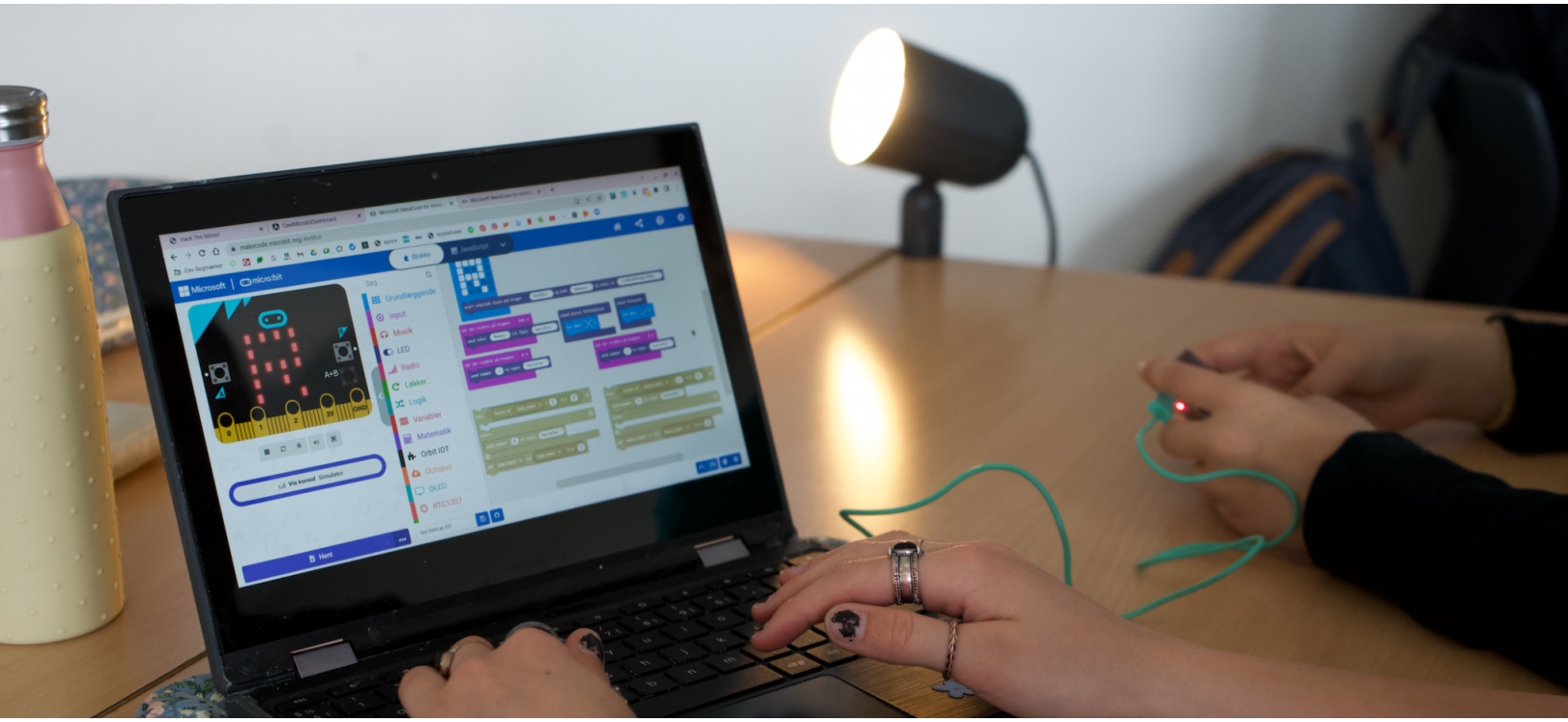
LÆRERVEJLEDNING

Pranking med IoT: Hack eller bliv hacket?

En guide til at facilitere et forløb i udskolingen om de tekniske og samfundsmæssige aspekter ved Internet of Things



Indholdsfortegnelse

Introduktion til lærervejledning

Kort beskrivelse af forløbet

Pranking med IoT er et forløb, hvor eleverne prøver kræfter med Internet of Things (IoT) og hacking af IoT.

Ved hjælp af et IoT Kit sætter eleverne selv et system op, hvor de kan tænde/slukke et 220V apparat (fx en lampe, en ventilator, en højtaler) fra en fjernbetjening. Når deres IoT system er opsat og testet, kan eleverne hacke henholdsvis deres klassekammeraters IoT-systemer og/eller apparater på skolens lærerværelse.

Forløbet har fokus på diskussioner og refleksioner over de tekniske og samfundsmæssige aspekter ved IoT og hacking.

Forløbets indledende fortælling

Forløbet indledes med en video/besked fra en fiktiv 9. klasses elev, der er hacker på elevernes egen skole. Eleven fortæller, at han har opdaget, hvordan man kan hacke apparaterne på skolens lærerværelse og derigennem "pranke" lærerne. Forløbet er derfor elevhackerens guide til andre elever, så de også kan prøve kræfter med at hacke 220 V apparaterne på lærerværelset.

Forløbets rammesætning

Målgruppe: 7.-9. klasse

Tidsforbrug:
7 - 8 lektioner (Forløbet passer bedst til en opdeling på to halve skoledage)

Organisering: Det fungerer bedst, hvis eleverne i grupper på 2-3 personer

Forløbets opgaver

Elevopgaverne indeholder en række opgaver, som hackeren har lavet, så eleverne lærer at hacke lærerværelset step-by-step.

Opgave 1 indeholder opgaver, hvor eleverne selv sætter et IoT kit op, programmerer og tester det og endelig ser, hvordan data fra de forskellige kits opsamles i Netværksovervågningen. Første del indeholder ikke opgaver omkring hacking, men skal give eleverne viden om og kendskab til IoT, der gør dem i stand til at hacke efterfølgende.

Opgave 2 indeholder opgaver, hvor eleverne forsøger at hacke hinandens IoT apparater og afslører hinandens identitet. Derefter arbejder eleverne med at beskytte dem selv mod hacking ved hjælp af programmering.

Opgave 3 indeholder opgaven, hvor eleverne skal hacke forskellige apparater på lærerværelset.

Opgave 1-3 indeholder alle spørgsmål til fælles klassesamtaler, der kan danne rammen om diskussioner og refleksioner over den samfundsmæssige betydning af IoT og konsekvenser ved hacking.

Forløbets ressourcer

Online-materialer

Nedenstående online-materialer anvendes i forløbet:

- Website med undervisningsmaterialet
  - Lærervejledning (dette dokument)
  - Elevopgaver
  - Slides til undervisningen_template
  - Programmer som hex-filer til MakeCode
    - Microbit Hex Filer (opgave 1A/3A)
    - Crypto Hex Filer (opgave 2B)
- ORBIT Cloud Netværksovervågning
- MakeCode

Slide-præsentationen er en template til brug i undervisningen, der indeholder præsentation og vejledning til de enkelte opgaver samt spørgsmål til de fælles klassesamtaler undervejs.

Udstyr fra Aarhus Universitet - ORBIT Lab

Forløbet kræver lån af hardware (et IoT kit). Udstyret skal hentes på Aarhus Universitet og kan lånes ved at sende en mail til vielandt@cc.au.dk (Ane Vielandt). IoT kittet indeholder:

- Micro:bits
- IoT boards
- Powerbanks
- Mobil bredbåndsrouter (adgang til Internet uden om skolens eget lukkede netværk)
- Relæ
- Modstandslus

Sammen med udstyret fra Aarhus Universitet - ORBIT Lab får I tilsendt et dokument på mail med bruger, kode og skole id, som eleverne skal bruge til programmerne i makecode. Derudover tilsendes også skolespecifik username og password til at logge ind og se dataindsamlingen i Netværksovervågningen.

Udstyr fra egen skole

Følgende udstyr er skolen selv ansvarlig for til forløbet:

- Computere
- Micro-USB kabler (til overførsel af programmer til Micro:bits)
- Elektriske 220V apparater (lamper, ventilatorer, højttalere, etc.)

Krav til forløbet

Kendskab til Micro:bit og MakeCode

Dette forløb kræver, at eleverne tidligere har arbejdet med Micro:bit og programmering i MakeCode til Micro:bit.

Det er en fordel, hvis eleverne tidligere har arbejdet med radiokommunikation - at sende og modtage informationer mellem Micro:bits.

Netværk

IoT kittet kan formodentlig ikke forbindes til skolens netværk. Det er derfor nødvendigt at opsætte et andet netværk til eleverne til forløbet. Med IoT udstyret får I derfor også udleveret et mobilt netværk, som skal opsættes inden for en rækkevidde, hvor elevernes IoT boards kan forbinde til det. Til opgave 3 (hacking af lærerværelset) vil det formodentlig være nødvendigt at sætte netværk op både i klasseværelset og i lærerværelset for at sikre, at forbindelsen kan oprettes. Her kan man anvende et mobilt hotspot fra egen telefon.

Forbindelse til mobilt netværk: I de forprogrammerede programmer til MakeCode (se ressourcer) er det programmeret, at Micro:bittens display viser, om der er forbindelse til netværk ved at vise enten et ╳, når den ikke er forbundet, eller et "S" (for sender) eller "M" (for modtager), når der er forbindelse. Det kan godt tage lidt tid at oprette forbindelse, så vær tålmodig.

Alternative versioner af forløbet

Vi anbefaler, at I laver alle opgaverne i forløbet sammen med eleverne for at få det optimale læringsudbytte. Men det er også muligt at gennemføre dele af forløbet ved kun at arbejde med udvalgte opgaver. I skemaet herunder ses to alternative versioner, der indeholder forskelligt fokus/læringsmål fra forløbet, som I kan vælge mellem. For begge versioner er gældende, at den indledende fortælling (video/besked) ikke skal inddrages.

Version 1 **(3-4 lektioner)**	**Version 2** **(2-3 lektioner)**
Indhold	
Indledning til forløbet ● KUN introduktion til hacking og hackertyper (slide 4-13) Opsætning af IoT kits Opgave 1 - Hvordan virker IoT? ● 1A - IoT programmering og afprøvning ● 1B - IoT dataopsamling Opgave 2 - Hack eller bliv hacket? ● 2A - Hack jeres klassekammerater **I denne version hacker elevernes kun hinandens IoT systemer - ikke lærerværelset**	Opsætning af IoT kits Opgave 1 - Hvordan virker IoT? ● 1A - IoT programmering og afprøvning ● 1B - IoT dataopsamling
Læringsfokus	
Læringsmålene for version 1 er stort set enslydende med målene for det fulde forløb (se “Mål med forløbet” i denne vejledning). Læringsmål omkring forståelse og anvendelse af kryptering er ikke inddraget i denne version	Læringsmålene for version 2 har fokus på de tekniske aspekter ved IoT: ● Hvordan virker IoT? ● Styrker og begrænsninger ved IoT

Mål med forløbet

Forløbet arbejder med målsætninger fra forsøgsfaget, teknologiforståelse med fokus på to kompetenceområder - digital myndiggørelse og teknologisk handleevne.

Digital myndiggørelse

- Eleven kan kritisk reflektere over digitale artefakters betydning for individ, fællesskaber og samfund
- Eleven har viden om digitale artefakters betydning for individ, fællesskaber og samfund
- Eleven har viden om egne handlemuligheder i forhold til digitale artefakters betydning i samfundet

Teknologisk handleevne

- Eleven kan læse og forstå programmer skrevet i et tekstbaseret programmeringssprog samt anvende et sådant til systematisk modifikation og konstruktion af programmer ud fra en problemspecifikation

Færdigheds- og vidensmålene fra faget konkretiseres i nedenstående læringsmål.

Læringsmål

1. Have viden om, hvordan dataflowet i et “Internet of Things” system virker
2. Reflektere over, hvilken betydning “Internet of Things” har for den enkelte og samfundet
3. Reflektere over, hvad hacking er og have viden om forskellige typer af hackere
4. Reflektere over de samfundsmæssige implikationer ved hacking af IoT systemer
5. At kunne forstå og anvende en simpel kryptering til at beskytte et IoT system mod hacking

Indledning til forløbet

Læringsmål

- at reflektere over, hvad hacking er og have viden om forskellige typer af hackere

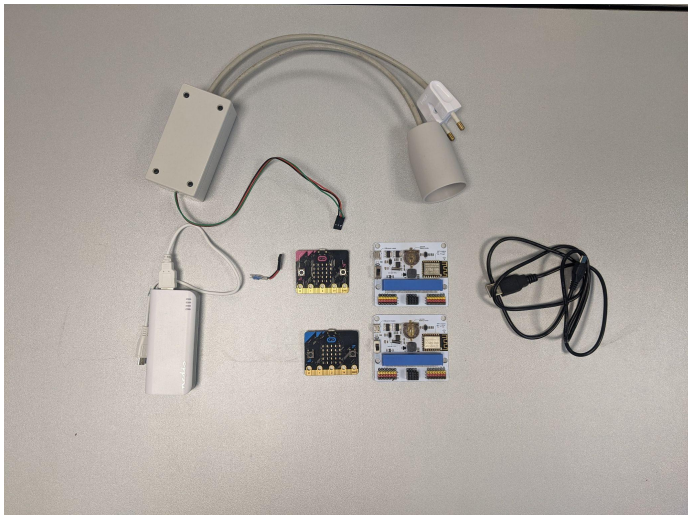
Aktiviteter (20 minutter)

1. Start forløbet med at vise eleverne videoen, "Hack The School" på youtube (slide 3). Videoen er fra en fiktiv elev på 9. årgang på skolen, som har opdaget, hvordan lærerværelset kan hackes. Videoen fungerer som rammesætning og igangsættende fortælling. Hackeren har skabt undervisningsmaterialet som en guide til dine elever, så de selv kan prøve at hacke. Videoen kan suppleres med den skriftlige besked fra hackeren (se elevopgaverne), der gentager en del af informationerne fra hackeren

2. Fælles klassesamtale ud fra spørgsmålene herunder: (slide 4)
    a. Hvad er en hacker?
    b. Hvilke former for hacking findes der?
    c. Kan hacking bruges til gode ting? Hvilke?
    d. Har I prøvet at blive hacket?

3. Vis eleverne slide 5-13, der gennemgår "Hacking og hacker-typer", så de får et yderligere indblik i, hvad hacking er, samt hvilke typer hackere, der findes

Opsætning af IoT-kits



Læringsmål

- at kunne opsætte hardware i et IoT system med henblik på at kontrollere elektriske apparater via Internettet

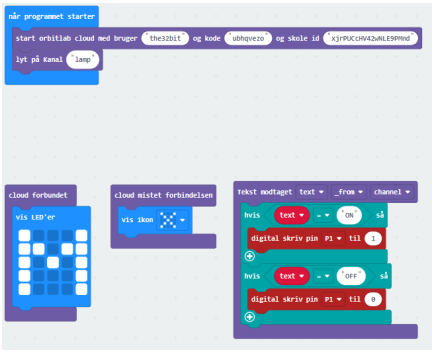
Aktiviteter (20 minutter)

1. Eleverne får udleveret IoT kits og IoT apparater i grupper og opsætter hardwaren. Der er fotos af opsætningen i elevopgaverne - alternativt kan I gøre det sammen med eleverne ud fra fotos i slide 14-18.

2. Introducer eleverne for begreberne: sender - modtager - relæ

Opgave 1 - Hvordan virker IoT?

Opgave IA - IoT programmering og afprøvning



Læringsmål

- at kunne programmere et IoT-system med henblik på at kontrollere elektriske apparater via Internettet

Aktiviteter (45 minutter)

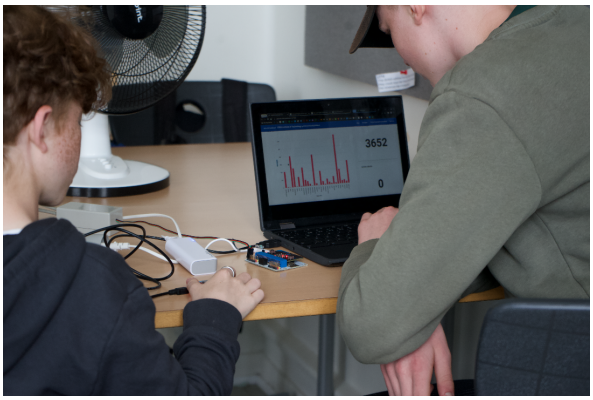
1. Eleverne downloader sender og modtager programmerne (hex.filerne) til deres computer. De åbnes begge i MakeCode til Micro:bit. Gennemgå evt. de to programmer med eleverne, så de forstår, hvad de forskellige kodeblokke gør (slide 19-20).

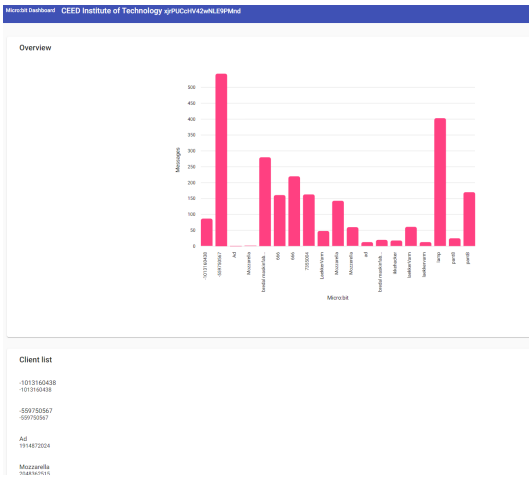
   Her udleveres bruger, kode og skole id, som skal skrives ind i programmerne (se ressourcer)

2. Programmerne downloades på henholdsvis sender og modtager Micro:bit i IoT kittet. Download modtager.hex til modtager Micro:bitten og sender.hex til sender Micro:bitten.

3. Eleverne afprøver nu, om de kan tænde og slukke deres apparat med senderen

Opgave 1B - IoT dataindsamling





Læringsmål

- at aflæse og forstå dataopsamlingen, når der sendes data i et IoT system
- at kunne forklare, hvordan et IoT system virker
- at reflektere over, hvilken betydning et IoT system kan/skal have for individ og samfund

Aktiviteter (45 minutter)

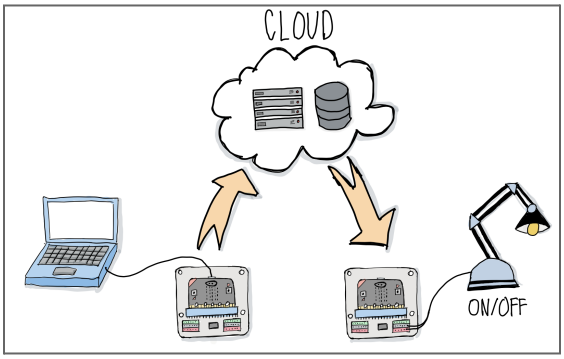
1. Introducer eleverne for dataindsamlingen på ORBIT Cloud Netværksovervågning. Her skal de have udleveret username og password (se ressourcer). (Slide 21-22)
    - Alle gruppers kanal-navn er “lamp” som er angivet i programmerne til sender og modtager. Hver gruppe har altså en kanal, der indsender data til Netværksovervågningen. Alle grupper sender derfor på samme kanal (“lamp”), der indsender data til dashboardet.
    - Søjlediagrammet viser, hvor mange gange, der er sendt en besked til Netværksovervågningen (hver gang eleverne tænder eller slukker deres apparat)
    - Hvis man “klikker” på en kanal (under søjlediagrammet), kan man se, at der bliver sendt 'ON' og 'OFF', når eleverne tænder og slukker deres apparat.

2. Eleverne skal nu ændre navnet på deres kanal i de to programmer, så de sender data til ORBIT Cloud Netværksovervågning med forskellige kanal-navne. Dvs. de steder i programmet, hvor der står “lamp” skal ændres til

et andet navn. Herefter downloades de nye programmer til de to Micro:bits (slide 23).

- VIGTIGT! Eleverne må ikke fortælle de andre gruppe, hvilket navn de vælger.
- Det kan være en fordel at bede grupperne om at vælge 'simple' navne, som er let for de andre at anvende (Så det ikke er svære kanalnavne, der forhindrer grupperne i at få succes med at hacke).
- Eleverne tjekker, hvordan dataindsamlingen ændrer sig på ORBIT Cloud Netværksovervågning med de nye kanal-navne.

3. Fælles klassesamtale (slide 24)
   - Bed eleverne om at forklare, hvordan IoT virker. De kan bruge illustrationen herunder som udgangspunkt.



Internet of Things beskriver apparater, der er koblet på Internettet. Via indbyggede sensorer sendes og modtages data. I dette forløb sendes data (ON/OFF) fra Micro:bit senderen til en netværksserver. Serveren videresender så dataen til Micro:bit modtageren, hvilket får IoT apparaterne til at tænde.

   - Hvad kan/skal vi bruge IoT til?
     Eksempler
     - Et køleskab forbundet til Internettet, der sender besked, hvis temperaturen er for høj/lav
     - En vaskemaskine forbundet til Internettet, der tænder automatisk, når strømmen er billigst
     - Ladestander til elbil forbundet til Internettet, som først lader, når prisen på el er under en bestemt pris

Opgave 2 - Hack eller bliv hacket?

Opgave 2A - Hack jeres klassekammerater

Læringsmål

- at anvende data fra et IoT system til at hacke sig ind på og styre andres elektriske apparater
- at reflektere over de samfundsmæssige implikationer ved at hacke andres IoT systemer

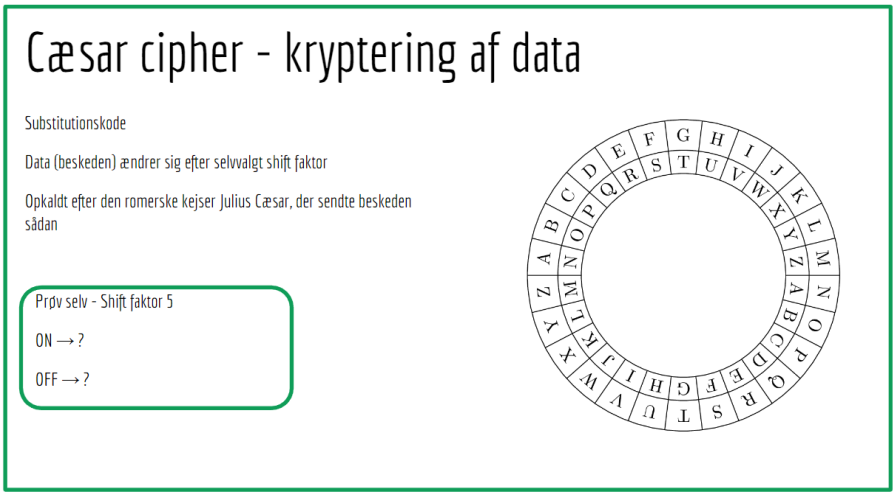
Aktiviteter (30 minutter)

1. Eleverne skal nu hacke hinandens IoT apparater. Til dette skal de kun arbejde med deres Micro:bit sender (slide 25-26).
   På Netværksovervågningen ORBIT Cloud Netværksovervågning kan eleverne se hinandens kanal-navne. Et af disse vælges og skrives ind kodeblokkene med "Kanal" i deres eget sender-program i MakeCode og downloades til deres Micro:bit sender.

2. Eleverne skal prøve at finde ud af, hvilken gruppe de har hacket med det nye kanal-navn. Det gør de ved at finde ud af, hvilket apparat de nu kan tænde og slukke med deres sender. De kan evt. prøve flere forskellige kanaler for at hacke og afsløre flere gruppers identitet.

3. Fælles klassesamtale ud fra spørgsmålene herunder: (slide 27)
    - Er alle gruppernes identitet afsløret? (Skriv evt. gruppernes kanal-navne på tavlen)
    - Hvilken type hacker er eleverne, når de hacker hinandens IoT apparater? (jf. slides fra undervisningen templates)
    - Hvordan var det at blive hacket?
    - Hvordan kan man mon undgå at blive hacket?
    - Hvordan kan man bruge hacking af et IoT system til noget positivt?

Opgave 2B - Beskyt jer mod hacking



Læringsmål

- at kunne anvende en simpel kryptering til at beskytte et IoT system mod hacking
- at få viden om, hvad det kræver at hacke forbi en kryptering af et IoT system
- at reflektere over positive og negative implikationer ved at hacke et IoT system

Aktiviteter (45-60 minutter)

1. Eleverne skal forsøge at ændre i deres programmer, så det bliver sværere for deres klassekammerater at hacke dem. Det kan de gøre ved at bruge crypto hex.filerne, som de importerer i MakeCode (slide 28).

2. Forklar eleverne Cæsar Cipher (slide 29).

   Princippet bag beskyttelsen i de to programmer er en simpel kryptering af den data, der bliver sendt i IoT systemet. Dette kalder Cæsar cipher. Krypteringen fungerer gennem en substitutionskode, hvor hvert bogstav i den sendte tekst erstattes af et andet bogstav i alfabetet efter en udvalgt "shift factor". Metoden er opkaldt efter Julius Cæsar, som brugte denne form for

kryptering i sin private korrespondance

Eksempel: Med en valgt shift factor på 3 bliver teksten “ACD” til “DFG”

3. Eleverne skriver nu en shift faktor ind i deres eget sender- og modtagerprogram og downloader dem på de to Micro:bits (slide 30).

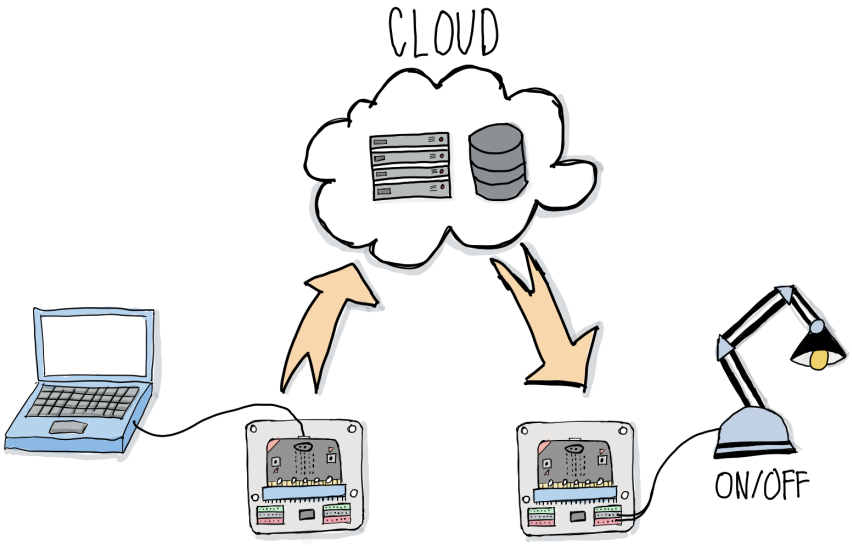
   HUSK! Eleverne skal også skrive deres eget kanalnavn, som de valgte i opgave 2A ind samt ændre bruger, kode og skole id (som i opgave 1A).

   EKSTRA: For ekstra sværhedsgrad kan eleverne kan også ændre ON og OFF i programmerne til en anden tekst.

4. Eleverne forsøger nu igen at hacke en anden gruppes IoT apparat (slide 31). Metoden til at hacke er
   - Eleverne klikker ind på en anden gruppes kanal på netværksovervågningen
   - De ser, hvilke to tekstbeskeder gruppen sender
   - De regner ud, hvilken shift-faktor gruppen har brugt ved at tælle, hvor mange shifts, der er tilbage til ON og OFF. (HJÆLP: Cæsar cipher hjulet går fra A-Z-a-z-1-9)
   - De skriver gruppens kanal-navn i sender-programmet og indtaster deres shift-faktor
   - De prøver at sende og ser, om de har hacket sig forbi krypteringen.

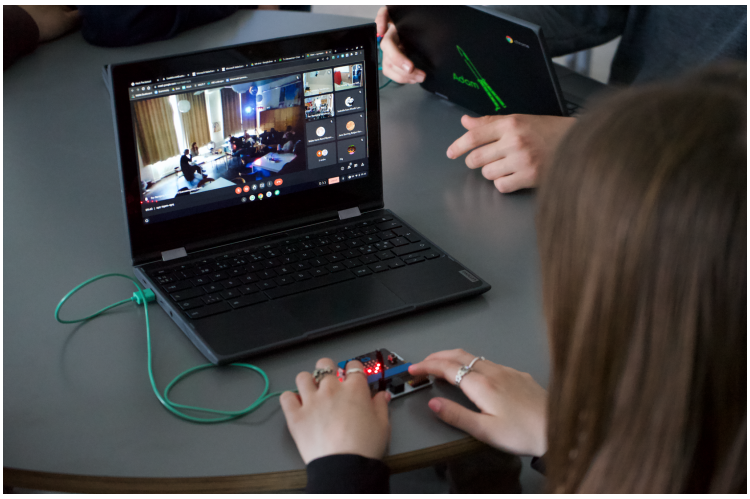
5. Fælles klassesamtale (slide 32)
   - Lykkedes det at undgå at blive hacket?
   - I hvilke situationer kan det være okay at hacke?
   - Lykkedes det at hacke nogen?
   - Kan vi nu sige noget om, hvad der generelt er vigtigt for at undgå at blive hacket?

- Hvor i IoT setuppet er der risiko for at blive hacket?



Der er risiko for hacking, når data bliver sendt til og fra serveren. Her vil den dog i langt de fleste tilfælde være krypteret, så en eventuel hacker vil have svært ved at få noget ud af dataen. Selve serveren kan også hackes, og her vil data ofte være ukrypteret. Derfor er det mere attraktivt for en hacker at hacke serveren.

Opgave 3 - Hack lærerværelset



Lærerens forberedelse

Det er sjovest, hvis eleverne kan følge med i, hvad der sker på lærerværelset, mens de hacker det. Den nemmeste måde er at sætte fx et teamsmøde eller et google meet op, hvor en computer i lærerværelset filmer, hvad der sker, og det vises på tavlen i klasseværelset.

Opgave 3A - Hack lærerværelset

Læringsmål

- at erfare og reflektere over, hvordan hacking af elektriske apparater i et specifikt miljø kan påvirke individer og fællesskab

Aktiviteter (45-60 minutter)

1. Eleverne vælger nu et IoT apparat, som de vil hacke lærerværelset med (slide 33)

2. De programmerer sender og modtager Micro:bit i makecode som i Opgave 1A

3. Modtager-delen sættes op, som de gerne vil have det i lærerværelset (slide 34)

4. Når lærerne pause starter, begynder eleverne at hacke deres IoT apparater og kan følge med på tavlen, hvad der foregår på lærerværelset

5. Fælles klassesamtale (slide 35)
    - I har lige hacket lærerværelset for at “pranke” lærerne. Kan I forestille jer at hacke lærerværelset hjælpe lærerne eller gøre deres arbejde nemmere? Hvordan?

Evaluering

Læringsmål

- at kunne opsummere egen læring

Aktiviteter (45 minutter)

Den løbende evaluering i forløbet foregår særligt i de diskussioner og refleksioner, som eleverne har i forbindelse med de fælles klassesamtaler.

Derudover kan eleverne undervejs i forløbet efter hver opgave eller som afsluttende evaluering på forløbet kan eleverne lave små video-klip, hvor de kommunikerer viden fra opgaverne. Det kan eventuelt italesættes sådan, at de skal sende deres klip til hackeren fra intro-videoen.

Videoerne kan f.eks. indeholde viden om:

- Hvordan virker dit IoT system, og hvad kan man bruge det til?
- Hvad er hacking og hvilke typer hackere findes der?
- Hvordan kan man undgå at blive hacket?