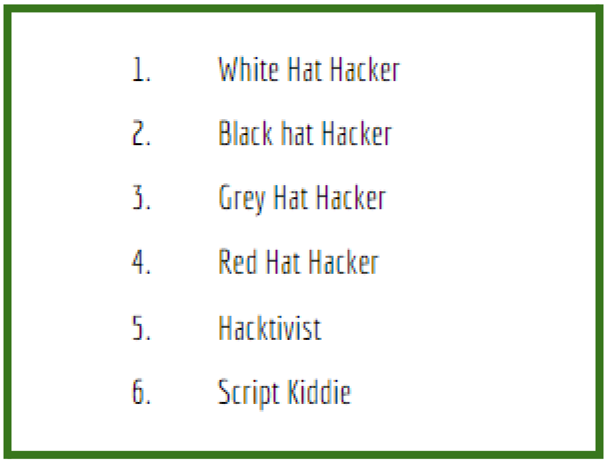
- To use data from an IoT system to hack and control other people's devices
- To reflect on the ethical implications of hacking other people's IoT systems

Activities (30 minutes)

1. The student pairs should now try to hack each other's IoT devices. For this assignment they will need only their transmitter micro:bit (slide 25-26). On the ORBIT Cloud dashboard, the student will be able to see each other's channel names. Each group chooses one of these channel names and writes it into their transmitter program in Makecode. Finally, they download the program to their transmitter micro:bit.

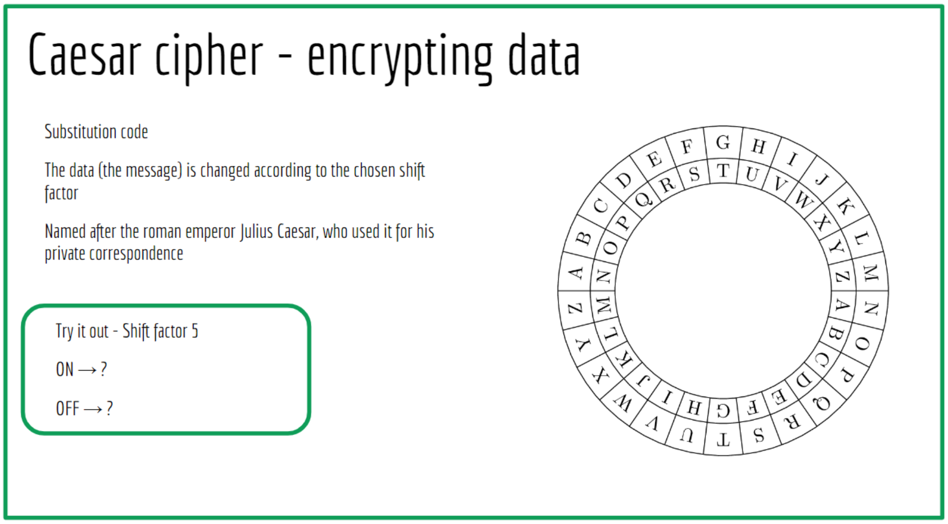
2. The assignment is for students to figure out which student pair they have hacked. They can do this by seeing which IoT device they are turning on and off with their transmitter. If time permits, they can try several different channel names to hack and reveal the identity of more student pairs.

3. Class discussion based on the following questions: (slide 27)
    - Were all the identities unmasked (If necessary, write the pairs' channel names on the board)
    - What kind of hackers are the students becoming when they are hacking each other's IoT devices? (see slides in the teaching presentation)
    - How does it feel to be hacked?
    - Do students have any ideas on how to avoid being hacked?
    - Could hacking an IoT device be used for a good cause?



1. White Hat Hacker
2. Black hat Hacker
3. Grey Hat Hacker
4. Red Hat Hacker
5. Hacktivist
6. Script Kiddie

Assignment 2B - Protect yourself from hacking



Caesar cipher - encrypting data

Substitution code

The data (the message) is changed according to the chosen shift factor

Named after the roman emperor Julius Caesar, who used it for his private correspondence

Try it out - Shift factor 5

ON → ?

OFF → ?

Learning objectives

- To be able to use simple encryption to protect an IoT system from hacking
- To gain knowledge on what it takes to hack past encryption in an IoT system
- To reflect on positive and negative implications by hacking an IoT system

Activities (45-60 minutter)

1. In this assignment the students should try to change their programs to make it harder for their classmates to hack them. For this they will need two new programs for the Micro:bit transmitter and receiver. They can download these from the website and import them to Makecode for Micro:bit (slide 28)

2. Start by explaining the Caesar cipher to the students (slide 29)

   The principle behind the protection in the two programs is a simple encryption of the data being sent in the IoT system. In this case we will be using the Caesar cipher. The encryption works through a substitution code in which each letter/number in the sent text is replaced by another letter/number, depending on the chosen 'shift factor.' This method is called after the Roman emperor Julius Caesar, who used this type of encryption for his private correspondence.

Example: With the shift factor 3, the text “ACD” becomes “DFG” when sent.

3. The student pairs now decide on a shift factor and write it into their transmitter and receiver program, then download the programs to their Micro:bits (slide 30)

   Important! Remind the students to change the channel name (chosen in assignment 2A) and change the username, password and school ID (as in assignment 1A)

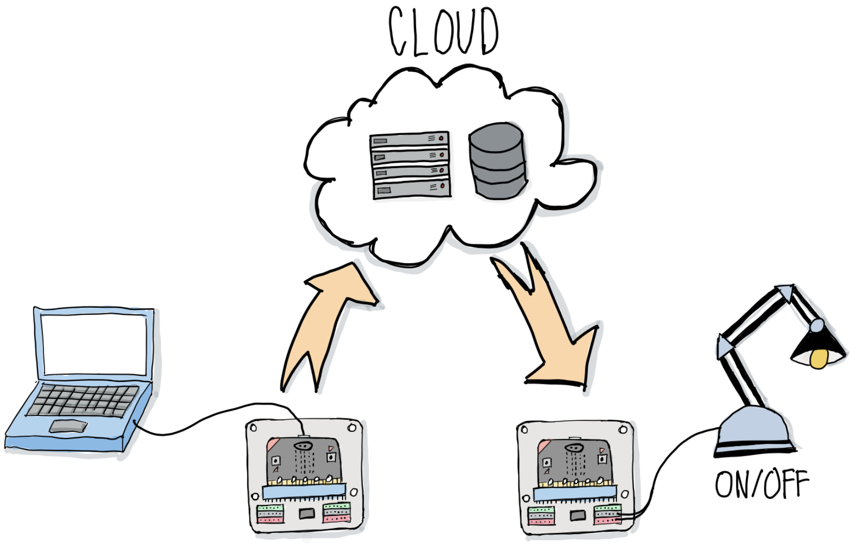
   Optional: Students who want a harder assignment can change the text ON and OFF in the programs to a different text.

4. The student pairs should now try to hack each other’s IoT devices once again (slide 31).

   The new method for hacking is:
   - Click on another student group's channel name on the ORBIT Cloud dashboard (below the bar graph)
   - Notice which two text messages are being sent
   - Work out what shift factor they are using, by counting how many shifts you can count back to ON and OFF. (Hint: The Caesar cipher wheel goes A–Z–a–z–1–9)
   - Insert the channel name of the target group and the shift factor into your transmitter program and download it to your transmitter micro:bit.
   - Turn the transmitterON and OFF to test whether you’ve hacked past the other team’s encryption

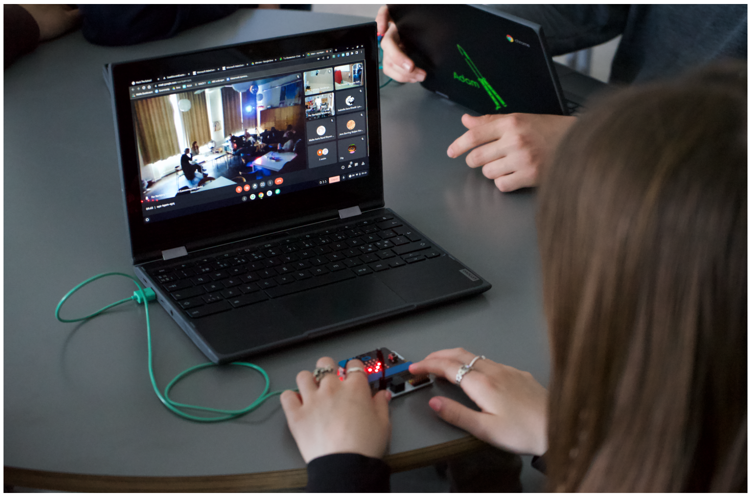
5. Class discussion (slide 32)
   - Did the students succeed in protecting themselves from being hacked?
   - Did the students succeed in hacking other student pairs despite the encryption?
   - In what situations could hacking be okay?

- Is it now possible to say anything in general about what needs to be done to prevent being hacked?
- Where in the IoT setup are there risks of being hacked?



Note: There is also a risk of being hacked as data is being sent to and from the server. In most cases the data would be encrypted, so it would not be easy for a potential hacker to make sense of the data. The server itself can also be hacked, and in such instances the data is often unencrypted. Hacking the server directly is therefore a much more attractive choice for the hacker.

Assignment 3 - Hack the teacher's room



Teacher preparation

For this assignment it is fun for the students to watch what is happening in the staffroom as they are hacking it. The easiest way for this is to set up a Teams meeting/Google Meet with a computer in the staffroom filming what happens, then show this on the classroom blackboard as a livestream.

Assignment 3A - Hack the teacher's room

Learning objective

- To experience and reflect on how hacking devices in a specific environment can affect individuals and community

Activities (45-60 minutter)

1. The student pairs choose the IoT device they will use to hack the teacher's room (slide 33)

2. They programme their transmitter and receiver Micro:bit (as in assignment 1A)

3. They take the receiver part of the IoT set up to the staffroom and set it up in the desired location (slide 34)

4. At teachers break time, the student pairs start hacking the IoT devices by turning the transmitter Micro:bit ON and OFF. They can follow the teachers' reactions in the staffroom on the blackboard showing the livestream

5. Classroom discussion (slide 35)
    - You have just hacked the staffroom as a practical joke on the teachers. Can you imagine hacking the staffroom to help the teachers, or make their job easier? How might you go about doing that?

Evaluation

Learning objective

- To be able to reflect and summarize your own learning processes and outcomes

Activities (45 minutter)

The formative assessment during the course is built into the classroom discussions and reflections guided by the course questions.

Additionally, after each assignment or as an overall evaluation at the end of the course, the students can make short videos to communicate the knowledge they have gained in the assignments. This could be framed as an assignment to send these videos to the hacker from the text message.

- Topics for the videos to contain could include: How does your IoT set up work, and what purposes can you use it for?
- What is hacking, and what kinds of hackers exist?
- How can you avoid being hacked?