

1STEM@BAVO

CODEREN – DECODEREN



2017, Sint-Bavohumaniora, Reep 4, 9000 Gent

Auteurs: N. Gesquière, J. Colson, B. Declercq, N. Van den Borre, C. De Sutter

Bronnen:

CS Unplugged, Tim Bell, Ian H. Witten en Mike Fellows, Bewerking voor onderwijs door Robyn Adams en Jane McKenzie; www.csunplugged.org

Wikipedia

Dit werk valt onder een Creative Commons-licentie.



De gebruiker mag

- * het werk kopiëren, verspreiden en doorgeven
- * remixen, afgeleide werken maken

Onder de volgende voorwaarden:

- **Naamsvermelding:** De gebruiker dient steeds de auteurs van het werk en Sint-Bavohumaniora te vermelden, een link naar de licentie te plaatsen en aan te geven of het werk veranderd is. De gebruiker mag dat op redelijke wijze doen, maar niet zodanig dat de indruk gewekt wordt dat de auteurs of Sint-Bavohumaniora instemmen met zijn werk of zijn gebruik van het werk.
- **Niet-commercieel:** De gebruiker mag het werk niet gebruiken voor commerciële doeleinden.
- **Gelijk delen:** Indien de gebruiker het werk bewerkt of op het werk heeft voortgebouwd, moet de gebruiker het veranderde materiaal verspreiden onder dezelfde of een gelijksoortige licentie als het originele werk.

INHOUDSTAFEL

1	Communicatie.....	5
1.1	Communicatiemiddel.....	5
1.2	Morsecode	6
2	Inleiding DwenguinoBlockly	9
2.1	Stappenplan om DwenguinoBlockly2.0 te openen	9
2.2	De basisblokken	9
2.3	Opslaan van DwenguinoBlockly2.0-bestanden	9
2.4	Uploaden naar Dwenguino-bordje	9
2.5	Uitbreidingsblokken	10
2.5.1	Lcd-scherm.....	10
2.5.2	Scherm leegmaken	10
2.5.3	Knoppen.....	10
2.5.4	Leds.....	11
2.5.5	Vertraging oproepen	11
2.5.6	Buzzer.....	11
2.5.7	Keuzestructuur.....	12
3	Morsecode met DwenguinoBlockly2.0	13
3.1	Leds laten oplichten door gebruik drukknoppen	13
3.1.1	DwenguinoBlockly2.0	13
3.1.2	Arduino	14
3.2	Boodschap vermelden en laten verdwijnen.....	15
3.2.1	DwenguinoBlockly2.0	15
3.2.2	Arduino	15
3.3	Zoemer/buzzer laten werken.....	16
3.3.1	DwenguinoBlockly2.0	16
3.3.2	Arduino	16
3.4	Morsecode-programma.....	17
3.4.1	DwenguinoBlockly2.0	17
3.4.2	Arduino	18
4	Van spreekbuis tot draadtelefoon.....	19
4.1	De spreekbuis	19
4.2	De blikjestelefoon – onderzoekend leren.....	20
4.2.1	O.....	20
4.2.2	V.....	20
4.2.3	U.....	21
4.2.4	R.....	21
5	Binaire getallen	23
5.1	Kaarten-methode	23
5.2	Bits en bytes.....	24
6	De ASCII-code	25
6.1	Van toetsaanslag naar binaire code.....	25
6.2	Tekst in binaire ascii-code.....	26
6.3	Binaire codes lezen, bewerken en opslaan	27
6.4	Gegevensuitwisseling tussen computers	29

7	Gegevensoverdracht - Pixels tekenen.....	31
7.1	<i>Introductie.....</i>	<i>31</i>
7.2	<i>Oefening: werken met pixels.....</i>	<i>31</i>
7.2.1	Opdracht 1	31
7.2.2	Opdracht 2: Maak de pixeltekening aan de hand van de code (Bron: CS Unplugged).....	32
7.2.3	Opdracht 3: Schrijf nu zelf de code bij deze pixeltekening!	33
7.3	<i>Waar gaat dit eigenlijk over?.....</i>	<i>33</i>
8	Controlegetallen (Bron: CS Unplugged)	34
8.1	<i>Introductie.....</i>	<i>34</i>
8.2	<i>Demonstratie: de "Magische Truc"</i>	<i>34</i>
8.3	<i>Waar gaat dit eigenlijk over?.....</i>	<i>34</i>
8.4	<i>Voorbeelden:</i>	<i>35</i>
8.4.1	Streepjescode	35
8.4.2	ISBN-nummer (Internationaal Standaard Boek Nummer)	36
8.4.3	Bankrekeningnummer	36
9	Caesarcijfer	37
9.1	<i>Codeervoorbeeld via Excel en codeerring</i>	<i>37</i>
9.2	<i>Decodeer.....</i>	<i>38</i>
9.3	<i>Decodeer in Python.....</i>	<i>38</i>
9.3.1	Wat is een string?.....	38
9.3.2	Bewerkingen op een String	38
9.3.3	Codes voor karakters: ord, chr	38
9.3.4	Uitgewerkt programma.....	39
9.4	<i>Voor de Bad Guys werken.....</i>	<i>41</i>
9.4.1	Brute force	41
9.4.2	Letterfrequentie-analyse.....	42
10	In de pers	43
10.1	<i>E-loket</i>	<i>43</i>
10.2	<i>FBI opent nieuw onderzoek naar e-mails</i>	<i>45</i>
	Bronvermelding afbeeldingen en artikels	46

1 COMMUNICATIE

1.1 COMMUNICATIEMIDDEL

Leerlingen luisteren naar volgende fragment:

https://upload.wikimedia.org/wikipedia/commons/e/e2/Morse_code.ogg

of

https://www.youtube.com/watch?v=u20sVtCxf_8

Hoe noem je deze code?

.....

Bedenk verschillende manieren om een codesignaal te versturen:

-
-
-
-
-

Kan je voorbeelden geven waar dit vroeger gebruikt werd?

-
 -
 -
 -
-

Waarom was dit vroeger succesvol?

.....

.....

.....

Wanneer wordt dit nu nog gebruikt?

Lichamelijk gehandicapten geven een morsecode in op een computer via zuigen en blazen op een rietje. Via een *voice box*¹ wordt het bericht hoorbaar voor derden.

Door het worden de pieptonen of lichtflitsen een **communicatiemiddel**: zo ontstaat een informatiedrager om mee te communiceren.

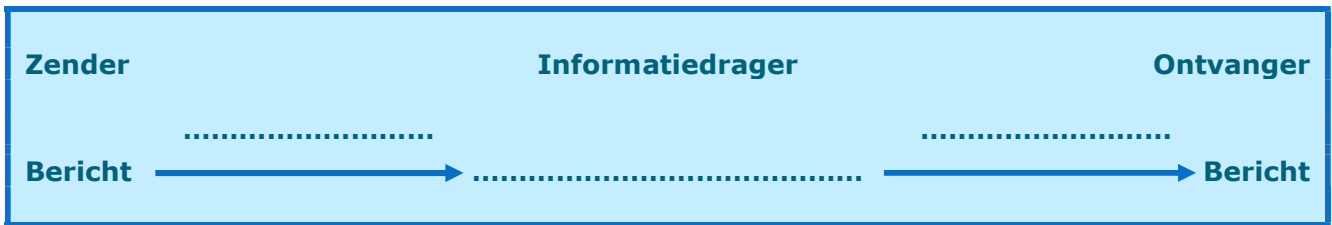
Geef andere vormen van communicatiemiddelen:

.....

.....

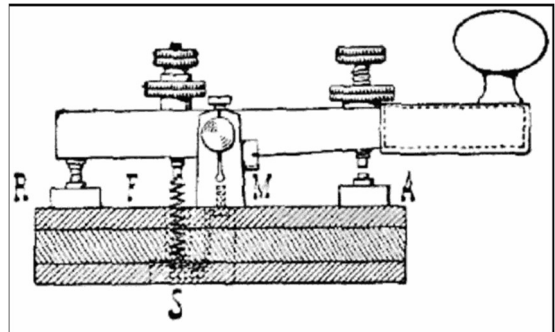
.....

¹ Toestel die code omzet in gesproken taal (te vergelijken met de stem van een gps-toestel).



1.2 MORSECODE

Morse is een **communicatiecode**, bestaande uit met tussenpozen uitgezonden signalen, die letters, leestekens en cijfers vertegenwoordigen. De code werd in 1835 uitgevonden en ontwikkeld door Samuel Morse met het doel deze te gebruiken voor de telegrafie. Bij de telegraaf kon men alleen maar kiezen uit een tijdsduur (kort of lang) en twee toestanden: sleutel naar beneden (= stroom) of sleutel niet bediend (= geen stroom). Telegrafie wordt algemeen beschouwd als een voorloper van de latere digitale communicatie.



Morsesignalen kunnen op verschillende manieren verzonden worden als:

-
-
-



Meer en meer is kennis van het morse niet meer vereist om te werken in lucht- en scheepvaart. Het morse is vervangen door andere communicatiemethoden of wordt door technologie omgezet in verstaanbare taal. De aanwezigheid van morse-apparatuur is dan niet langer vereist. Een groot voordeel is dat men geen marconist (een persoon die is opgeleid in het zenden en ontvangen van morsecodesignalen) meer aan boord hoeft te hebben. Morse wordt wel nog gebruikt in de scheepvaart voor lichtmorsecommunicatie en bij radiozendamateurs.

Maar morsecode is zeker nog niet afgeschreven!

Op 15 juli 2017 publiceerde "The Office of Naval Research TechSolutions" volgend YouTube bericht:

<https://youtu.be/8dpdBPylOLA>

Hierin zie je hoe het onderzoekscentrum het "Flashing Light to Text Converter"-project (FLTC) ondersteunt. In de bestaande seininstallatie op een schip wordt de lamp vervangen door een led-module die zowel de lichtmorsecommunicatie kan versturen als ontvangen. Via een tabletcomputer wordt met de gepaste software een chatsessie gestart tussen twee schepen.



Het morsealfabet:

<https://www.youtube.com/watch?v=EmXsSSHCnsI>

Letter	Morse	Letter	Morse	Cijfer	Morse
A	· —	N	— ·	0	— — — — —
B	— · · ·	O	— — —	1	· — — — —
C	— · — ·	P	· — — ·	2	· · — — —
D	— · ·	Q	— — · —	3	· · · — —
E	·	R	· — ·	4	· · · · —
F	· · — ·	S	· · ·	5	· · · · ·
G	— — ·	T	—	6	— · · · ·
H	· · · ·	U	· · —	7	— — · · ·
I	· ·	V	· · · —	8	— — — · ·
J	· — — —	W	· — —	9	— — — — ·
K	— · —	X	— · · —		
L	· — · ·	Y	— · — —		
M	— —	Z	— — · ·		

ii

Timing en codering:

Morse kent twee symbolen: punten en streepjes, ofwel *dits* en *dahs*.

De lengte van de '*dit*' (= punt) bepaalt de snelheid waarmee de boodschap wordt verzonden en wordt als 'eenheid' gebruikt.

Een *dah* (=streep) is volgens de afspraken drie keer zo lang als een dit.

Spaties tussen *dits* en *dahs* binnen een lettercode hebben de lengte van één dit.

Spaties tussen letters in een woord hebben de lengte van 3 *dits*, en spaties tussen woorden zijn 7 *dits* lang.

Schrijf je naam in morsecode:

Met de onderstaande tabel kunnen de meest gangbare morsecodes snel worden herleid tot de bijbehorende letter. Vooral handig bij het 'ontsleutelen'.

E ·								T —							
I ·				A —				N ·				M —			
S ·		U —		R ·		W —		D ·		K —		G ·		O —	
H ·	V —	F ·	—	L ·	—	P ·	J —	B ·	X —	C ·	Y —	Z ·	Q —	·	—

iii

De volgende code

— — — — · · · · · / — · · — — — — · · ·

wordt als volgt gelezen:

DahDah DahDahDah DiDahDit DiDiDit Dit, DahDiDahDit DahDahDah DahDiDit Dit

Een streep wordt altijd als *dah* gelezen. Een punt in een lettercode als *di* en op het einde *dit*.

Via volgende website kan je een tekst laten omzetten in een morsecode:

<https://morsecode.scphillips.com/translator.html>

Antwoord met één woord: "Wat vind je van dit STEM-project?"

Woord:

Zet dit om in morsecode:

Zit er een systeem in de manier waarop het alfabet is gecodeerd?

.....

.....

.....

Als je een codelengte van max 4 dits/dahs gebruikt voor de letters, hoeveel verschillende letters kan je dan coderen?

.....

.....

.....

Welke morsecode zou je zeker uit het hoofd moeten kennen?

.....

2 INLEIDING DWENGUINOBLOCKLY

2.1 STAPPENPLAN OM DWENGUINOBLOCKLY2.0 TE OPENEN


- 1 Dubbelklik op de snelkoppeling van Arduino op je bureaublad.
- 2 Klik in de menubalk op "Hulpmiddelen".
- 3 Klik op "DwenguinoBlockly2.0"

2.2 DE BASISBLOKKEN

Als je DwenguinoBlockly2.0 opent, dan verschijnt de basisstructuur onmiddellijk in het rechterdeelvenster.



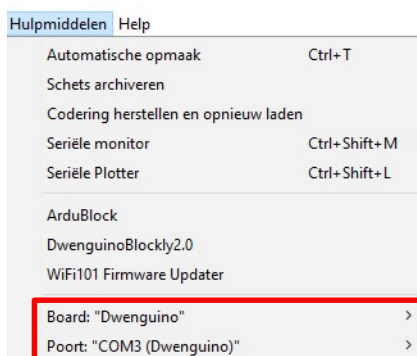
2.3 OPSLAAN VAN DWENGUINOBLOCKLY2.0-BESTANDEN


- 1 Klik bovenaan op het "Sla de blokken op naar een lokaal bestand"-icoontje. 
- 2 Kies de gewenste map.
- 3 Geef je bestand een correct gekozen naam.
- 4 (Je bestand krijgt .xml als extensie.)

2.4 UPLOADEN NAAR DWENGUINO-BORDJE

- 1 Verbind het Dwenguino-bordje met de USB-kabel met de computer.
- 2 Controleer of het bordje dat zal aangesproken wel het Dwenguino-bordje zal zijn. Klik hiervoor bij Arduino op "Hulpmiddelen" - "Board". Selecteer het correcte bordje.

Controleer ook of de poort waarop het Dwenguino-bordje moet aangesproken worden wel correct is. Klik hiervoor bij Arduino op "Hulpmiddelen" - "Poort". Selecteer de correcte poort.

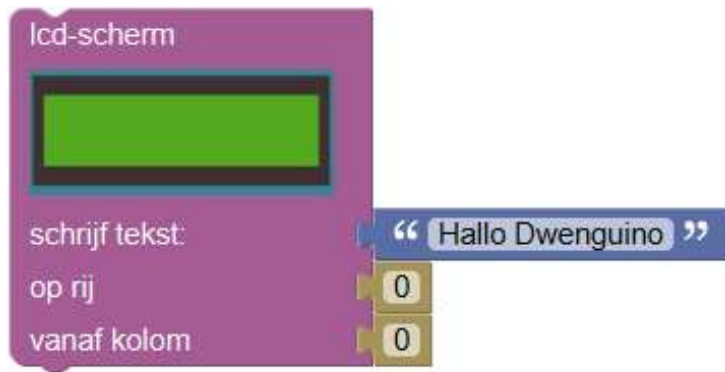


- 3 Klik bovenaan op het "play"-icoontje.
- 4 Je zal het bestand nog eens moeten opslaan als een Arduino-bestand.
- 5 Kies de gewenste map.
- 6 Geef je bestand een correct gekozen naam.
- 7 (Je bestand krijgt .ino als extensie.)
- 8 Nadat alles is geüpload, mag je de USB-kabel verwijderen.
- 9 (Een eerder gemaakt DwenguinoBlockly2.0-bestand opnieuw opvragen doe je met het "Laad een block-bestand in dat je eerder hebt opgeslagen"-icoontje.) 

2.5 UITBREIDINGSBLOKKEN

2.5.1 LCD-SCHERM

Om iets op het lcd-scherm te plaatsen, klik je in het linkerdeelvenster op **Dwenguino** en gebruik je:



De tekst 'Halo Dwenguino' kan je aanpassen. De twee nullen betekenen: eerste lijn, eerste karakter.

Verander je bij '**op rij:**' de 0 in een 1, dan komt je tekst op de tweede lijn.

2.5.2 SCHERM LEEGMAKEN

Om het lcd-scherm leeg te maken, moet je klikken in het linkerdeelvenster op **Dwenguino**. Daarna kies je voor: **maak lcd-scherm leeg**.

2.5.3 KNOPPEN

Gebruik maken van knoppen doe je met **lees waarde knop NOORD**. Klik hiervoor eerst in het linkerdeelvenster op **Dwenguino**.

Je kan de vijf knoppen aanspreken, door in het keuzemenu de gewenste optie te kiezen: NOORD, OOST, ZUID, WEST of CENTER.



- Noord = de bovenste knop
- Oost = de rechtse knop
- Zuid = de onderste knop
- West = de linkse knop
- Center = de centrale knop

Een knop die ingedrukt is, heeft de waarde 'LAAG', als ze niet ingedrukt is dan is het 'HOOG'.

Dit vind je in het linkerdeelvenster bij **Dwenguino** en dan **HOOG** (**NIET INGEDRUKT**) of **LAAG** (**INGEDRUKT**).

2.5.4 LEDS

Om leds te kunnen gebruiken, moet je in het linkerdeelvenster klikken op **Dwenguino**. Daarna kies je voor: **LED 0** of **leds 0b01010101**.

Gebruik je **leds 0b01010101** dan laat je de "0b" altijd staan. De acht bits die hierop volgen verwijzen naar de toestand van de overeenkomstige leds op het Dwenguino-bordje: **0** staat voor **led uit** en **1** staat voor **led aan**.

VOORBEELDEN:

- De eerste led (meest rechtse) moet branden = LD0
- De tweede led (tweede van rechts) moet branden = LD1
- De 1ste, 3de, 5de en 7de led moet branden

leds 0b00000001
leds 0b00000010
leds 0b01010101

2.5.5 VERTRAGING OPROEPEN

Om een vertraging op te roepen in je programma, moet je klikken in het linkerdeelvenster op **Dwenguino**. Daarna kies je voor: **wacht 100 ms**.

De 100 staat voor 100 milliseconden = 0,1 seconde.

Vertragingen in je programma roep je op door die 100 zo aan te passen dat je het gewenste aantal seconden vertraging hebt. Wil je dat het programma 2 seconden wacht, dan verander je dit in 2000 milliseconden.

2.5.6 BUZZER


Om de zoemer/buzzer te laten werken, klik je in het linkerdeelvenster op **Dwenguino**. Daarna kies je voor: **speel toon af op pin BUZZER met frequentie 440**.

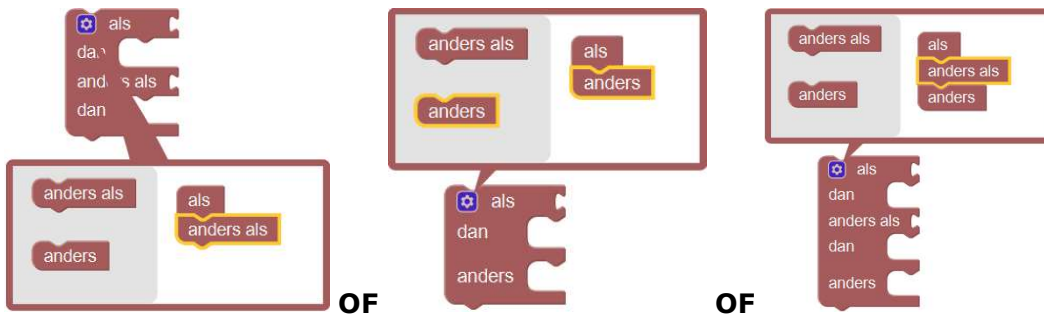
- Frequentie drukt uit hoe vaak iets gebeurt binnen een bepaalde tijd. Frequentie wordt uitgedrukt in Hertz (Hz).
Bijvoorbeeld: Een snaar van een gitaar trilt met een frequentie van 440 Hz. Dit betekent dat de snaar 440 keer trilt in 1 seconde.
- Met deze knop stel je de frequentie in van het geluid op de zoemer, m.a.w. de toonhoogte van dat geluid. Het gehoor van een kind kan geluidstrillingen horen met een maximale frequentie van 16 à 20 kHz. Bij ouderen is de bovengrens veel lager.


2.5.7 KEUZESTRUCTUUR

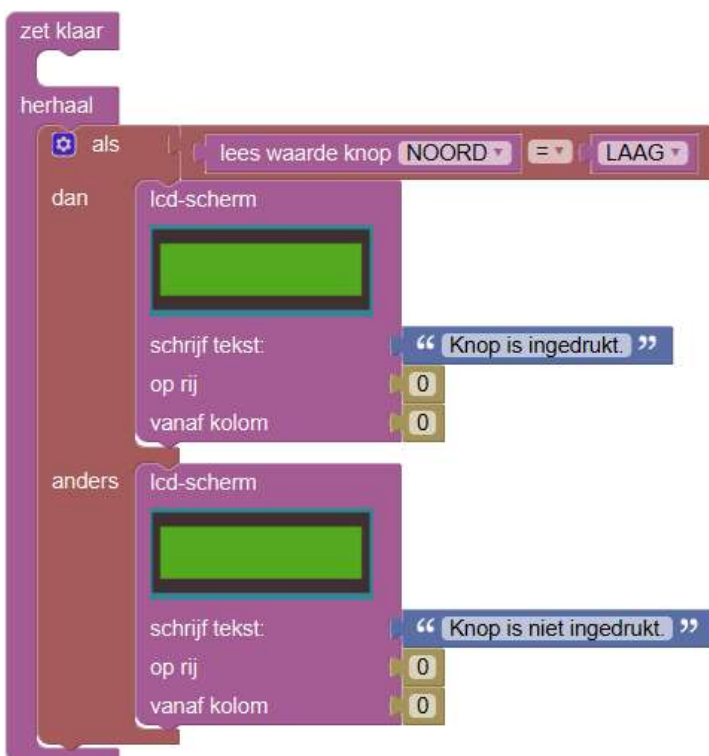
Om een keuzestructuur te gebruiken, klik je in het linkerdeelvenster op **Logica** en gebruik je:



Via  kan je deze structuur omvormen naar:



Om bijvoorbeeld te *controleren* of de Noord-knop is ingedrukt maak je gebruik van een vergelijksoperator. Klik in het linkerdeelvenster op **Logica** en gebruik: 

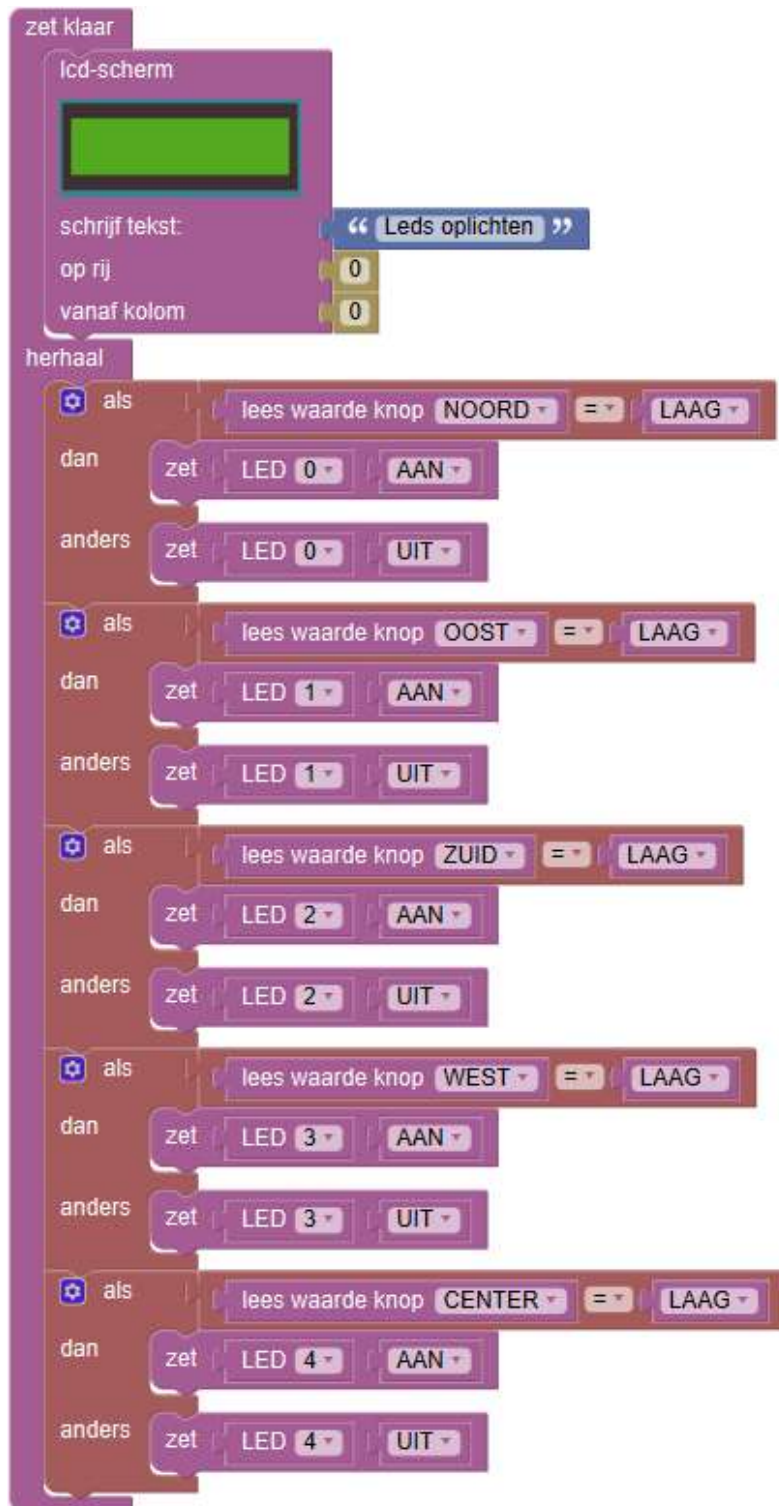


3 MORSECODE MET DWENGUINOBLOCKLY2.0

3.1 LEDS LATEN OPLICHTEN DOOR GEBRUIK DRUKKNOPPEN

Plaats de tekst "Leds oplichten" op het lcd-scherm. Laat telkens een andere led oplichten, als je op de N-knop, O-knop, Z-knop, W-knop of C-knop (center = midden) drukt. (N-knop led 0 (de meest rechtse led "LD0"), O-knop led 1 "LD1", Z-knop led 2 "LD2", W-knop led 3 "LD3" en C-knop led 4 "LD4").

3.1.1 DWENGUINOBLOCKLY2.0



3.1.2 ARDUINO

```
#include <Wire.h>

#include <Dwenguino.h>

#include <LiquidCrystal.h>

void setup()
{
  pinMode(32, OUTPUT);
  pinMode(33, OUTPUT);
  pinMode(34, OUTPUT);
  pinMode(35, OUTPUT);
  pinMode(36, OUTPUT);
  initDwenguino();
  dwenguinoLCD.setCursor(0,0);
  dwenguinoLCD.print(String("Leds oplichten"));
}

void loop()
{
  if (digitalRead(SW_N) == LOW) {
    digitalWrite(32, HIGH);

  } else {
    digitalWrite(32, LOW);
  }

  if (digitalRead(SW_E) == LOW) {
    digitalWrite(33, HIGH);

  } else {
    digitalWrite(33, LOW);
  }

  if (digitalRead(SW_S) == LOW) {
    digitalWrite(34, HIGH);

  } else {
    digitalWrite(34, LOW);
  }

  if (digitalRead(SW_W) == LOW) {
    digitalWrite(35, HIGH);

  } else {
    digitalWrite(35, LOW);
  }

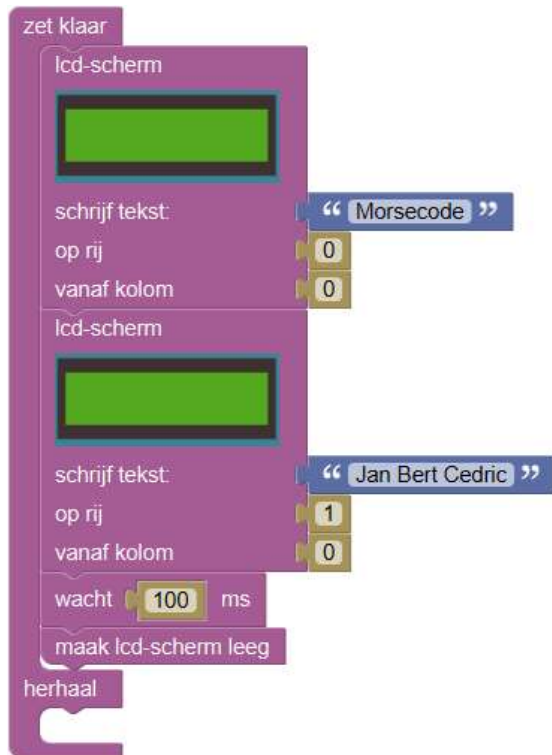
  if (digitalRead(SW_C) == LOW) {
    digitalWrite(36, HIGH);

  } else {
    digitalWrite(36, LOW);
  }
}
```

3.2 BOODSCHAP VERMELDEN EN LATEN VERDWIJNEN

Plaats de tekst "Morsecode" op de eerste lijn en je groepsnaam op de tweede lijn van het lcd-scherm. Laat deze tekst 2 seconden staan en laat hem dan verdwijnen.

3.2.1 DWENGUINOBLOCKLY2.0



3.2.2 ARDUINO

```
#include <Wire.h>

#include <Dwenguino.h>

#include <LiquidCrystal.h>

void setup()
{
  initDwenguino();
  dwenguinoLCD.setCursor(0,0);
  dwenguinoLCD.print(String("Morsecode"));
  dwenguinoLCD.setCursor(0,1);
  dwenguinoLCD.print(String("Jan Bert Cedric"));
  delay(100);
  dwenguinoLCD.clear();
}

void loop()
{
}
```

3.3 ZOEMER/BUZZER LATEN WERKEN

Laat de buzzer 1 seconde zoemen telkens als je op de West-knop drukt.

3.3.1 DWENGUINOBLOCKLY2.0



3.3.2 ARDUINO

```
#include <Wire.h>

#include <Dwenguino.h>

#include <LiquidCrystal.h>

void setup()
{
  pinMode(BUZZER, OUTPUT);
  initDwenguino();
}

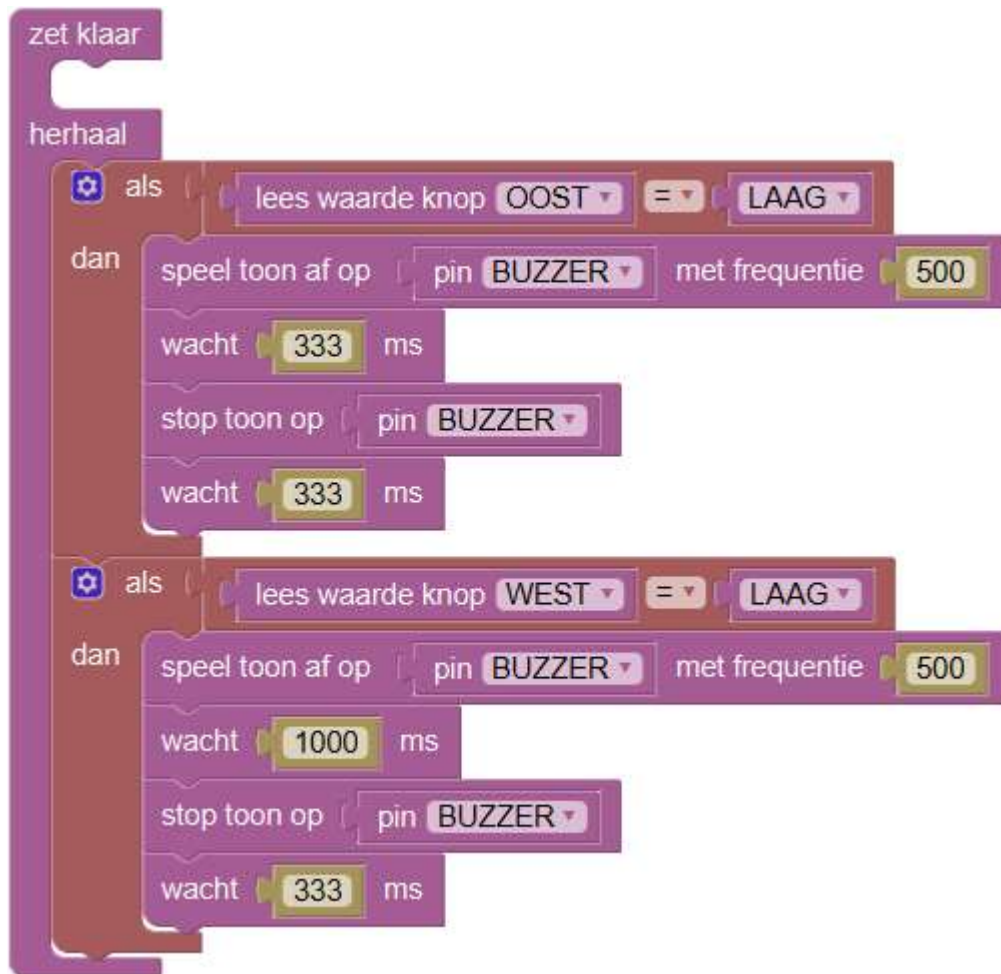
void loop()
{
  if (digitalRead(SW_W) == LOW) {
    tone(BUZZER, 440);
    delay(1000);
    noTone(BUZZER);
  }
}
```


3.4 MORSECODE-PROGRAMMA

Schrijf een programma zodat je met 2 verschillende drukknoppen een **dit** (SW_E) en **dah** (SW_W) signaal kan ingeven.

- De lengte van een **dit** is 333 milliseconden. De uitvoer is een toon van 500 Hz voortgebracht door de buzzer.
- De lengte van een **dah** is 1000 milliseconden. De uitvoer is een toon van 500 Hz voortgebracht door de buzzer.
- De pauze tussen twee signalen is de lengte van een **dit**.

3.4.1 DWENGUINOBLOCKLY2.0



3.4.2 ARDUINO

```
#include <Wire.h>

#include <Dwenguino.h>

#include <LiquidCrystal.h>

void setup()
{
  pinMode(BUZZER, OUTPUT);
  initDwenguino();
}

void loop()
{
  if (digitalRead(SW_E) == LOW) {
    tone(BUZZER, 500);
    delay(333);
    noTone(BUZZER);
    delay(333);
  }
  if (digitalRead(SW_W) == LOW) {
    tone(BUZZER, 500);
    delay(1000);
    noTone(BUZZER);
    delay(333);
  }
}
```

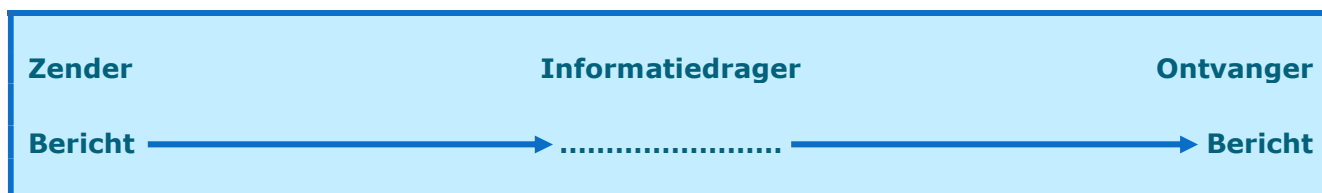
4 VAN SPREEKBUIS TOT DRAADTELEFOON

4.1 DE SPREEKBUIS

Als de gezagvoerder op een zeeschip aan de machinist wilde laten weten dat hij het toerental of de draairichting van de schroef moest aanpassen, kon hij de telegraaf gebruiken. Voor aanvullende informatie gebruikte hij een spreekbuis. Dat is een metalen buis waarmee werd van de brug naar machinekamer. Aan beide einden van de buis zit een mondstuk met daarin een fluit. De gezagvoerder nam de fluit uit het mondstuk en blies in de spreekbuis. In de machinekamer floot het fluitje, het werd uit de buis gehaald en de machinist hield zijn oor tegen de buis. De gezagvoerder riep dan in het mondstuk en zo was er communicatie tussen brug en machinekamer.

Door zijn eenvoud en het feit dat het werkte zonder elektriciteit, was de spreekbuis een betrouwbaar systeem dat communicatie over afstanden van tientallen meters in een lawaaijige omgeving mogelijk maakte.

De brug moet wettelijk een systeem hebben om te kunnen communiceren met de machinekamer en met de hut van de kapitein, onafhankelijk van de scheepsenergievoorziening. Vroeger gebeurde dit met de spreekbuizen. De spreekbuis is voor dit doel vervangen door een met een eigen accu als alternatieve energiebron. Of men gebruikt voorzien van een dynamo. Men dient het toestel zo'n 10 seconden op te winden totdat een luide zoemtoon klinkt en er een spreekverbinding tot stand is gebracht.



Bij de spreekbuis is er van de informatiedrager. De techniek bestaat erin dat de geluidsgolven in een metalen buis geleid worden van de ene ruimte naar een andere.

4.2 DE BLIKJESTELEFOON – ONDERZOEKEND LEREN

We kennen allemaal een blikjestelefoon.
Met twee blikken, twee spijkers en een lang touw kun je dit realiseren.
Je hebt ook een hamer en een schaar nodig om de klus te klaren.



Kun je dit proces in een schema
zender – informatiedrager – ontvanger plaatsen?

.....

.....

Je wil nu onderzoeken wat de invloed is van de draad of de blikken op de werking van jouw telefoon. Welke factoren spelen een rol?

.....

.....

Tijdens dit onderzoek werk je met de **OVUR-methode**. Deze methode bestaat uit 4 stappen die doorlopen worden om een kwalitatief onderzoek op te stellen en uit te voeren.

4.2.1 O.....

In deze fase ga je op zoek naar een probleemstelling en een goede onderzoeksvraag.

4.2.2 V.....

In deze fase bereid je je onderzoek voor.

STAP 1:

Brainstorm over een mogelijke werkwijze om de probleemstelling op te lossen met het verkregen materiaal. Noteer op het A3-blad.

- Wat weet je al?
- Wat wil je nog te weten komen?
- Welke onderzoekstechnieken bestaan hiervoor?
- Welke onderzoekstechniek kies je?

STAP 2:

Schrijf nu op de achterkant een werkwijze uit.

- Schrijf iedere handeling uit die je zult doen, met welk materiaal en de reden. STAPSGEWIJS
- Is het onderzoeksprobleem voldoende afgebakend, beperkt tot één probleem of parameter?
- Denk na over mogelijke invloedfactoren die de proef zullen beïnvloeden tijdens het uitvoeren.
- Denk na over een manier hoe je het aantal invloedfactoren kan minimaliseren.
- Wat ga je meten? Hoe ga je dit meten? Welke meetinstrumenten gebruik je?
- Wie doet wat? Uitvoeren, meten, noteren. Is er een beurtrol?
- Als je metingen doet, denk dan ook al na over een manier hoe je de gemeten waarden kan weergeven. Tabel, grafiek, een werkblad...?

Wanneer je denkt dat de werkwijze duidelijk op papier staat en alle stappen goed zijn uitgeschreven mag je bij de leerkracht gaan om feedback te vragen. Luister aandachtig naar de tips.

STAP 3:

Nu herwerk je de werkwijze aan de hand van de verkregen tips.

4.2.3 U.....

Je voert je stappenplan nauwkeurig uit en noteert je metingen.

Je houdt je aan de tijdsafspraken.

Formuleer nu een antwoord op de onderzoeksvraag.

.....

.....

4.2.4 R.....

Hoe goed voerde je deze delen van het onderzoek uit?

DENK NA OVER VOLGENDE VRAGEN:

- Heb je je doel bereikt?
- Wat is goed/fout gelopen?
- Wat kan er anders?
- Met welke invloedfactoren heb je geen rekening gehouden?
- Hoe zou je het onderzoek in de toekomst doen?

.....

.....

.....

.....

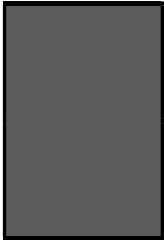
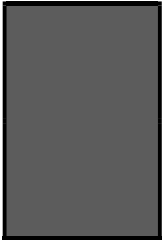
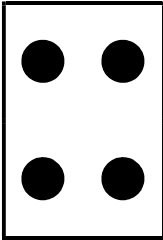
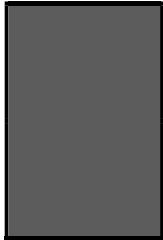
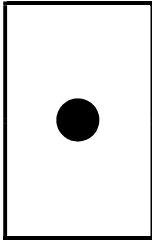
	Mvb	Zwak	Goed	Zeer goed
Samenwerking				
Volgen van het stappenplan				
Verwerken van de metingen				
Goed verwoorden van het antwoord op de onderzoeksvraag				

Moet veel beter	Zwak	Goed	Zeer goed
Ik hoor zelden waar de groep het over heeft.	Ik luister soms naar de inbreng van groepsgenoten.	Ik luister vaak naar de inbreng van groepsgenoten.	Ik luister aandachtig naar de inbreng van groepsgenoten.
Ik rem de groep af en stimuleer niet, maar verstoort.	Ik doe enkel iets als een ander dat vraagt. Ik stimuleer de anderen niet.	Ik neem initiatief, maar moet er soms toe aangezet worden. Ik stimuleer niet zoveel.	Ik neem vaak initiatief en stimuleer de anderen.
Ik voel me niet verantwoordelijk voor het resultaat van de groep.	Ik voel me pas verantwoordelijk voor het resultaat van de groep als iemand me daarop wijst.	Ik voel me vaak verantwoordelijk voor het resultaat van de groep.	Ik voel me zeer verantwoordelijk voor het resultaat van de groep.
De groep werkt chaotisch en houdt geen rekening met het stappenplan.	De groep heeft veel hulp nodig bij het volgen van het stappenplan.	De groep controleert regelmatig hoe het stappenplan vordert en heeft wat hulp nodig om bij te sturen als het fout loopt.	De groep controleert voortdurend hoe het stappenplan vordert en stuurt bij waar nodig.
Ik heb altijd hulp nodig bij het verwerken van de meetresultaten.	Ik heb veel hulp nodig bij het verwerken van de meetresultaten.	Ik kan de meetresultaten goed verwerken, maar heb wel wat hulp nodig.	Ik kan de meetresultaten goed en zelfstandig verwerken.
Het antwoord op de onderzoeksvraag is fout geformuleerd.	Het antwoord op de onderzoeksvraag is onnauwkeurig geformuleerd.	Het antwoord op de onderzoeksvraag is redelijk goed geformuleerd.	Het antwoord op de onderzoeksvraag is zorgvuldig geformuleerd.
Bij het formuleren van het antwoord werd niet gelet op de taal.	Bij het formuleren van het antwoord werd nauwelijks gelet op de taal.	Bij het formuleren van het antwoord werden slechts enkele taalfoutjes gemaakt.	Bij het formuleren van het antwoord werd ook de taal verzorgd.

5 BINAIRE GETALLEN








5.1 KAARTEN-METHODE








Het binaire systeem gebruikt en om weer te geven of een kaart is omgedraaid of niet. Nul betekent dat de kaart **omgekeerd** ligt en dus niet meegeteld wordt. Een één betekent dat je de stippen op de kaart ziet en deze wel gerekend worden. Om de waarde van een getal te kennen, tel je het aantal stippen dat je ziet. De eerste kaart ligt rechts en heeft 1 stip. Elke nieuwe kaart links van de vorige kaart bevat dubbel zoveel stippen als de vorige kaart.








						
Binaire code	0	0	1	0	1	= 5
Aantal stippen als macht 2	2⁴	2³	2²	2¹	2⁰	
Aantal stippen op de kaart	= 16	= 8	= 4	= 2	= 1	








Het binaire getal 00101 is dus gelijk aan het getal 5 in de decimale schrijfwijze.









Probeer deze gecodeerde getallen te ontcijferen:








1      =
( = 1,  = 0)

2      =
( = 1,  = 0)

3      =
( = 1,  = 0)

4      =
( = 1,  = 0)

5       =
( = 1,  = 0)

6      =
( = 1,  = 0)

- 7 $++\times+=$
 ($+= 1, \times = 0$)
- 8 $\cup\cup\cup\cup\cup=$
 ($\cup = 1, \cup = 0$)
- 9 $\blacktriangle\blacktriangledown\blacktriangle\blacktriangledown\blacktriangledown=$
 ($\blacktriangle = 1, \blacktriangledown = 0$)
- 10 $\spadesuit\heartsuit\spadesuit\heartsuit\spadesuit=$
 ($\spadesuit = 1, \heartsuit = 0$)

5.2 BITS EN BYTES

Elke kaart die tot nu toe werd gebruikt, stelt een '.....' voor op de computer ('bit' is een afkorting van '.....', binair cijfer of kleinste eenheid van data in een digitaal systeem; in het Engels).

In de informatica worden samen gelezen. Ze vormen ('byte' is een afkorting van 'by eight', per acht in het Engels). Een byte bestaat dus uit acht bits. Een byte is de eenheid van informatie.

Om een byte gemakkelijk te kunnen lezen is er een spatie tussen de 4^{de} en 5^{de} bit.

Schrijf rechts de decimale waarde van volgende binaire getallen:

0000 0000 =

0000 0001 =

0000 1000 =

0000 1111 =

0001 0000 =

1000 0000 =

Wat is het grootste binair getal dat we met 1 byte = 8 bits kunnen schrijven?

..... =

Als je bij 'gewone' getallen (= decimale getallen) rechts een 0 toevoegt, wordt het getal 10 keer zo groot. Bijvoorbeeld 9 wordt 90 en 30 wordt 300.

Maar wat gebeurt er als je een 0 achter een binair getal zet? Probeer dit eens:

1001 = 9

1 0010 =

Doe het met nog een aantal getallen om te zien of je idee klopt. Wat is de regel en waarom denk je dat dit gebeurt?

.....

.....

6 DE ASCII-CODE

6.1 VAN TOETSAANSLAG NAAR BINAIRE CODE

Kijk eens naar een toetsenbord en ga eens na hoeveel karakters een computer moet kunnen weergeven. Hoeveel bits moet je gebruiken om voor elk van deze karakters een code te kunnen toekennen?

Computers gebruiken allemaal het binaire systeem om informatie weer te geven. Het heet **binair** omdat er maar twee getallen worden gebruikt. Het wordt ook wel het **tweettallig stelsel** genoemd (in het dagelijks leven gebruiken we het decimale, tientallige stelsel). Elke **0 of 1** heet een **bit (binary digit)**

De meeste computers gebruiken tegenwoordig een weergave die (**American Standard Code for Information Interchange = Amerikaanse Standaard Code voor Informatie-uitwisseling**) heet. In deze tabel wordt aan elke letter of teken een unieke binaire code toegekend die één byte groot is. Deze code wordt door de computer in zijn binaire vorm gelezen, verwerkt en opgeslagen.

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	\$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

6.2 TEKST IN BINAIRE ASCII-CODE

Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	Char
0	0000 0000	00	[NUL]	32	0010 0000	20	space	64	0100 0000	40	@	96	0110 0000	60	`
1	0000 0001	01	[SOH]	33	0010 0001	21	!	65	0100 0001	41	A	97	0110 0001	61	a
2	0000 0010	02	[STX]	34	0010 0010	22	"	66	0100 0010	42	B	98	0110 0010	62	b
3	0000 0011	03	[ETX]	35	0010 0011	23	#	67	0100 0011	43	C	99	0110 0011	63	c
4	0000 0100	04	[EOT]	36	0010 0100	24	\$	68	0100 0100	44	D	100	0110 0100	64	d
5	0000 0101	05	[ENQ]	37	0010 0101	25	%	69	0100 0101	45	E	101	0110 0101	65	e
6	0000 0110	06	[ACK]	38	0010 0110	26	&	70	0100 0110	46	F	102	0110 0110	66	f
7	0000 0111	07	[BEL]	39	0010 0111	27	'	71	0100 0111	47	G	103	0110 0111	67	g
8	0000 1000	08	[BS]	40	0010 1000	28	(72	0100 1000	48	H	104	0110 1000	68	h
9	0000 1001	09	[TAB]	41	0010 1001	29)	73	0100 1001	49	I	105	0110 1001	69	i
10	0000 1010	0A	[LF]	42	0010 1010	2A	*	74	0100 1010	4A	J	106	0110 1010	6A	j
11	0000 1011	0B	[VT]	43	0010 1011	2B	+	75	0100 1011	4B	K	107	0110 1011	6B	k
12	0000 1100	0C	[FF]	44	0010 1100	2C	,	76	0100 1100	4C	L	108	0110 1100	6C	l
13	0000 1101	0D	[CR]	45	0010 1101	2D	-	77	0100 1101	4D	M	109	0110 1101	6D	m
14	0000 1110	0E	[SO]	46	0010 1110	2E	.	78	0100 1110	4E	N	110	0110 1110	6E	n
15	0000 1111	0F	[SI]	47	0010 1111	2F	/	79	0100 1111	4F	O	111	0110 1111	6F	o
16	0001 0000	10	[DLE]	48	0011 0000	30	0	80	0101 0000	50	P	112	0111 0000	70	p
17	0001 0001	11	[DC1]	49	0011 0001	31	1	81	0101 0001	51	Q	113	0111 0001	71	q
18	0001 0010	12	[DC2]	50	0011 0010	32	2	82	0101 0010	52	R	114	0111 0010	72	r
19	0001 0011	13	[DC3]	51	0011 0011	33	3	83	0101 0011	53	S	115	0111 0011	73	s
20	0001 0100	14	[DC4]	52	0011 0100	34	4	84	0101 0100	54	T	116	0111 0100	74	t
21	0001 0101	15	[NAK]	53	0011 0101	35	5	85	0101 0101	55	U	117	0111 0101	75	u
22	0001 0110	16	[SYN]	54	0011 0110	36	6	86	0101 0110	56	V	118	0111 0110	76	v
23	0001 0111	17	[ETB]	55	0011 0111	37	7	87	0101 0111	57	W	119	0111 0111	77	w
24	0001 1000	18	[CAN]	56	0011 1000	38	8	88	0101 1000	58	X	120	0111 1000	78	x
25	0001 1001	19	[EM]	57	0011 1001	39	9	89	0101 1001	59	Y	121	0111 1001	79	y
26	0001 1010	1A	[SUB]	58	0011 1010	3A	:	90	0101 1010	5A	Z	122	0111 1010	7A	z
27	0001 1011	1B	[ESC]	59	0011 1011	3B	;	91	0101 1011	5B	[123	0111 1011	7B	{
28	0001 1100	1C	[FS]	60	0011 1100	3C	<	92	0101 1100	5C	\	124	0111 1100	7C	
29	0001 1101	1D	[GS]	61	0011 1101	3D	=	93	0101 1101	5D]	125	0111 1101	7D	}
30	0001 1110	1E	[RS]	62	0011 1110	3E	>	94	0101 1110	5E	^	126	0111 1110	7E	~
31	0001 1111	1F	[US]	63	0011 1111	3F	?	95	0101 1111	5F	_	127	0111 1111	7F	[DEL]

VOORBEELDEN:

De letter "A" wordt in de computer met volgende binaire code geschreven: "0100 0001".

De letter "a" wordt in de computer met volgende binaire code geschreven:

De letter "z" wordt binair als volgt doorgestuurd: "1111010".

"Sint-Bavo Strafste school 2017!"

Deze tekst ziet er binair als volgt uit:

```
01010011 01101001 01101110 01110100 00101101 01000010 01100001 01110110
01101111 00001101 00001010 01010011 01110100 01110010 01100001 01100110
01110011 01110100 01100101 00100000 01110011 01100011 01101000 01101111
01101111 01101100 00100000 00110010 00110000 00110001 00110111 00100001
```

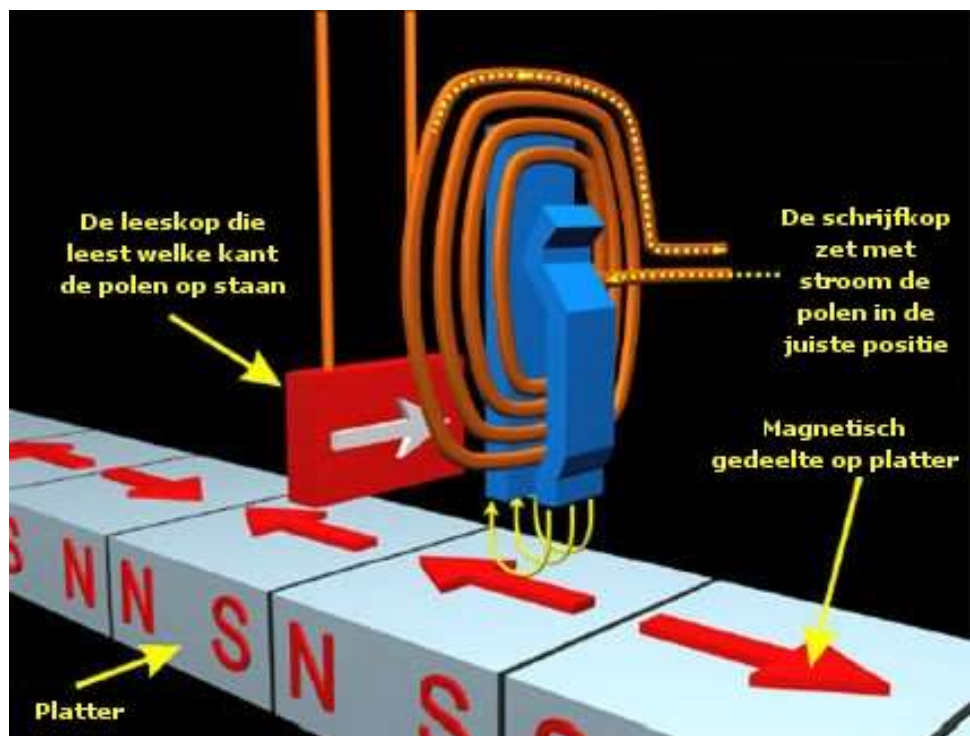
(omgezet met een "tekst to binary converter": <http://www.unit-conversion.info/texttools/convert-text-to-binary/>)

6.3 BINAIRE CODES LEZEN, BEWERKEN EN OPSLAAN

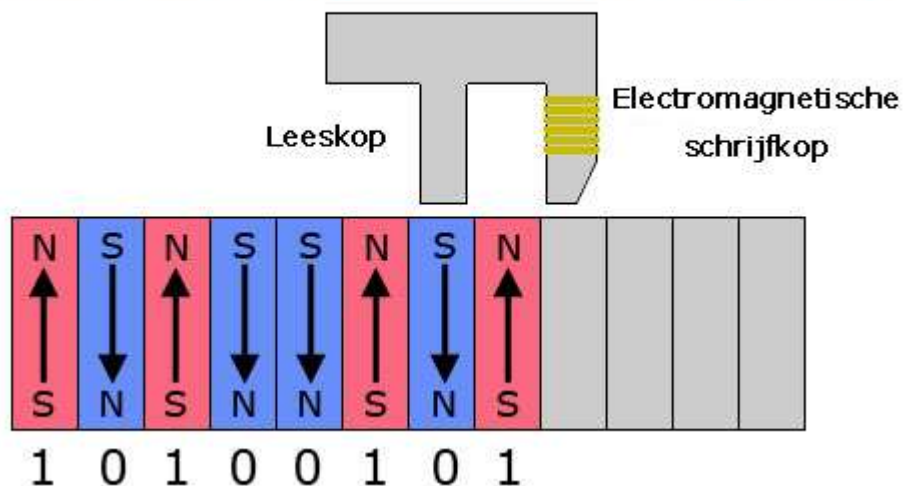
Een bit wordt in de computer meestal weergegeven in het geheugen door een transistor die aan of uit staat of een condensator die geladen of ontladen is.



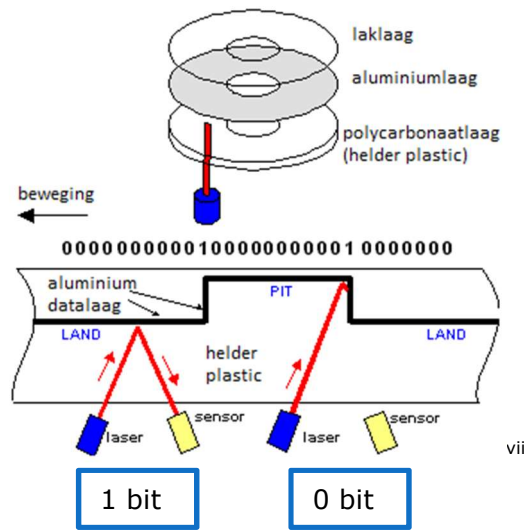
Op **magnetische schijven**, zoals een harde schijf, worden de bits weergegeven door de richting van het magnetisch veld op de oppervlakte van de schijf, Noord-Zuid of Zuid-Noord.



Harde schijf lees-/schrijfkop



Audio-cd's, cd-roms en dvd's bewaren bits **optisch**—het deel van het oppervlak dat voor 1 bit staat, reflecteert het licht of net niet. Bij reflectie leest de computer een 1-signaal (links). Dan wordt er een 1 bit doorgegeven aan het programma. Valt de laserstraal in een putje dan is er geen reflectie op de leessensor en wordt een 0 bit doorgegeven.

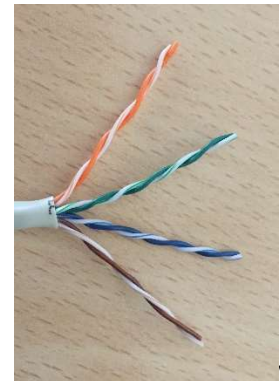
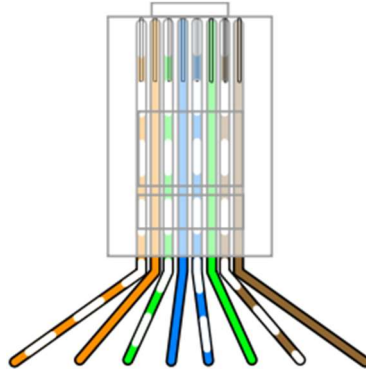
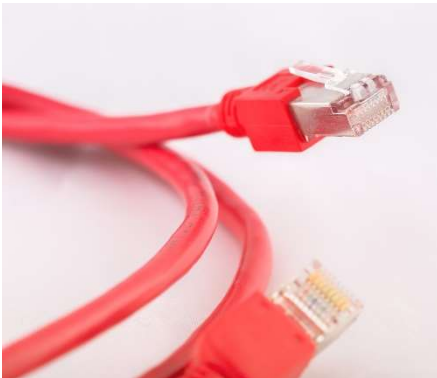


Wanneer data van een computer naar een faxapparaat door een telefoondraad worden gezonden, wordt de binaire code omgezet in een code van hoge en lage tonen. Een lage toon staat voor een 0, een hoge toon voor een 1. Als je per ongeluk een faxnummer belt, herken je dit onmiddellijk. Je hoort een schrille pieptoon.

https://www.youtube.com/watch?v=NnR03_10ai4
<https://www.youtube.com/watch?v=iHW1ho8L7V8>

6.4 GEGEVENSUITWISSELING TUSSEN COMPUTERS

Hieronder zie je twee voorbeelden van bekabeling tussen computer en netwerk. Zoek voor beide volgende gegevens op.



viii

Benaming:

.....

Informatiedrager:

.....

.....

Snelheid / capaciteit:

.....

Maximale afstand:

.....

Decodeer-toestel:

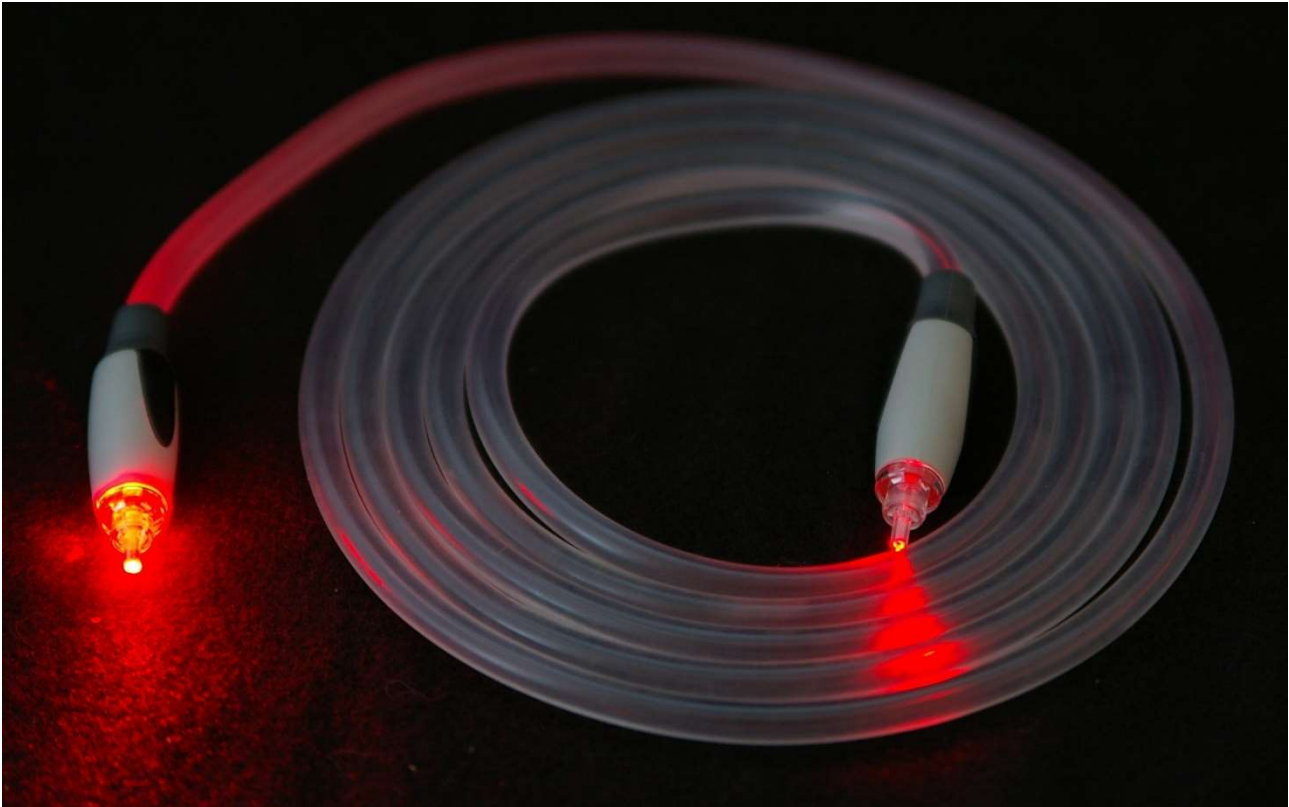
.....

.....

Waar te gebruiken:

.....

.....



ix

Benaming:

.....

Informatiedrager:

.....

.....

Snelheid / capaciteit:

.....

Maximale afstand:

.....

Codeer-Decodeer-toestel:

.....

.....

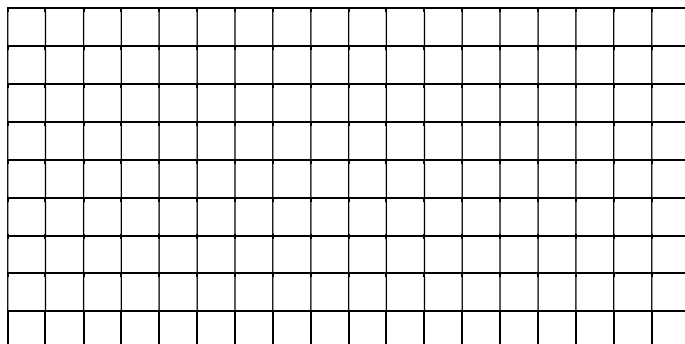
Waar te gebruiken:

.....

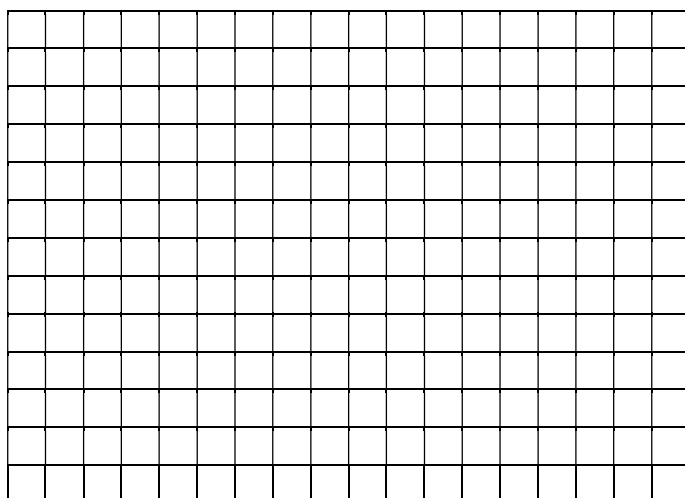
.....

7.2.2 OPDRACHT 2: MAAK DE PIXELTEKENING AAN DE HAND VAN DE CODE (BRON: CS UNPLUGGED)

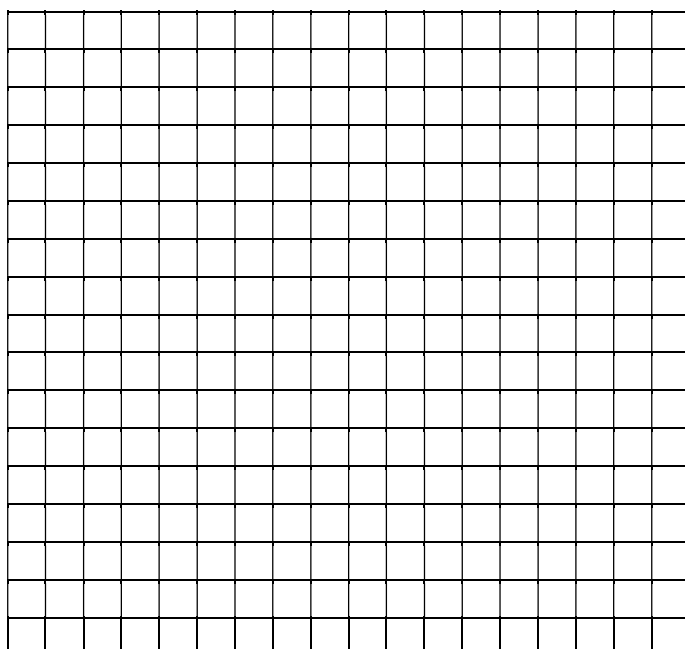
Een fout is zo gemaakt dus doe het met potlood en houd een gum in de buurt!



4, 11
4, 9, 2, 1
4, 9, 2, 1
4, 11
4, 9
4, 9
5, 7
0, 17
1, 15

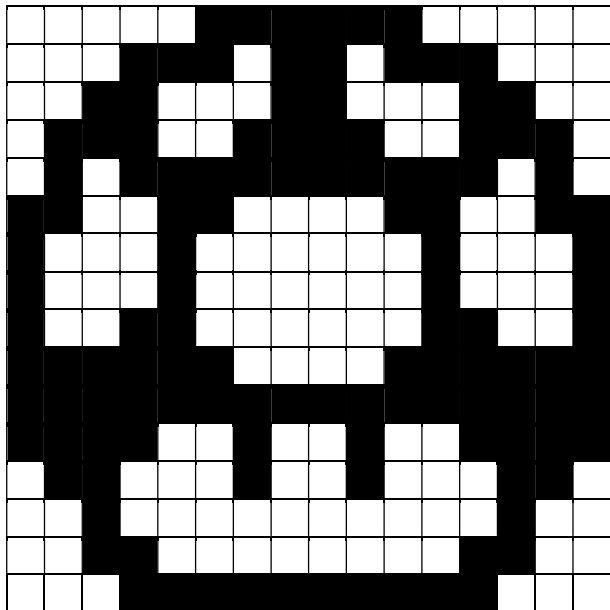


6, 5, 2, 3
4, 2, 5, 2, 3, 1
3, 1, 9, 1, 2, 1
3, 1, 9, 1, 1, 1
2, 1, 11, 1
2, 1, 10, 2
2, 1, 9, 1, 1, 1
2, 1, 8, 1, 2, 1
2, 1, 7, 1, 3, 1
1, 1, 1, 1, 4, 2, 3, 1
0, 1, 2, 1, 2, 2, 5, 1
0, 1, 3, 2, 5, 2
1, 3, 2, 5



6, 2, 2, 2
5, 1, 2, 2, 2, 1
6, 6
4, 2, 6, 2
3, 1, 10, 1
2, 1, 12, 1
2, 1, 3, 1, 4, 1, 3, 1
1, 2, 12, 2
0, 1, 16, 1
0, 1, 6, 1, 2, 1, 6, 1
0, 1, 7, 2, 7, 1
1, 1, 14, 1
2, 1, 12, 1
2, 1, 5, 2, 5, 1
3, 1, 10, 1
4, 2, 6, 2
6, 6

7.2.3 OPDRACHT 3: SCHRIJF NU ZELF DE CODE BIJ DEZE PIXELTEKENING!



7.3 WAAR GAAT DIT EIGENLIJK OVER?

Afbeeldingen kunnen op je computer veel ruimte innemen en al snel te groot worden om te e-mailen. Gelukkig hebben veel foto's veel 'herhaling' in zich, bv. blauwe lucht of witte sneeuw met allemaal pixels met dezelfde kleur. **Om** de benodigde **opslagruimte** voor een foto **te beperken** kunnen programmeurs verschillende toepassen. De methode die we in deze opdrachten gebruikten, heet '**run-length encoding**' en is een efficiënte manier om afbeeldingen of filmpjes mee te Als men afbeeldingen of filmpjes niet zouden verkleinen, zouden ze erg veel ruimte op een harde schijf innemen en zouden ze veel moeilijker via internet verspreid kunnen worden. De zou veel minder vlot verlopen.

8 **CONTROLEGETALLEN (BRON: CS UNPLUGGED)**

8.1 INTRODUCTIE

Wanneer data worden opgeslagen op een harde schijf of worden verzonden van de ene computer naar de andere, nemen we aan dat de data niet veranderen tijdens dit proces.

Maar soms gaat het fout en worden de data per ongeluk gewijzigd. De activiteit die we nu gaan doen, gebruikt een magische truc om te laten zien hoe je erachter kan komen dat data fout (corrupt) zijn en hoe je die fout weer kan herstellen.

8.2 DEMONSTRATIE: DE "MAGISCHE TRUC"^x

8.3 WAAR GAAT DIT EIGENLIJK OVER?

Stel je voor: je stort € 10 op je bankrekening. De baliemedewerker typt het bedrag in en stuurt het naar een centrale computer. Maar wat als er iets misgaat en de code voor € 10 verandert in € 1.000? Dat is niet erg als je de klant bent, maar het is natuurlijk wel erg voor de bank!

Het is belangrijk om fouten op te sporen in verzonden data. Daarom moet een ontvangende computer de data die binnenkomen kunnen controleren op **fouten door elektrische verstoring onderweg**. Als er een fout ontdekt wordt, kunnen de data soms opnieuw verstuurd worden. In andere gevallen is dat niet mogelijk, bijvoorbeeld als een disk of band is **beschadigd** door blootstelling aan magnetische of elektrische straling, door warmte of door fysieke schade. Het wachten wordt wel heel vervelend lang als de data door een fout opnieuw verzonden moeten worden vanaf een ruimtesonde. (Het duurt meer dan een half uur om een radiosignaal te versturen van Jupiter naar de aarde.)

Het is dus belangrijk om **fouten** in data te kunnen (.....)
en de **originele data** te kunnen (.....).

Bij computers wordt dezelfde techniek als bij het spel "kaarten omkeren" gebruikt. Door de bits in denkbeeldige rijen en kolommen te zetten, en **controlebits** aan elke rij en kolom toe te voegen, kunnen we niet alleen ontdekken dat er een fout is opgetreden, maar ook waar. Het beschadigde deel wordt hersteld en daarmee is een foutcorrectie uitgevoerd.

Natuurlijk hebben computers vaak veel complexere foutdetectiesystemen die meerdere fouten kunnen ontdekken en herstellen. Een groot deel van de harde schijf in een computer is bedoeld voor het herstellen van fouten zodat de computer betrouwbaar werkt, ook als delen van de disk niet goed werken. De systemen die hiervoor gebruikt worden lijken heel sterk op het controleschema.

8.4 VOORBEELDEN:

8.4.1 STREEPJESCODE

Een ander voorbeeld van een controlecijfer is bij de streepjescode op boodschappen. Daarbij wordt een specifieke formule gebruikt. Als de streepjescode verkeerd wordt gelezen, dan is het controlecijfer anders dan het berekende cijfer. In dat geval maakt de scanner een geluid en kan de kassamedewerker de code opnieuw scannen.

Bijvoorbeeld de streepjescode = 4 002359 002861

4	0	0	2	3	5	9	0	0	2	8	6	1
/	1	2	3	4	5	6	7	8	9	10	11	12

- 1 Het eerste cijfer is het controlecijfer, dat telt dus niet mee.
- 2 Tel de waarde van alle cijfers in oneven posities (cijfers 1 3 5 7 9 en 11) op.
 $0 + 2 + 5 + 0 + 2 + 6 = \dots\dots\dots$
- 3 Vermenigvuldig deze uitkomst met 3.
 $15 * 3 = \dots\dots\dots$
- 4 Tel de waarde van alle cijfers in even posities (cijfers 2 4 6, 8 en 10) op.
 $0 + 3 + 9 + 0 + 8 + 1 = \dots\dots\dots$
- 5 Tel deze uitkomst (21) bij de uitkomst van stap 3 (45) op.
 $21 + 45 = \dots\dots\dots$
- 6 Neem het nummer in stap 5 (66). Welk cijfer moet je erbij optellen om aan een veelvoud van 10 te komen?
 $66 + ? = 70$
Het controlecijfer = $\dots\dots\dots$

9 CAESARCIJFER

..... is de kunst en de wetenschap van het verbergen van de betekenis van informatie, zodat alleen sommige mensen die informatie kunnen begrijpen. In deze les introduceren we één van de eenvoudigste cryptografische methoden, het Caesarcijfer (ook bekend als de Caesarrotatie of kortweg Rot).

Bij het Caesarcijfer wordt elke letter uit het alfabet vervangen door een andere letter. Meer bepaald, wanneer je een tekst wilt coderen, moet je een verschuivingsgetal S kiezen, dat is een getal tussen 0 en 25. Dan vervang je elke letter in de tekst door de letter die S posities later in het alfabet staat en waarbij je teruggaat naar het begin van het alfabet wanneer je Z, het einde van het alfabet, hebt bereikt.

9.1 CODEERVOORBEELD VIA EXCEL EN CODEERING

Stel dat je de geheime boodschap "**SINT BAVO STRAFSTE SCHOOL**" wil coderen door middel van de verschuivingswaarde $S=2$. De encryptieregel zegt dat elke letter zal worden vervangen door degene die twee posities verder in het alfabet voorkomt.

Maak in Excel een verschuivingstabel. Maak gebruik van de formule: $A2=C1$

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	BA
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	

Bedenk een methode om ook de laatste letters van het alfabet om te zetten.

De eerste letter van de boodschap, de S, wordt vervangen door de letter U. Verder zal de I vervangen worden door K, de N door P, enz. Om de letter Y te coderen, dienen we terug te gaan naar het begin: na de Y komt de Z, dan de A, dus Y wordt vervangen door A. Evenzo wordt de Z vervangen door de B. De gecodeerde versie van onze geheime boodschap wordt aldus:

.....

Wanneer de een of andere spion deze boodschap ziet, zal hij niet onmiddellijk begrijpen waar het over gaat.

Wat is het resultaat van het versleutelen van SPY CODER met de verschuivingswaarde $S = 5$? (Gebruik hoofdletters.)

.....

Je kan natuurlijk ook een decodeerring in 3D printen om de omzetting snel te bekomen.



9.2 DECODEER

Wanneer je vrienden de boodschap hebben gekregen en zij het geheime verschuivingsgetal *S* kennen, is het voor hen gemakkelijk om de boodschap te ontcijferen: elke letter moet worden vervangen door degene die *S* plaatsen eerder in het alfabet voorkomt. Bijvoorbeeld, wanneer *L* moet worden gedecodeerd, ga je twee stappen terug in het alfabet en je vindt *J*, waarvan ze dan weten dat dat de eerste letter is van de geheime boodschap. Opnieuw moeten ze het alfabet zien als een cirkel, waarbij de *Z* voor de *A* komt.

Gebruik dezelfde middelen als in 9.1 om te decoderen.

9.3 DECODEER IN PYTHON

9.3.1 WAT IS EEN STRING?

Alle gegevens die op een computer worden bewaard bestaan uit 0-en en 1-en, inclusief tekst, digitale boeken, plaatjes, liedjes, video's en "programma's" zoals spelletjes en toepassingen.

Strings, een voorbeeld van tekst, worden op de volgende wijze opgeslagen:

- Een string is een rij karakters, bv. de string "Hello, World!" bestaat uit 13 karakters waaronder de letters "H", "e" en tekens als " " (spatie) en "!".
- Elk karakter wordt gerepresenteerd door een getal, bv. "H" wordt gerepresenteerd door het getal 40; dat heet de ASCII/Unicode waarde.
- Getallen worden intern op hun beurt weer bewaard in een 0-1 binair formaat.

9.3.2 BEWERKINGEN OP EEN STRING

Je kunt een string zien als een rij karakters: `S[]`.

Om een string te kunnen bewerken is het nodig om de individuele karakters te kunnen selecteren. In Python wordt dit op de volgende manier gedaan: bij een string *S* en een integer *index*, is `S[index]` het karakter van *S* op positie *index*. Volgens afspraak begint de string bij index 0, dus is `S[0]` het eerste karakter en `S[1]` het tweede karakter, enz.

In "Hello, World!" bestaat de lijst van karakters uit:

- Index: 0 1 2 3 4 5 6 7 8 9 10 11 12
- Rij karakters: H e l l o , W o r l d !
- Merk op dat het karakter met index 6 een spatie is.

9.3.3 CODES VOOR KARAKTERS: `ORD`, `CHR`

Zoals we in de introductie van deze les al noemden, wordt in de computer elk karakter vastgelegd door een getal. Welk karakter correspondeert met welk getal? In het algemeen hangt dat af van de codering die je gebruikt, maar vrijwel alle moderne computers gebruiken dezelfde standaardset voor de getallen tussen 32 en 255.

In Python kun je een karakter omzetten in zijn bijbehorende code door middel van de `ord`-functie. De `chr`-functie doet het omgekeerde: de input is een getal en de uitvoer is het karakter met die code.

Voorbeeld

Voorbeeld van ord en chr

```
print(ord('a'), ord('b'), ord('A'), ord('B'), ord(' '))
print(chr(35), chr(43), chr(100))
```

Uitvoeren
Open in the console
Visualiseer

Het programma is uitgevoerd zonder te crashen.

Het programma heeft de volgende uitvoer gegeven:

```
97 98 65 66 32
# + d
```

</>

Schrijf een programma dat een karakter als input neemt (een string met lengte één), waarbij we aannemen dat het een hoofdletter is, en de output is de volgende letter uit het alfabet. Maar als de input 'Z' is, dan moet de output 'A' zijn. (Je zult daarbij een *if statement* nodig hebben.) Voor nog een aanwijzing:

```
1 letter=input()
2 getal=ord(letter)
3 getal= getal+1
4 if getal == 91:
5     getal=65
6 print(chr(getal))
7
```

9.3.4 UITGEWERKT PROGRAMMA

Een tekst coderen

```
1  n = int(input('Geef verschuiving: '))
2  tekst = input('Geef de tekst die je wil coderen: ')
3  uitvoer = ''
4
5  for karakter in tekst:
6      if karakter.isalpha():
7          ascii = ord(karakter)
8
9          if ord('A') <= ascii <= ord('Z'):
10             ascii += n
11             if ascii < ord('A'):
12                 ascii += 26
13             if ascii > ord('Z'):
14                 ascii -= 26
15         else:
16             ascii += n
17             if ascii < ord('a'):
18                 ascii += 26
19             if ascii > ord('z'):
20                 ascii -= 26
21
22         karakter = chr(ascii)
23     uitvoer += karakter
24
25 print(uitvoer)
26
```

Een tekst decoderen waarvan je de verschuiving kent:

```
1  n = int(input('Geef het natuurlijk getal van de verschuiving: '))
2  tekst = input('Geef de gecodeerde tekst die je wil decoderen: ')
3  uitvoer = ''
4
5  for karakter in tekst:
6      if karakter.isalpha():
7          ascii = ord(karakter)
8
9          if ord('A') <= ascii <= ord('Z'):
10             ascii -= n
11             if ascii < ord('A'):
12                 ascii += 26
13             if ascii > ord('Z'):
14                 ascii -= 26
15         else:
16             ascii -= n
17             if ascii < ord('a'):
18                 ascii += 26
19             if ascii > ord('z'):
20                 ascii -= 26
21
22         karakter = chr(ascii)
23     uitvoer += karakter
24
25 print(uitvoer)
26
```


9.4 VOOR DE BAD GUYS WERKEN

Je bent ingehuurd door een spion om te helpen bij het ontcijferen van een gecodeerde boodschap waarbij een verschuivingswaarde is gebruikt. Jammer genoeg weet de spion de waarde van S niet.

9.4.1 BRUTE FORCE

Je kan natuurlijk alle mogelijke sleutels gebruiken om de boodschap te decoderen. We noemen dit **brute force**.

Is dit haalbaar denk je?

.....

Hoeveel verschillende Caesarcijfer-codes zijn er mogelijk?

.....

Is de Caesarcijfer-versleuteling veilig in onze digitale wereld?

.....

Deze methode om de code te ontcijferen is mogelijk als we op een cyclische manier versleutelen: elke letter heeft dezelfde verschuiving.

Als het niet op een cyclische manier gebeurt, werkt brute force niet, omdat er $26 \cdot 25 \cdot \dots \cdot 1$ mogelijke substitutie-cijfers zijn, wat neerkomt op ongeveer $4 \cdot 10^{26}$ mogelijke codes (0,4 quadriljard). Zelf met de krachtigste computer ter wereld een onmogelijke klus.

9.4.2 LETTERFREQUENTIE-ANALYSE

Je gaat statistisch onderzoek gebruiken om een programma te schrijven dat een goede kans heeft de juiste waarde van S op te sporen.

Bij deze methode maak je gebruik van letterfrequentie-analyse. In het Engels komen sommige letters (zoals de E) vaak voor en sommige heel weinig (zoals de J). Hier volgt een frequentietabel, gebaseerd op het tellen van letters in een grote hoeveelheid tekst.

A	B	C	D	E	F	G	H	I
.0817	.0149	.0278	.0425	.1270	.0223	.0202	.0609	.0697
J	K	L	M	N	O	P	Q	R
.0015	.0077	.0402	.0241	.0675	.0751	.0193	.0009	.0599
S	T	U	V	W	X	Y	Z	
.0633	.0906	.0276	.0098	.0236	.0015	.0197	.0007	

Zo is, bijvoorbeeld, de frequentie van L $0.0402=4.02\%$, en dat betekent dat in een doorsnee Engelse tekst 4.02% van de letters L zijn.

Noem de juist-waarde van een letter de waarde ervan in de tabel hierboven. Definieer dan in onze statistische methode de juist-waarde van een zin als de som van de juist-waarde van elk van de letters. Zo is bijvoorbeeld de juist-waarde van de string GOOD.

$$\text{juist-waarde("GOOD")} = 0,0202 + 0,0751 + 0,0751 + 0,0425 = 0,2129$$

Nu is het idee van frequentie-analyse dat strings met een hogere juist-waarde waarschijnlijker een Engelse tekst weergeven. Wanneer bijvoorbeeld, de spion de gecodeerde boodschap "JRRG" ziet, dan is het zowel mogelijk dat de originele tekst "GOOD" is met verschuivingswaarde $S=3$, als "IQQF" met $S=1$. Maar de juist-waarde van "IQQF" is.

$$\text{juist-waarde("IQQF")} = 0,0697 + 0,0009 + 0,0009 + 0,0223 = 0,0938$$

En omdat $0,0938 < 0,2129$, dient je programma de conclusie te trekken dat het meer waarschijnlijk is dat GOOD de juiste boodschap is dan dat IQQF de juiste is.

10 IN DE PERS

10.1 E-LOKET

HLN, 27 september 2017

Eén op vijf gemeentelijke websites gooit gegevens van inwoners te grabbel

Vereniging Vlaamse Steden en Gemeenten "Heel bezorgd"^{xi}



INTERNET Eén op de vijf Vlaamse gemeentewebsites gebruikt geen veilige HTTPS-verbinding voor een digitaal loket. Daardoor kunnen cybercriminelen persoonlijke gegevens van inwoners onderscheppen, meldt VRT NWS. De Vereniging van Vlaamse Steden en Gemeenten (VVSG) zegt heel bezorgd te zijn en het rapport te zullen bestuderen.

Officiële attesten opvragen, politietoezicht aanvragen tijdens een vakantie in het buitenland of een adreswijziging doorgeven: het zijn diensten die gemeenten steeds vaker online aanbieden in een digitaal loket op hun website.

Voor veel van die aanvragen moet je als inwoner vaak privacygevoelige informatie invullen. Maar die gegevens worden niet altijd op een veilige manier verstuurd, waardoor die in handen kunnen vallen van cybercriminelen. Met mogelijke identiteitsfraude tot gevolg, blijkt uit een onderzoek van enkele ethische hackers, in samenwerking met Canvasprogramma Terzake.

"Onaanvaardbaar"

De grootste problemen doen zich volgens VRT NWS voor bij gemeenten die op hun digitaal loket geen beveiligde HTTPS-verbinding gebruiken. Met zo'n verbinding worden gegevens versleuteld op het moment dat een gebruiker informatie verstuurt. Maar in 61 gemeenten is dat niet het geval. Dat is zo'n 21 procent van alle sites met een digitaal loket. Vooral wie met een onbeveiligde wifiverbinding surft, is kwetsbaar voor cybercriminelen.

Staatssecretaris voor Privacy Philippe De Backer spreekt van "een onaanvaardbare situatie". "Het is de taak van de gemeente om de gegevens van haar inwoners goed te beschermen. Het is onaanvaardbaar dat ze de Privacywet niet volgen." Bovendien worden volgens De Backer ook voldoende sessies georganiseerd om de gemeenten te informeren hoe ze gegevens voldoende

kunnen beveiligen. De Backer bevestigt ook dat bij de hervorming van de Belgische Privacycommissie meer aandacht zal gaan naar het controleren van onder andere gemeentewebsites.

"Lessen trekken"

"We zijn heel bezorgd", reageert de Vereniging van Vlaamse Steden en Gemeenten (VVSG). "We werken volop aan digitale maturiteit en gaan hieruit lessen trekken." De vereniging benadrukt ook dat 80 procent van de gemeentewebsites wel veilig is. Ook de gemeenten zijn volgens de VVSG bezorgd. "De mensen moeten erop kunnen vertrouwen dat die gegevens veilig zijn", klinkt het nog. "We werken hier aan."

Als mogelijke verklaring geeft de vereniging mee dat gemeenten soms met externe leveranciers werken, die niet altijd uit zichzelf met een HTTPS-verbinding werken.

10.2 FBI OPENT NIEUW ONDERZOEK NAAR E-MAILS^{xii}

De Redactie, 31 mei 2017

"De FBI opent een onderzoek naar nieuwe e-mails die zijn opgedoken en die een verband lijken te hebben met het eerdere onderzoek van de e-mails van Hillary Clinton. Dat heeft FBI-topman James Comey gemeld in een brief aan het Congres. Donald Trump is opgetogen over de "heropening" van het onderzoek, een term die de Democraten betwisten. Volgens Trump is de affaire "groter dan Watergate."

Het FBI-onderzoek naar de persoonlijke e-mailserver van Clinton werd eerder dit jaar afgesloten. De conclusie was toen dat de presidentskandidate zeer onvoorzichtig was geweest, maar niet bewust de wet had overtreden. Ze werd dan ook niet vervolgd. Dat de FBI nu vlak voor de verkiezingen een nieuw onderzoek opent, is een opmerkelijke beslissing die Clinton slecht uitkomt.

Het nieuwe onderzoek zou gaan over e-mails die nog niet eerder onderzocht werden. In de brief aan het Congres zegt FBI-directeur Comey dat nagegaan wordt of die nieuwe e-mails geheime informatie bevatten. "Momenteel kan de FBI nog niet inschatten of de informatie significant is", luidt het. Comey geeft in zijn brief geen aanduiding over hoe lang dit nieuwe onderzoek zal duren.

De e-mailaffaire: waarover gaat het?

De e-mailaffaire achtervolgt Clinton al de hele campagne. Als minister van Buitenlandse Zaken heeft ze een eigen 'private server' gebruikt om e-mails te versturen. Een deel van die e-mails bevatte gevoelige informatie, die zo mogelijk blootgesteld werd aan "vijandige actoren".

De FBI kwam in juli tot de conclusie dat Clinton "zeer onvoorzichtig" was geweest maar niets gedaan had waarvoor ze vervolgd moest worden.

De Republikeinen en presidentskandidaat Donald Trump voeren de kwestie aan als argument dat Clinton ongeschikt is voor het presidentschap, of zelfs in de cel thuishoort."

Zoek op het net naar oplossingen om je data te versleutelen:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

BRONVERMELDING AFBEELDINGEN EN ARTIKELS

ⁱ U.S. Navy photo, John F. Williams. *The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.*

ⁱⁱ <https://nl.wikipedia.org/wiki/Morse>

ⁱⁱⁱ <https://nl.wikipedia.org/wiki/Morse>

^{iv} 'tin can phone', Kit Cowan, CC-licentie BY-NC-ND

^v http://www.hoehetwerkt.nl/index.php/Harde_schijf, geraadpleegd op 14 oktober 2017

^{vi} <https://www.computerhope.com/jargon/h/harddriv.htm>, geraadpleegd op 14 oktober 2017

^{vii} Computer Desktop Encyclopedia, <http://www.computerlanguage.com/>, CD-ROM, geraadpleegd op 15 oktober 2017

^{viii} Johan Braeken, CC-licentie BY, https://commons.wikimedia.org/wiki/File:Utp_diy02_sequenceInCable.jpg

^{ix} Hustvedt, CC-licentie BY-ND, https://commons.wikimedia.org/wiki/File:Fiber_optic_illuminated.jpg

^x Ik kan al programmeren, <http://www.dwengo.org/wegostem>, WeGoSTEM2017_boekje.pdf

^{xi} <https://www.hln.be/ihln/internet/een-op-de-vijf-gemeentelijke-websites-gooit-gegevens-van-inwoners-te-grabbel~a0e7951b/>, 27 september 2017, geraadpleegd op 14 oktober 2017

^{xii} <http://deredactie.be/cm/vrtnieuws/buitenland/1.2805667>, 31 mei 2017, geraadpleegd op 14 oktober 2017