Hoofdstuk 4: Hoe het internet werkt

Hoofdstuk 4 Les 1: Betrouwbare Communicatie, 1

Originele tekst:	Verbetering:
In deze les leer je de basis van de werking van het Internet.	In deze les leer je in de basis hoe het internet werkt.
zie je hoe een website je de bestanden stuurt die je opvraagt en leer je een aantal termen om over het Internet te spreken.	Zie je hoe een website je bestanden toestuurt wanneer je deze opvraagt, en je leert een aantal termen die je kan gebruiken als je over het internet praat.
zaken	dingen
standard	standaard
domain name	domeinnaam
path	pad
, en om de server te vragen het bestand privacy.html uit de map website op te sturen.	en vraagt de server om het bestand privacy.html uit de map website op te sturen.
(zoals WhatsApp),	geen komma
verzorgt.Het	verzorgt. Het (spatie vergeten)

Het doet dit vooral door gebruik te maken van een aantal protocollen	Het internet maakt hierbij gebruik van een aantal protocollen
localiseert	lokaliseert
gemetene	gemeten
dus mensen konden geen video verzenden	hierdoor konden mensen geen video verzenden
Streaming video	Een video streamen
Maar tegenwoordig, vereisen	geen komma
rekenkracht, en deze	rekenkracht. Deze
gegevens. Of iemand onderschept de data terwijl ze naar de cloud worden gestuurd	gegevens, of iemand onderschept de data terwijl ze naar de cloud worden gestuurd
Improved security and privacy over storing data on a personal computer.	Verbeterde veiligheid en privacy bij het opslaan van data op een persoonlijke computer.

Hoofdstuk 4 Les 1 betrouwbare communicatie 2:

you will learn how the layout of the Internet is redundant (more than one path from here to there) in order to ensure reliability.

ga je leren dat de layout van het internet overtollig is (er zijn meerdere routes van begin tot eind) om betrouwbaarheid te kunnen garanderen.

Given the enormous amount of data traveling around, the Internet needs to be reliable. We have achieved this by building many redundant connections into the physical systems of the Internet. Wherever information is going, there is more than one way to get there, so that if part of the Internet fails, the rest remains connected even if the

failed part is in the usual path from one place to another. This increases the Internet's fault tolerance (ability to work around problems). And it also helps the Internet scale (expand) to more devices and people.

Omdat er gigantische hoeveelheden data rondgaan moet het internet betrouwbaar werken. Dat hebben we bereikt door veel overtollige connecties in het fysieke systeem van het internet te bouwen. Waar informatie ook naartoe gaat, er moeten meerdere manieren zijn om er te komen, zodat als een deel van het internet uitvalt de rest in connectie kan blijven, ook als dat niet de normale route is die de informatie neemt. Dit maakt de faal tolerantie van het internet (de vaardigheid om om een probleem heen te werken) groter, ook zorgt het er voor dat het internet kan vergroten naar meer apparaten en mensen.

Internet scalability is the ability of the net to keep working even as the size of the network and the amount of traffic over the network increase. The page Internet 2012 in numbers has some astonishing numbers about Internet traffic from a few years ago.

Less

internet schaalbaarheid is de vaardigheid om het net werkende te houden, ook als de grootte van het netwerk wordt uitgebreid. Pagina http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/ heeft overweldigende cijfers over het internetverkeer van een aantal jaar geleden.

Describe what's going on in this animation.

Beschrijf wat er gebeurt in deze animatie.

Work through the following questions.

Maak de volgende vragen.

In this model of a network, what is the minimum number of nodes (connection points) that can stop working before the sender and the receiver can't communicate? (Other than the sender or the receiver themselves, of course.)

Less

Welke connectiepunten moeten minimaal uitvallen willen de verzender en ontvanger niet meer kunnen communiceren?

There are no nodes that are vital to the system. Pick any node to stop working, and you can still find another path.

Er zijn geen connectiepunten die vitaal zijn voor het systeem, en in hun eentje het netwerk kunnen ontwrichten.

Correct! If the node with 6 connections goes down and also either of the two to its left, the sender and receiver can't communicate.

Correct! als de twee connectiepunten die direct aan de ontvanger gekoppeld zijn uitvallen is er geen connectie meer mogelijk.

Try to find a smaller number of nodes that can stop working and still break communication.

Er is een lager aantal connectiepunten die uitgeschakeld kunnen worden waarbij de connectie wordt verloren.

Try to find a smaller number of nodes that can stop working and still break communication.

Er is een lager aantal connectiepunten die uitgeschakeld kunnen worden waarbij de connectie wordt verloren.

Try to find a smaller number of nodes that can stop working and still break communication.

Er is een lager aantal connectiepunten die uitgeschakeld kunnen worden waarbij de connectie wordt verloren.

You have successfully completed this question!

Je hebt de vraag succesvol beantwoord.

In the same model network, what is the maximum number of nodes that can fail and still let Sender and Receiver communicate?

In hetzelfde model netwerk, hoeveel connectiepunten kan je maximaal uitschakelen zonder dat je de connectie tussen de zender en ontvanger doorbreekt.

If all 10 nodes fail, the sender and receiver can't communicate.

Als alle 10 de connectiepunten uitvallen kunnen de zender en de ontvanger niet meer communiceren.

If 9 nodes fail, the sender and receiver can't communicate.

Als 9 connectiepunten uitvallen kunnen de zender en de ontvanger niet meer communiceren.

Try to find a higher number of nodes that can stop working and still ensure communication.

Probeer een andere connectieroute te vinden waarmee je meer connectiepunten uit kan laten vallen.

Try to find a higher number of nodes that can stop working and still ensure communication.

Probeer een andere connectieroute te vinden waarmee je meer connectiepunten uit kan laten vallen.

Address Hierarchy

you will learn how to interpret the pieces of a domain name or an IP address.

ga je leren hoe je delen van een domeinnaam of IP-adres interpreteert.

There are two hierarchical addressing systems on the Internet: domain names and IP addresses. People use domain names (like snap.berkeley.edu) to visit websites. Computers that are part of the domain name system translate those domain names to IP addresses (like 128.32.189.18) to locate and send data behind the scenes.

Less

Er zijn twee Hiërarchische systemen voor naamgeving op het internet: domeinnaam en IP-adres, je gebruikt domeinnamen (zoals snap.berkeley.edu) om een website op te zoeken. Computers die deel uitmaken van het domein naam systeem, vertalen de domeinnamen naar IP-adressen (zoals 128.32.189.18) om data op te zoeken en te verzenden achter de schermen.

A hierarchy is an arrangement of things with the biggest or highest category at the top and things ranked into subcategories below. A hierarchy is often depicted as a triangle.

More

Een hiërarchie is een rangorde op basis van grote, belang of macht.

For example, in a school, the principal is at the top, the department chairs oversee the teachers, and the teachers lead the students. In biology, we use a taxonomic hierarchy: kingdom, phylum, class, order, family, genus, species. And on computers, we store files in a hierarchy of folders within folders.

Less

Voorbeeld, in een school staat de directeur/directrice bovenaan, het schoolbestuur daar onder, de leerlingenraad daaronder, dan komen de leraren en dan de leerlingen.

Before the Internet, there were only small networks of computers (like the Arpanet, which peaked at around 200 computers), and every computer knew the name of all the other computers on the network. That worked for small networks, but it's not realistic for the 3 billion computers on the Internet now. So now, a hierarchy allows the system to distribute requests for IP addresses to domain name servers across the growing network.

Less

Voordat het internet bestond waren er alleen nog kleinschalige netwerken van computers (zoals het Arpanet die op zijn piek bestond uit 200 computers), elke computer kende de naam van alle andere computers. at werkte voor kleine netwerken maar dat is niet realistisch voor 3 miljard computers over de hele wereld die nu op het internet zitten. De hiërarchie zorgt ervoor dat het systeem verzoeken om IP-adressen kan toekennen aan domeinnaamservers in een groeiend netwerk.

Domain Name Hierarchy

Domeinnaam Hiërarchie

Just as the path in a URL locates a specific file in a hierarchy of folders on the server, domain names locate a specific website within a hierarchical domain name system (DNS). The hierarchy of the domain name system simplifies the process of finding the computer with the desired domain name because the DNS servers that help locate domains don't need enormous lists with every host name in the world. Instead, any user's computer only has to know where to find a root domain server (the one that knows where to find the top-level domains such as .org and .edu), and that server knows where to find the domain (like berkeley.edu), and that server knows where its subdomains are (like snap.berkeley.edu), and so on. The root domain may be a country code (such as .mx for Mexico) or a category code (like .gov for government). The last two segments of a domain name (like berkeley.edu) make up the primary domain, the main address for a site. Subdomains are subsections of primary domains or of other subdomains. For example:

Less

Net zoals het pad in een URL een specifieke folder in een Hiërarchie van folders op de server zoekt, worden domeinnamen door het domeinnaam systeem (DNS) in de Hiërarchie gezocht. De Hiërarchie van het domeinnaam systeem versimpeld het proces voor het zoeken van de juiste informatie op de juiste computer omdat het DNS systeem niet een enorme lijst hoeft te hebben met elke host naam ter wereld. In Plaats daarvan hoeven computers alleen te weten waar zij het root-domein moeten vinden (Het domein dat weer waar je alle top-level domeinen zoals .org en .edu moet vinden), Doe weten dan weer waar je domeinen zoals berkeley.edu moet vinden, die server weet op zijn plaats weer waar je een subdomein zoals like snap.berkeley.edu moet vinden enzovoorts. Het root- domein kan een landcode zijn zoals .nl voor Nederland of .uk voor het Verenigd koninkrijk, of een categorie code zoals .gov voor goverment (landsbestuur). de laatste 2 segmenten van een domeinnaam bepalen het primaire domein, het hoofdadres van een site. Subdomeinen zijn voor subsecties ofterwijl aparte pagina's op een website. Voorbeeld:

This question is similar to those you will see on the AP CSP exam.

Deze vraag is vergelijkbaar met de vragen van het AP CSP examen.

Which of the following could be a subdomain of the domain bicycles.com?

Welke van de onderstaande zou een subdomein kunnen zijn van bicycles.com?

Correct! about.bicycles.com could be a subdomain on the bicycles.com domain.

Correct! dit zou een subdomein kunnen zijn van bicycles.com.

bicycles.co.uk would be used for a commercial site in the United Kingdom.

Helaas, bicycles.co.uk zou wel gebruikt kunnen worden voor een commerciële site in het verenigd koninkrijk

bicycles.org is a completely different domain name that would be on a .org (not .com) name server.

bicycles.org is een compleet andere domeinnaam niet op .org zit in plaats van .com.

bicycles.com.org is not a typical address format because it has both the .com and .org category codes.

bicycles.com.org is geen gebruikelijk adres omdat het zowel .com en .org bevat.*

When we type in a domain name, the browser queries the domain name system to find the Internet Protocol (IP) address of the server we want to visit. IP addresses are unique numerical addresses assigned to every device on the Internet. Both the domain name syntax and IP addresses are hierarchical; however unlike domain names, with IP addresses, the individual site is on the right and the top-level groupings are on the left (see image at right).

*Als je een domeinnaam intypt onderzoekt de browser de domeinnaam om het **Internet Protocol (IP) adres te vinden** van de opgevraagde server. IP-adressen zijn unieke nummers die online adressen weergeven van elk apparaat op het internet. zowel de domeinnaam als de syntax en het IP-adres zijn Hiërarchisch gesorteerd; domeinnamen en IP-adressen verschillen wel van elkaar door het feit dat de*

If your connection blocks YouTube,

Als je connectie YouTube blokkeert

watch the video here.

kijk dan de video via deze link (http://scratch.mit.edu/discuss/youtube/5o8CwafCxnU).

What's an undecillion? One undecillion is 103610^{36}1036, a billion billion billion billion, a 1 with 36 zeros after it, 109 · 109 · 109 · 10910^9 \cdot 10^9 \cdot 10^9 \cdot 10^9109 · 109 · 109 · 109.

Less

Wat is een sextiljoen*? een *sextiljoen* is een 1 met 36 nullen.*

Pick one:

Kies een van de onderstaande:

Write an explanation of the DNS and IP address hierarchy.

Schrijf een uitleg van de DNS en IP-adres Hiërarchie.

When you specify an IP address, you are using an abstraction. Why? What is the more detailed thing that you are abstracting away? Write out your explanation.

Als je een IP-adres uit een domeinnaam haalt gebruik je een compacte versie. Wat is daar de reden voor? Wat is het meest gedetailleerde dat je compacter opschrijft? schrijf een uitleg.

Hoofdstuk 4 Les 1: Betrouwbare Communicatie, 4

Originele tekst	verbetering / verandering
you will learn about the history of the Internet.	ga je leren over de geschiedenis van het internet
in role	Weghalen
voorspelt	voorspeld
Zle	Zie
Watvoor	Wat voor
grotoe	grote

Unit 4 Lab 2: Communication Protocols, Page 1

Vertalingen:

Unit 4 Lab 2: Communication Protocols, Page 1
Hoofdstuk 4, les 2: Communicatieprotocollen, pagina 1

you will learn about some of the abstractions that make the Internet work.
ga je leren over een aantal van de abstracties die het internet laten werken.

you will learn how machine-readable computer addresses work.
ga je leren hoe machine leesbare computer adressen werken.

The Internet isn't just a network of computers. It's a network of networks. The connection points between networks are called routers, networking devices that route traffic between subnetworks on the Internet. The routers only know how to pass information on to the next router or to the final destination; the routers do not analyze what's inside each packet of data (as long as you live in a country without Internet censorship). Making sense of the information happens at the destination computer. This is called the end to end principle.
Het internet is niet alleen een netwerk van computers. Het is een netwerk van netwerken. De verbindingspunten tussen netwerken heten routers, wat netwerk apparaten zijn die zorgen voor het routeverkeer tussen subnetwerken op het internet. De routers weten alleen hoe ze informatie aan de volgende router of aan de eindbestemming door moeten geven: De routers analyseren niet wat er in elk pakketje data staat (als je niet in een land woont met internet censoring). Het begrijpen van de informatie gebeurt op de doelcomputer. Dit wordt het end to end principe genoemd.

A router is a computer that passes information from one network to another.
een router is een computer die informatie van het ene netwerk naar het andere verplaatst.

Depending on where you live, you might pronounce "route" differently, but "router" is always pronounced the same: like "outer."
Afhankelijk van waar je woont, kun je 'route' anders uitspreken, maar 'router' wordt altijd hetzelfde uitgesproken: zoals 'outer'.

The end to end architecture of the Internet means that routers only know how to find an IP address; they don't do anything with the content of the message. Making sense of content is the job of the endpoint computers: the sender and the receiver.
Het end to end ontwerp van het internet betekent dat de router alleen weten hoe ze een IP adres moeten vinden: ze doen niks met de context van het bericht. De context begrijpen is de taak van de eindbestemming computers: De verzender en de ontvanger.

How Do Routers Know Where to Find the Computer You Want?

Hoe weten routers waar ze de computer vinden die jij wilt?

Every device on the Internet has a unique Internet Protocol (IP) address (or more than one, if it's a router), like a postal or email address. The Internet Protocol specifies how a router handles a request for a different IP address. Each router knows the layout of its specific neighborhood of the Internet and knows which way to send each message to get it a little bit closer to where it's going. The fact that each router doesn't have to know the complete Internet improves scalability.

Elk apparaat op het internet heeft een uniek Internet Protocol (IP) adres (of meer dan een, als het een router is), zoals een post of email adres. Het Internet Protocol specificeert hoe een router een verzoek om een ander IP-adres afhandelt. Elke router weet de layout van zijn specifieke buurt op het internet en weet op welke manier elk bericht moet worden verzonden om het een beetje dichter bij hun doel te krijgen.Het feit dat elke router niet het complete internet hoeft te kennen, verbetert de schaalbaarheid.

Usually, there are many possible paths from one endpoint to another. This redundancy allows IP to find an alternate pathway if some system in the middle doesn't respond to requests by finding an alternate pathway. This is the principle of fault tolerance. When you send a data over the Internet, the IP program in your computer divides it into packets that it sends individually. (Each may take a different path.) This process is what makes the Internet a packet switching network.

Normaal zijn er veel verschillende mogelijke paden van een eindpunt naar een andere. Deze overtolligheid staat IP toe om een alternatief pad te vinden als een systeem in het midden niet op verzoeken reageert door een alternatief pad te vinden. Dit is het principe van een foutentolerantie. Wanneer je data verstuurt over het internet, verdeelt het IP programma in je computer het in pakketjes die het individueel kan versturen (elk kan een ander pad nemen). Dit proces is wat het internet een pakketgeschakeld netwerk maakt.

An IP address is a unique number assigned to each device on a computer network. P
acket switching means that the Internet sends short bursts of information, not long continuous strings.

Een IP adres is een uniek nummer, toegewezen aan elk apparaat op een computer netwerk. Pakket wisselen betekent dat het internet korte hoopjes informatie stuurt, in plaats van continue rijen.

Why does the graph of the Internet look like a tangle in the middle with fireworks on the outsides?

Waarom ziet de grafiek van het Internet eruit als een kluwen in het midden met vuurwerk aan de buitenkant?

Discuss how this shape is related to how people connect to the Internet (though an Internet Service Provider, etc.). Write out a brief description and/or explain it to someone else.

Bespreek hoe deze vorm in verband staat met hoe mensen verbinden met het internet (door een Internet Service Provider, etc.) Schrijf een korte beschrijving en/of leg het aan iemand anders uit.

Visit http://bot.whatismyipaddress.com/ for your current IP address.

Ga naar http://bot.whatismyipaddress.com/ om te zien wat je huidige IP adres is.

Visit http://ipinfo.io/. What information does that page give you? (You don't need to enter your email address. Just click "See more details.")

Ga naar http://ipinfo.io/ Welke informatie geeft deze pagina je? (Je hoeft je email adres niet in te vullen. Je kunt klikken op "See more details.")

You can add any IP address to the end of that URL like this:

Je kunt zo elk IP adres toevoegen aan het einde van de URL

The amount of detailed information available from an IP address is pretty amazing (and a little scary), especially when you think about the ways that information can be used.

De hoeveelheid gedetailleerde informatie die beschikbaar is van een IP adres is best geweldig (en een beetje eng), zeker als je denkt over de manieren waarop die informatie gebruikt kan worden.

Some of the information might have slight inaccuracies. IP addresses often give the location of an Internet service provider, possibly at a different location.

Sommige informatie kan kleine onnauwkeurigheden bevatten. IP adressen geven vaak de locatie van een Internet Service Provider, die mogelijk op een andere locatie is.

Each of the four numbers in a typical IP address today is an eight-bit byte with a value between 0 and 255 (see right). A 32-bit IPv4 (the "v" stands for "version") address is big enough to support 232 computers. That's about four billion (4 · 109), but there are more than seven billion people on Earth, so there aren't enough IP addresses to go around.

Elk van de vier nummers in een typisch Ip adres dat we vandaag de dag gebruiken is een acht-bit byte met een waarde tussen 0 en 255 (zie rechts). Een 32-bit IPv4 (de “v” staat voor “versie”) adres is groot genoeg om 232 computers te ondersteunen. Dat is ongeveer vier biljoen (4 · 109), maar er zijn meer dan zeven biljoen mensen op aarde, dus er gaan zijn niet genoeg IP adressen.

Why does IPv4 support 232 computers? There are 32 bits in an IPv4 address (see right), and each bit can be one of two possible values (0 or 1). So, there are 232 possibilities with thirty-two bits.

Waarom ondersteunt IPV4 232 computers? Er zijn 32 bits in een IPv4 adres (zie rechts), en elke bit kan een van de twee mogelijke waarde zijn (0 of 1). Dus, er zijn 232 mogelijkheden met tweeëndertig bits.

he long-term solution is to increase the length of an IP address. The new IP addresses are 128 bits wide, which is enough to support 2128 (about 1038) computers.

De lange termijn oplossing is om de lengte van een IP adres te vergroten. De nieuwe IP adressen zijn 128 bits breed, wat genoeg is om 2128)ongeveer 1038) computers te ondersteunen.

Will this always be enough, or will we need to upgrade the addressing system again? There are an estimated 1029 stars in the observable universe. So even if the Internet is extended to include other planets or space aliens, we'll still have enough addresses with IPv6.

Zal dit altijd genoeg zijn, of moeten we het adresseringssysteem opnieuw upgraden? Er zijn geschat 1029 sterren in het waarneembare universum. Dus, zelfs als het Internet uitgebreid is om andere planeten of ruimtewezens te omvatten, hebben we nog genoeg adressen met IPv6.

Is your IP address in IPv4 or IPv6?

Is je IP adres een IPv4 of een IPv6 adres?

Read

Lees

Most likely, the router in your home or school uses a protocol that allows all the computers on the local network (such as in one building) to share a single IP address on the Internet, which can be cheaper. The router that creates the local network gives each computer a local address. For example, although the outside world may think someone's computer has IP address 108.26.181.226, that computer itself might think its address is 192.168.1.11.

Hoogstwaarschijnlijk gebruikt de router bij je thuis of op school een protocol dat alle computers op het lokale netwerk (bijvoorbeeld in een gebouw) toestaat een IP adres op het internet te delen, wat goedkoper kan zijn. De router dat het lokale netwerk creëert, geeft iedere computer een lokaal adres. Een voorbeeld, de buitenwereld kan denken dat iemands computer het Ip adres 108.26.181.226 heeft, maar de computer zelf kan dan denken dat zijn Ip adres 192.168.1.11 is.

Look up your current local IP address in your system preferences or settings. It's usually under network or Internet settings and may be listed with the computer device supporting that connection (wifi, Ethernet, wifi, Bluetooth, etc.).

Zoek je huidige IP adres op in je systeemvoorkeuren of instellingen. Het staat gebruikelijk onder netwerk of internetinstellingen en kan worden vermeld met het apparaat dat de connectie ondersteunt (wifi, Ethernet, Bluethooth, etc.)

The 192.168 domain (the block of IP addresses that all start with 192.168) is reserved for local networks, but no computer on the Internet has an address in that range. Another such domain is 10.0.

Het 192.168 domein (het blok van IP adressen dat begint met 192.168) is gereserveerd voor lokale netwerken, maar geen computer in het internet heeft een adres in dat bereik. Een ander domein zoals dit is 10.0

Unit 4 Lab 2: Communication Protocols, Page 2

Vertalingen:
Unit 4 Lab 2: Communication Protocols, Page 2
Hoofdstuk 4, les 2: Communicatieprotocollen, pagina 2

Reliable Transmission on Unreliable Networks: TCP

Betrouwbare overdrachten op onbetrouwbare netwerken: TCP

Op deze pagina, you will learn the system for ensuring that communication is reliable on the Internet.
Op deze pagina, ga je het systeem leren om te kunnen verzekeren dat communicatie op het internet betrouwbaar is.

Computers, servers, and routers are fairly reliable, but every once in a while a packet will be lost, and devices on the Internet need to tolerate these faults. One way to tolerate faults is not to care. (If you lose one frame of video, it doesn't matter.) Another way (called TCP) is to keep sending packets until they are acknowledged as having been received correctly. ***TCP (Transmission Control Protocol)*** *guarantees reliable data transmission by keeping track of which packets have been received successfully, resending any that have been lost or damaged, and specifying the order for reassembling the data on the other end.*

Computers, servers en routers zijn best betrouwbaar, maar soms raakt er toch een paketje kwijt. Apparaten op het internet moeten deze fouten tolereren. Een manier om fouten te tolereren is door er niks om te geven (het maakt niks uit als je een frame video verlies). Een andere manier (TCP) is om pakketjes te blijven verzenden totdat ze als correct ontvangen worden erkend. **TCP T(ransmission Control Protocol)** garandeert bertrouwbare data overdracht door bij te houden welke pakketjes succesvol zijn ontvangen, de verloren of beschadigde opnieuw te sturen en specificeert de rangschikking om de data aan de andere kant opnieuw in elkaar te zetten.

TCP/IP is a pair of protocols that provide an abstraction. IP lets your computer pretend it has a direct connection to another computer. TCP lets your computer pretend it has a reliable connection to the other computer.
TCP/IP zijn een paar protocollen die voor een abstractie zorgen. IP laat je computer denken dat het een directe verbinding heeft met een andere computer. TCP laat je computer denken dat het een betrouwbare connectie heeft met de andere computer.

If your connection blocks YouTube, watch the video here.

Als je verbinding YouTube blokkeert, bekijk dan hier de video.

The TCP/IP end-to-end design of the Internet is an abstraction:
- *The computers (including servers) at the two endpoints of a communication run the Transmission Control Protocol (TCP), which guarantees reliable transmission.*
- *The routers at every connection point on the Internet run the Internet Protocol (IP), which transmits packets from one IP address to another.*

The routers don't know anything about the messages they carry; all they care about is transmitting them. The computers that send and receive the messages are the only ones concerned with what the messages mean.

Het end to end ontwerp van TCP/IP van het internet is een abstractie:
- De computers (inclusief servers) aan de twee einden van een communicatie runnen het Transmission Control Protocol (TCP), die een betrouwbare overdracht garandeert.
- De routers bij elk verbindingspunt op het internet runnen het Internet Protocol (IP), die pakketjes vervoeren van het ene IP adres naar het andere.

De routers weten niks over de berichten die ze dragen; ze geven alleen om het vervoeren van ze. De computers die de berichten verzenden en ontvangen zijn de enige die iets geven om wat de berichten betekenen.

1. *This project provides a simulation of unreliable data transmission by Internet Protocol.*
    - *Click the green flag to initialize the incoming transmission variables before each experiment.*
    - *Click either character to enter a message for it to send to the other one.*

2. *Compare the result with what you sent. What problems do you see?*

In this simulation, the complete message is a string of text that is divided into packets of one letter each. In reality, the packet length is not so strictly limited and messages are usually much longer.

1. Dit project biedt een simulatie van onbetrouwbare data overdrachten door Internet Protocol aan.
    - Klik op de groene vlag om de binnenkomende overdrachts-variabelen voor elk experiment te initialiseren.
    - Klik op een van beide karakters om een bericht in te voeren om naar de ander te sturen.
2. Vergelijk het resultaat met wat je verstuurd hebt. Welke problemen zie je?

In deze simulatie, is de complete boodschap een rij van tekst die verdeeld is in pakketjes van elk 1 letter. In het echt is de lengte van een pakketje niet zo streng gelimiteerd, berichtjes zijn dus gewoonlijk ook veel langer.

TCP works by including additional information along with each packet so that the receiving computer can keep track of how many packets it has received, re-request any missing packets, and reorder the packets to reconstruct the original message. In this simulation, a packet either arrives correctly (even if it's out of order) or it doesn't arrive at all. But on the Internet, it's possible for a packet to arrive with erroneous data, so the real TCP has to check for errors and request re-transmission of packets with errors too.

TCP werkt door bij elk pakket aanvullende informatie op te nemen, zodat de ontvangende computer kan bijhouden hoeveel pakketten het heeft ontvangen, ontbrekende pakketten opnieuw kan aanvragen en de pakketten opnieuw kan ordenen om het oorspronkelijke bericht opnieuw samen te stellen. In deze simulatie komt een pakket correct aan (zelfs als het niet in orde is) of komt het helemaal niet aan. Maar op internet is het mogelijk dat een pakket aankomt met foute gegevens, dus de echte TCP moet controleren op fouten en moet ook het opnieuw verzenden van pakketjes met fouten aanvragen.
read blown to bits pages 306-309
lees blown to bits pagina 306-309

Build a simple TCP. Resolve the unreliability so that messages are received reliably despite the limitations of IP packets. You'll need to change the definitions of:

Bouw een simpele TCP.. Los de onbetrouwbaarheid op, zodat de berichten betrouwbaar worden ontvangen, ondanks de limitaties van IP pakketjes. Je moet de definities veranderen van:

Do not change the definition of Geen Afbeelding. That block simulates the unreliable network. You could "solve" the problem by rewriting this block to simulate a perfect network instead of an imperfect one, but that misses the point.
Verander de definitie van Geen afbeelding niet. Dat blok bootst een onbetrouwbaar netwerk na. Je kunt dit probleem “oplossen” door dit blok te herschrijven om een perfect netwerk na te bootsen in plaats van een imperfecte, maar dat is niet het punt.

To solve this problem, you'll need a way to keep track of the order of the data and a way to re-request missing packets:

- *First, solve the problem of packets arriving out of order. You can include extra header information in addition to the packet data in order to help the receiver reconstruct the message. This will require cooperation by both sender and receiver (that is, changes to both gray blocks).*
- *Then, solve the problem of packets not arriving at all. That is, make the transmission reliable even though IP is unreliable. This, too, will require changing both sender and receiver.*

Om dit probleem op te lossen, heb je een manier nodig om de volgorde van de data bij te houden en een manier om vermiste pakketjes opnieuw op te vragen.

- Los eerst het probleem op dat pakketjes niet in volgorde aankomen. Je kunt naast de pakket data extra koptekst informatie opnemen om de ontvanger te helpen met het opnieuw in elkaar zetten van het bericht. Dit vereist medewerking van de verzender en de ontvanger (dit betekent wijzigingen in beide grijze blokken.)
- Los daarna het probleem op dat pakketjes helemaal niet aankomen. Dit betekent dat je de overdracht betrouwbaar moet maken, ook al is IP onbetrouwbaar. Dit betekent ook dat wijzigingen bij de verzender en de ontvanger nodig zijn.

Unit 4 Lab 2: Communication Protocols, Page 3

Vertalingen:
Unit 4 Lab 2: Communication Protocols, Page 3
Hoofdstuk 4, les 2: Communicatieprotocollen, pagina 3

A Hierarchy of Open Protocols
Een hiërarchie van open protocollen

Op deze pagina, you will learn about the communication standards used on the Internet and how they work together.
Ga je leren over de standaarden van communicatie die gebruikt worden op het internet en hoe ze samenwerken.

There are billions of devices connected to the Internet, and hundreds of different kinds of devices: laptops, tablets, phones, refrigerators, handheld credit card readers, and so on. How do they all know how to find and talk to each other? Protocols (standards) ensure that the variety of devices interact with each other smoothly.
Er zijn biljoenen apparaten die verbonden zijn met het internet, honderden verschillende soorten: laptops, tablets, telefoons, koelkasten, draagbare credit card lezers en ga maar door. Hoe weten ze allemaal hoe ze elkaar kunnen vinden en hoe ze met elkaar moeten communiceren? Protocollen (standaarden) zorgen ervoor dat de verscheidenheid aan apparaten gemakkelijk met elkaar kunnen communiceren.

There are a lot of protocols! The Internet was designed with several layers of abstraction that sort the protocols according to what part of the process they support.
Er zijn heel veel protocollen! Het internet is ontworpen met verschillende lagen abstractie die de protocollen rangschikt op welk deel van het process ze ondersteunen.

Internet Abstraction Hierarchy
De hiërarchie van internet abstractie

This hierarchy of abstractions manages the complexity of the Internet by hiding the details of lower levels of the system. The highest level of abstraction includes the most general features of the Internet that have to work the same across all devices. At lowers levels of abstraction, things get more device-specific.
De hiërarchie van abstracties beheert de complexiteit van het internet door details te verbergen over de lagere levels van het systeem. De hoogste levels van abstractie omvat de meest algemene kenmerken van het internet dat hetzelfde moet werken bij alle apparaten. Bij de lagere levels van abstractie worden dingen wat meer specifiek per apparaat.

Application Layer Protocols are the highest level of abstraction because they manage how data is interpreted and displayed to users. These protocols give meaning to the bits sent by lower-level protocols; user and server computers must agree on what the bits mean, and application protocols (like HTTP) offer this.
Application Layer Protocols zijn het hoogste level van abstractie, omdat ze beheren hoe data geïnterpreteerd en weergeven wordt aan gebruikers. Deze protocollen geven betekenis aan de bits die verzonden zijn door lagere level protocollen; gebruiker en server computers moeten het eens zijn over wat de bits betekenen, en application protocollen (zoals HTTP) bieden dit aan.

Browsers use HTTP (HyperText Transfer Protocol) to interpret HTML instructions for page formatting. DNS (Domain Name System) converts user-friendly web addresses into IP addresses. Your email inbox may use SMTP (Simple Mail Transfer Protocol) to send and IMAP (Internet Message Access Protocol) to read email.
Browsers gebruiken HTTP (HyperText Transfer Protocol) om HTML instructies voor pagina-opmaak te interpreteren. DNS (Domain Name System) zet gebruiksvriendelijke webadressen om tot IP adressen. De inbox van je email kan SMTP (Simple Mail Transfer Protocol) gebruiken om te verzenden en IMAP (Internet Message Access Protocol) om email te lezen.

Transport Layer Protocols manage the breakdown of a message into packets to be transmitted by lower level protocols and also the reconstruction of the message from the packets upon arrival.
Transport Layer Protocollen beheren dat de afbraak van een bericht naar pakketjes via een lager level protocol wordt verzonden en ook de heropbouw van het bericht van de pakketjes als het arriveert.

TCP (Transmission Control Protocol) simulates a reliable, long-term connection between two computers by only displaying data once all packets have arrived. When speed is more important than accuracy, people use UDP (User Datagram Protocol), such as for real-time video streaming, where one missed packet doesn't matter much.
TCP (Transmission Control Protocol) simuleert een betrouwbare, lange termijn connectie tussen twee computers, door alleen de data te laten zien als alle pakketjes zijn gearriveerd. Wanneer snelheid belangrijker is dan nauwkeurigheid gebruiken mensen UDP (User Datagram Protocol), bijvoorbeeld voor real-time video streaming, waarbij een gemist pakketje niet zo belangrijk is.

Internet Layer Protocols manage the pathways that the data packets travel across networks. These protocols treat the Internet like one large network even though the physical reality on the lower level is one of many tiny subnetworks.

Internet Layer Protocols beheren de paden die pakketjes gebruiken om tussen netwerken te reizen. Deze protocollen behandelen het internet als een groot netwerk, ook al is de fysieke realiteit op het lagere level een van de vele kleine subnetwerken.

Every device on the Internet needs an IP address so other devices can find it. IP (Internet Protocol) addresses are upgrading from IPv4 to IPv6. Routers use Internet layer protocols to detect and work around network congestion.
Elk apparaat op het internet heeft een IP adres nodig zodat andere apparaten het kunnen vinden. IP (Internet Protocol) adressen zijn aan het upgraden van IPv4 naar IPv6. Routers gebruiken Internet Layer Protocols om netwerk ophopingen te ontdekken en eromheen te kunnen werken.

Network Interface Hardware (Link Layer): All Internet devices connect through a physical interface that uses a protocol to manage the connection to the local network. These local protocols are the least abstract because they deal directly with your physical hardware.
Netwerk Interface Hardware (Koppel laag): Alle internet apparaten verbinden door een fysieke interface die een protocol gebruikt om de verbinding met het lokale netwerk te beheren. Deze lokale protocollen zijn het minst abstract omdat ze direct met je fysieke hardware werken.

You may connect to the Internet with an Ethernet cable or perhaps a WiFi radio antenna inside the case of your computer. Either connects computers to a local network router which then connects to an Internet provider. Cell phones use a longer-range cellular connection to a phone carrier.
All four of these levels include more protocols than listed here.
Je kunt met het internet verbinden met een Ethernet kabel of misschien met een wifi radio antenne in de behuizing van je computer. Beiden verbinden computers met een lokale netwerk router, die ze dan verbind met een internet provider. Mobiele telefoons gebruiken een langere bereik mobiele connectie naar een telefoonmaatschappij. Alle vier deze levels omvatten meer protocollen dan hier vermeld.

Open Protocols
Open protocollen

These are all open standards: anyone can look up a protocol and code with it to make new hardware or software without permission. The Internet is probably the largest and most complicated artifact in human history, and it relies on cooperation. Despite some governments' attempts to censor the net, the big picture is one of strong cooperative spirit.
Dit zijn allemaal open standaarden: iedereen kan een protocol opzoeken en ermee coderen om een nieuwe hardware of software te maken zonder toestemming. Het internet is waarschijnlijk het grootste en meest gecompliceerde artefact in de menselijke geschiedenis en het vertrouwt op samenwerking. Ondanks de pogingen van sommige overheden om het net te censureren, is het grote plaatje een van een sterke samenwerking.

Just think...
Your T-Mobile cell phone can talk to your friend's Verizon phone.
You can send email to someone in a country that's considered an enemy of your country (from the US to Iran, for example).
An engineer at Microsoft can read a web page at Apple even though their companies are competitors.
Before the Internet, there were several different network protocols that were secrets belonging to particular manufacturers. So if you had a particular brand of computer or router, it could talk only to other computers of the same brand.

Denk er eens over na…
Je T-Mobile mobieltje kan communiceren met je vriend zijn Verizon mobieltje
Je kunt een email verzenden aan iemand in een land dat als de vijand van je land wordt beschouwd (Van de US naar Iran, bijvoorbeeld).
Een ingenieur van microsoft kan een webpagina bij apple lezen, ook al zijn de bedrijven concurrenten.
Voor het internet, waren er meerdere verschillende netwerkprotocollen die geheim waren en bezit waren van bepaalde fabrikanten. Dus, als je een computer of router had van een bepaald merk, dan kon deze alleen communiceren met andere computers van hetzelfde merk.

Explain how each of these protocols is an abstraction. What details does each one hide?
HTTP: HyperText Transfer Protocol—the protocol that your browser uses to access an HTML web page
DNS: Domain Name System—the hierarchical addressing protocol that is human-readable
TCP: Transmission Control Protocol—the protocol that assures reliable transmission of data
IP: Internet Protocol—the hierarchical addressing protocol that manages routing of data between computers; we are upgrading from IPv4 to IPv6 for more addresses
Leg uit hoe elk van deze protocols een abstractie is. Welke details verbergen ze?
HTTP: Hypertext Transfer Protocol - het protocol dat je browser gebruikt om toegang te krijgen tot een HTML webpagina.
DNS: Domain Name System- Het hiërarchische adresserings protocol dat leesbaar is voor mensen.
TCP: TRansmission Control Protocol- Het protocol dat betrouwbare verzendingen van data verzekerd.
IP: Internet Protocol- Het het hiërarchische adresserings protocol die de routering van gegevens tussen computers beheert; we upgraden van IPv4 naar IPv6 voor meer adressen

Read Blown to Bits pages 309-312.

Unit 4 Lab 2: Communication Protocols, Page 4

Who's In Charge of the Internet?	***Wie is de baas van het internet?***

you will learn about the communities of people who control how the Internet works.	*leer je over de groepen mensen die bepalen hoe het internet werkt.*

Some people think that nobody's in charge of the Internet—that everyone just cooperates freely with no central organization. It's true that free cooperation plays an important role, but people can't just pick any IP address or host name they want, or else there would be conflicts. For example, we can't start a server named bjc.org, because that name is already in use (by a health care provider in St. Louis, Missouri). Until 2009, the Internet domain name hierarchy was entirely controlled by the United States government, with the details delegated to ICANN (the Internet Corporation for Assigned Names and Numbers).	*Sommige mensen denken dat niemand de baas is van het internet -- dat iedereen gewoon vrij samenwerkt zonder centrale organisatie. Het is waar dat vrije samenwerking een belangrijke rol speelt, maar mensen kunnen niet gewoon zomaar elk IP-adres of elke domeinnaam pakken die ze willen, anders zouden er conflicten ontstaan. Bijvoorbeeld, wij kunnen niet een server opstarten die "bjc.org"heet, want die naam is al in gebruik (door een verzekeringsmaatschappij in Missouri). Tot 2009 was de internet domeinnaam hiërarchie volledig in de controle van de overheid van de Verenigde Staten, met de details toegekend aan ICANN (de Internet Corporatie voor Toegewezen Namen en Nummers).*
In 2009 the US Department of Commerce signed a new agreement with ICANN recognizing it as an independent, multinational organization, although it is still under contract with the Department of Commerce to maintain certain principles. International critics are still not satisfied that ICANN is truly independent of the United States.	*In 2009 heeft het Amerikaanse Departement van Handel een nieuw verdrag met ICANN getekend, waarin ICANN wordt erkent als een zelfstandige, multinationale organizatie, hoewel ze nog steeds onder contract zijn bij het Departement van Handel om bepaalde principes te onderhouden. Internationale critici zijn nog steeds niet tevreden over het feit dat ICANN zelfstandig is aan de Verenigde Staten.*
The Power of Open Protocols	*De Kracht van Open Protocollen*
The growth of the Internet has been fueled by open protocols, standards that are not owned by a company.	*De groei van het internet is aangespoord door **open protocollen**, standaarden die niet in bezit zijn van een bedrijf*
Examples of open protocols: Standards for sharing information and communicating between browsers and servers on the Web include HTTP, Simple Mail Transfer Protocol (SMTP) and secure sockets layer/transport layer security (SSL/TLS) Standards for packets and routing include transmission control	*Voorbeelden van open protocollen:* ● *Standaarden voor het delen van informatie en het communiceren tussen browsers en servers op het Web zijn*

protocol/Internet protocol (TCP/IP).	*onder andere HTTP, Simple Mail Transfer Protocol (SMTP), secure sockets layer/transport layer security (SSL/TLS)* ● *Standaarden voor paketten en routing bevatten transmissiecontroleprotocol/Internet Protocol (TCP/IP).*
The protocols for the Internet change over time. The Internet Engineering Task Force (IETF) are the experts in charge of developing and approving these protocols. ICANN controls the DNS hierarchy and the allocation of IP addresses.	*De protocollen voor het internet veranderen na verloop van tijd. De Internet Engineering Task Force (IETF) zijn de experts die verantwoordelijk zijn voor het ontwikkelen en goedkeuren van deze protocollen. ICANN controleert de DNS hiërarchie en de verdeling van IP-adressen.*
Learn more about these organizations.	*Leer meer over deze organisaties.*
The Issue of US Control	*Het Probleem van VS controle*
If you think it's strange for one country to control a worldwide network, you're not alone. Other countries have never been happy about the US control of the Internet, which was officially under US control until 2009 and is still, according to many critics, unofficially dominated by the US government.	*Als je het vreemd vindt dat één land de controle heeft over een wereldwijd netwerk, ben je niet de enige. Andere landen zijn nooit blij geweest met de controle van de VS van het internet., dat tot 2009 officieel in de handen van de VS was, en volgens veel critici nog steeds onofficieel gedomineerd wordt door de Amerikaanse overheid.*
For example until 2009, all DNS domain names had to use the English alphabet, despite constant requests to accommodate other languages.	*Bijvoorbeeld, tot 2009 moesten alle DNS domeinnamen het Engelse alfabet, ondanks constante verzoeken om andere talen te ondersteunen.*

The issue of US control has become much more heated since 2013 when Edward Snowden (shown right, source: Wikipedia) exposed the US National Security Agency (NSA) for spying on Internet traffic worldwide. It's too soon to know how these concerns will eventually be resolved.	*De kwestie over de macht van de VS nam toe in felheid toen in 2013 Edward Snowden (zie rechts, bron: Wikipedia) blootlegde dat de VS Nationale Veiligheidsinstantie spioneerde op wereldwijd internetverkeer. Het is te vroeg om te weten hoe deze kwesties uiteindelijk zullen worden opgelost.*
How Did the US End Up In Charge?	*Hoe heeft de VS de macht gekregen?*
Read Blown to Bits pages 312-316.	*Lees Blown to Bits pagina's 312-316.*

Cryptography

staan geen grammaticale fouten of moeilijk leesbare zinnen in

Symmetric Cryptography

goede aanpassing	***fout origineel***
*Je hebt misschien al een keer een **vervanging-cipher** gebruikt op een bericht te versleutelen. Vervang elke letter van het alfabet met een andere. je kan ze vervangen door elke andere letter, op deze manier;* *De vertaling hiervan staat er al boven op de website, dus dit is geloof ik vergeten weggehaald te worden*	*You might have used a substitution cipher to encode your message, substituting each letter of the alphabet with some other letter. You could substitute letters in any order, like this:*
computers nodig	*computers voor nodig*

Caesar Cipher Project

you will work with the Caesar Cipher.
Ga je werken met de Caesar versleuteling

A Caesar cipher (or shift cipher) is a simple encryption method. Each letter in what's called plaintext (the un-encrypted text) shifts some fixed number of positions along the alphabet. After Z, the shifting "wraps around" and goes back to A. For example, “ABCZ123abcz” shifted by 4 would become “EFGD567efgd”. This technique is named after Gaius Julius Caesar, who ruled Rome 49-44 BC and used encryption in his correspondence.

Een Caesar versleuteling (of schuif-versleuteling) is een simpele versleutelingsmethode. Elke letter in zogenaamde platte tekst (de niet-versleutelde tekst) verschuift een vast aantal posities langs het alfabet. Na Z loopt het verschuiven rond en gaat het terug naar A. Bijvoorbeeld, “ABCZ123abcz” verschoven met 4 zou “EFGD567efgd” worden. Deze techniek is vernoemd naar Gaius Julius Caesar, die over Rome heerste (49-44 v.C.) en versleuteling gebruikte in zijn correspondentie.

In this project you will develop a program that uses a shift cipher that does not wrap around, but instead uses other characters like [and { to follow Z and z.

In dit project ga je een programma ontwikkelen dat een schuif-versluiteling gebruikt dat niet rond loopt, maar in plaats daarvan andere karakters als [en { gebruikt om Z en z te volgen.

Internally, computers store keyboard characters (capital and small letters, punctuation marks, space, digits, symbols, and so on) and others (like Enter, or Command-Z, or Shift-Ctrl A) as numbers—binary sequences. The computer industry standard numbering is called Unicode. For most purposes, even programmers and web developers don't need to know what number represents what character, but sometimes we do need to specify a character by its number. This table shows the Unicode for some of the keyboard characters.

Intern slaan computers toetsenbord tekens (hoofdletters en kleine letters, leestekens, spaties, cijfers, symbolen, enzovoort) en andere (zoals Enter of Command-Z of Shift-Ctrl A) op als cijfers - binaire reeksen. De standaardnummering in de computerindustrie wordt Unicode genoemd. Voor de meeste doeleinden hoeven zelfs programmeurs en webontwikkelaars niet te weten welk nummer welk teken vertegenwoordigt, maar soms moeten we wel een teken specificeren aan de hand van zijn nummer. Deze tabel laat de Unicode zien voor enkele toetsenbordtekens.

The unicode of block reports the number that is used for a particular character:

Het Unicode van blok meldt het nummer dat gebruikt wordt voor een bijzonder karakter.

The unicode as letter block reports the character that a given Unicode number represents:

Het Unicode als letter blok meldt het karakter dat een gegeven Unicode nummer representeert

Why do we see characters like

Waarom zien we karakters als

On paper, use a shift cipher to encrypt and decrypt a short message to get a feel for how this cipher works.

Gebruik, op papier, een schuif-versleuteling om een kort bericht te versleutelen en te ontcijferen, om een gevoel te krijgen hoe deze versleuteling werkt.

Develop an algorithm for this procedure that works for any input text and any shift value.

Ontwikkel een algoritme voor versleuteling procedure dat werkt bij elke tekstinvoer en elke schuifwaarde

Try to code the shift cipher on your own in Snap! using the algorithm you have developed. If you get stuck, look at this page for hints on how to proceed.

Probeer zelf de schuif-versleuteling te coderen in Snap! door het algoritme te gebruiken dat je hebt ontwikkeld. Als je vastloopt kun je op deze pagina kijken voor hints om verder te kunnen.

You can extract the encrypted messages from the Snap! interface by right-clicking on the variable that holds the encrypted message and selecting the “Export” option which will download a text file to your computer which then you can copy/paste.

Je kunt de versleutelde berichten uit de Snap! interface halen door met de rechtermuisknop te klikken op de variabele die de versleutelde berichten bevat en de "export" optie te selecteren, wat een tekstbestand zal downloaden op je computer dat je kan kopiëren/plakken.

Now test your work. Agree with your partner on a shift value for the encryption. Then use your program to encrypt a secret message and e-mail it to your partner. Then let your partner decrypt your message by using the program to reverse the shift.

Test nu je werk. Verzin samen met je partner welke schuifwaarde je gebruikt voor de versleuteling. Gebruik daarna je programma om een geheim bericht te coderen en mail het naar je partner. Laat je partner hierna het bericht ontcijferen door het programma de verschuiving ongedaan te laten maken.

I'm missing some letters. Where did they go?

Ik mis letters. Waar zijn ze heen?

If you copy your encrypted message with a method other than by using copy and paste (for example, by writing it by hand or typing it into a phone), some characters may disappear from your message. This is because some of the Unicode characters after 126 are printing characters that symbolize things like "delete." These characters won't get displayed in Snap!, so you can't copy them by hand, but if you use copy and paste, Snap! knows they are there. In Take It Further exercise A, you can develop a method of encryption that avoids this problem.

Als je je gecodeerde bericht op een andere manier kopieert dan door kopiëren en plakken (bijvoorbeeld door het met de hand te schrijven of in een telefoon te typen), kunnen sommige tekens uit het bericht verdwijnen. Dit komt omdat sommige Unicode-tekens na 126 tekens afdrukken die zaken als "verwijderen" symboliseren. Deze karakters worden niet weergegeven in Snap!, Dus kun je deze niet met de hand kopiëren. Alleen als je kopiëren en plakken gebruikt, weet Snap! dat ze er zijn. In Take It Further, oefening A, kun je een coderingsmethode ontwikkelen om dit probleem te voorkomen.

Implement a version of the Caesar Cipher that not only shifts the characters but also wraps them round the alphabet when the end of the alphabet is reached. You may wish to restrict your alphabet to the set of printable characters given above in the Unicode table.

Voer een versie van de Caesar versleuteling uit dat niet alleen de karakters verschuift, maar ook rond het alfabet gaat als het einde van het alfabet bereikt is. Mogelijk wil je je alfabet limiteren tot de set printbare karakters die hierboven in de Unicode tabel zijn gegeven.

If you came across a long message encrypted in the Caesar Cipher but did not know the shift value, what are some ways you might be able to break the system and decrypt the message? Discuss the weaknesses of a Caesar Cipher and how it is prone to breaking.

Wat zijn sommige van de manier die je kunt gebruiken om het systeem te kraken en het bericht te ontcijferen, als je een lang bericht tegenkomt dat versleuteld is in de Caesar versleuteling, maar je de schuifwaarde niet weet? Bespreek de zwaktes van een Caesar versleuteling en hoe het vatbaar is om gekraakt te worden.

Do some research on other types of ciphers used historically. Especially read about the Vigenere Cipher which was used extensively in communicating sensitive information during World War 2.

Doe onderzoek naar andere types van versleuteling die in de geschiedenis gebruikt zijn. Lees vooral over de Vigenere versleuteling, die gebruikt werd voor het communiceren van gevoelige informatie tijdens de tweede wereldoorlog.

Create your own encryption/decryption scheme and implement it in Snap!.

Creëer je eigen versleutel/ontcijfer schema en voer deze uit in Snap!

Public Key Encryption

you will learn about a commonly used method of cryptography that is more secure.

Ga je leren over een algemeen gebruikte methode van cryptografie die veiliger is.

The fundamental problem that cryptography is trying to solve is how to get a message to your friend that can't be intercepted by your enemies. Symmetric encryption has a fundamental weakness: the encryption key is itself a message that needs to be send to your friend but not intercepted by your enemy.

Het fundamentele probleem dat cryptografie op probeert te lossen, is hoe je een bericht naar je vriend kan sturen zonder dat je vijand deze onderschept. Symmetrische versleuteling heeft een fundamentele zwakte: De coderingssleutel zelf is een bericht dat je naar je vriend moet sturen, wat niet onderschept mag worden door je vijand.

Public key cryptography is a mathematical technique to avoid the need to communicate a secret key from one person to another. Instead, each person has two keys: a private key known only to that person and a public key that everyone in the world is allowed to know. If Bob wants to send Alice a secret message, he encrypts it with Alice's public key. Then no one but Alice can decrypt it. Only her private key can undo the encryption, and no one can figure out the private key from the public key.

Public key cryptografie is een wiskundige techniek om te voorkomen dat je een geheime sleutel van de ene naar de andere persoon moet doorgeven. In plaats daarvan heeft elke persoon twee sleutels: een privésleutel, alleen bekend bij deze persoon en een publieke sleutel die iedereen ter wereld mag weten. Als Bob een geheim bericht wilt sturen naar Anna, dan codeert hij deze met Anna’s publieke

sleutel. Zo kan niemand hem ontcijferen, behalve Alice. Alleen haar privésleutel kan de versleuteling ontcijferen, en niemand kan de privésleutel uit de publieke sleutel halen.

The public key idea was invented and first published by Whitfield Diffie and Martin Hellman in 1976. It turns out that it had been invented earlier but kept secret by governments.

Het publieke sleutel idee is uitgevonden en voor het eerst gepubliceerd door Whitfield Diffie en Martin Hellman in 1976. Het blijkt dat het al uitgevonden was, maar dat het geheim werd gehouden door overheden.

If your connection blocks YouTube, watch the video here, but start it at 2:25.

Als je verbinding Youtube blokkeert, kun je de video hier bekijken, start hem vanaf 2:25.

It may seem incredible that Alice can make her encryption key public and still no one except her can decrypt her message. The public key method relies on some mathematics and on some limitations on the speed of current computers. Read "Secrecy Changes Forever" (Blown to Bits pages 178-181) to understand some of how this works.

Het lijkt misschien ongelooflijk dat Anna haar coderingssleutel openbaar kan maken en alsnog als enige haar bericht kan ontcijferen. De openbare-sleutemethode is gebaseerd op wat wiskunde en op enkele beperkingen van de snelheid van huidige computers. Lees "Secrecy Changes Forever" (Blown to Bits pagina's 178-181) om te begrijpen hoe dit werkt.

Here is a model of public key encryption (from wikimedia.org)

Hier is een model van publieke sleutel versleuteling (van wikimedia.org)

With a partner, discuss how this method is different from symmetric cryptography described on previous pages. Would you trust this method to work to send a credit card number?

Discussieer met een partner over hoe deze methode afwijkt van symmetrische cryptografie, die beschreven werd op de afgelopen pagina's. Zou je deze methode vertrouwen om een creditcardnummer te versturen?

It's also possible to use the private key for encryption and the public key for decryption...
That's no good for secret messages (why not?), but it's useful for digital signatures. I use my private key to encrypt a message; you use my public key to decrypt it. If you get a meaningful message as the result, that proves that the message was encrypted with my private key. (If I want both secrecy and digital signing, I encrypt the message with my private key to sign it, then encrypt the encrypted result again with your public key to keep it secret. You decrypt it twice, first with your private key and then with my public key.) This is a nice example of composition of functions: the output from the first encryption is the input to the second encryption.

Het is ook mogelijk om de privésleutel te gebruiken voor codering en de openbare sleutel voor decodering

Dit is niet goed voor geheime berichten (waarom niet?), Maar het is wel handig voor digitale handtekeningen. Ik gebruik mijn privésleutel om een bericht te versleutelen; je gebruikt mijn publieke sleutel om het te ontcijferen. Als je een zinvol bericht als resultaat krijgt, bewijst dat dat het bericht is versleuteld met mijn privésleutel. (Als ik zowel geheimhouding als digitale ondertekening wil, versleutel ik het bericht met mijn privésleutel om het te ondertekenen, en vervolgens versleutelt ik het versleutelde resultaat opnieuw met jouw openbare sleutel om het geheim te houden. Jij ontcijfert het twee keer, eerst met je privésleutel en vervolgens met mijn openbare sleutel.) Dit is een mooi voorbeeld van samenstelling van functies: de uitvoer van de eerste versleuteling is de invoer naar de tweede versleuteling.

Secure HTTP

Veilige HTTP

Secure HTTP connections (those that use https:// instead of http://) use a protocol called Transport Layer Security (TLS) or maybe an older version called Secure Sockets Layer (SSL). Both are based on public key cryptography. With SSL/TLS, the site you are visiting sends its public key, and your browser uses it to encrypt the information you send.

Veilige HTTP verbindingen (degenen die https:// gebruiken in plaats van http://) gebruiken een protocol genaamd Transport Layer Security (TLS) of misschien een oudere versie genaamd Secure Sockets Layer (SSL). Beide zijn gebaseerd op cryptografie met publieke sleutel. Met SSL/TLS verzend de site de publieke sleutel, je browser gebruikt dit om de informatie die je verzendt te versleutelen .

SSL/TLS (secure sockets layer/transport layer security) is the standard used for cryptographically secured information transfer on the Internet.

SSL/TLS (secure sockets layer/transport layer security) is de standaard die wordt gebruikt voor cryptografisch beveiligde informatieoverdrachten op het internet.

If your connection blocks YouTube, watch the video here, but start it at 4:40.

Als je verbinding Youtube blokkeert, kun je de video hier kijken, maar start hem op 4:40

Open standards help security...
In order to work properly, a cryptographic function has to be easy for the private key holder to invert, but hard for anyone else to invert. How do we know what "hard" means? For example, current cryptographic methods rely on the difficulty of finding prime factors of very large numbers. There's no proof that someone won't come up with a fast way to do that, but people are pretty confident about it because the problem has been well studied by many mathematicians. (On the other hand, when quantum computers become practical, factorization will be easy, and new cryptographic methods will be needed.) What makes it possible for mathematicians to study the difficulty of breaking Internet cryptography is that the method used—the cryptographic function—is openly published. This may seem strange; if you want to keep secrets, shouldn't you keep the technique secret, too? But secret algorithms can have weaknesses that go undiscovered until some bad guy exploits them. Open standards allow an algorithm to be studied before it is used in practice.

Open standaarden helpen de beveiliging ...
Om goed te kunnen werken, moet een cryptografische functie gemakkelijk kunnen worden omgedraaid door de beheerder van een privésleutel, maar moeilijk om te keren door iemand anders.

Hoe weten we wat "moeilijk" betekent? De huidige cryptografische methoden vertrouwen bijvoorbeeld op de moeilijkheid om priemfactoren van zeer grote aantallen te vinden. Er is geen bewijs dat iemand dat niet snel zal bedenken, maar mensen hebben er veel vertrouwen in omdat het probleem door veel wiskundigen goed is bestudeerd. (Aan de andere kant, wanneer kwantumcomputers praktisch worden, zal ontbinding gemakkelijk zijn en zullen nieuwe cryptografische methoden nodig zijn.) Wat het voor wiskundigen mogelijk maakt om de moeilijkheid van het doorbreken van internet cryptografie te bestuderen, is dat de gebruikte methode - de cryptografische functie - openlijk gepubliceerd wordt. Dit lijkt misschien vreemd; als je geheimen wilt bewaren, moet je de techniek dan ook niet geheim houden? Maar geheime algoritmen kunnen zwakke punten hebben die niet worden ontdekt totdat een of andere slechterik ze uitbuit. Met open standaarden kan een algoritme worden bestudeerd voordat het in de praktijk wordt gebruikt.

Certificate Authorities

Certificaatautoriteiten

Public key cryptography doesn't solve all the problems, because an eavesdropper (say, Eve) might publish a fake public key pretending to be Alice. Then Bob might accidentally encrypt their message for Alice using the Eve's fake key, and then the Eve can read the message. In practice, this is partly fixed by relying on trusted third parties, called Certificate Authorities, to certify public keys. In your browser's security options you can see all of the Certificate Authorities that it trusts.

Public key cryptography lost niet alle problemen op, omdat een iemand die afluistert (bijvoorbeeld Eva) een nep public key zou kunnen publiceren die zich voordoet als Anna. Dan kan Bob per ongeluk zijn bericht voor Anna versleutelen met de nep-sleutel van Eva, en dan kan Eva het bericht lezen. In de praktijk wordt dit gedeeltelijk verholpen door een betrouwbare derde partij, de zogenaamde Certificate Authorities, om openbare sleutels te certificeren. In de beveiligingsopties van uw browser kunt u alle certificaatautoriteiten zien die deze vertrouwt.

Certificate authorities issue digital certificates that verify who owns the encryption keys used for secured communications.

Certificaatautoriteiten geven digitale certificaten die verifiëren wie de eigenaar is van de coderingssleutels die worden gebruikt voor beveiligde communicatie

But this just pushes the problem back a layer. How does the Certificate Authorities know that you are who you say you are? The problem is a little bit like how your bank knows that you who you say you are when you call them on the phone. Namely, they ask you questions for which they hope only you know the answer.

Maar dit duwt het probleem alleen een laag terug. Hoe weten de certificaatautoriteiten dat jij degene bent die je zegt dat je bent? Het probleem is een beetje zoals hoe je bank weet dat jij het bent als je belt en zegt dat jij het bent. Ze stellen namelijk vragen waarvan ze hopen dat alleen jij ze weet.

Read "The Key Agreement Protocol" and "Public Keys for Private Messages" (Blown to Bits pages 181-183) for more details on Public Key Encryption.

Lees "The Key Agreement Protocol" en "Public Keys for Private Messages" (Blown to Bits paginas 181-183) voor meer details over publieke sleutel versleuteling.

Do some research about modern encryption systems such as the RSA cryptosystem, which is used to do secure transactions on the Internet

Doe wat research over moderne versleutelingssystemen zoals de RSA cryptosysteem, dat gebruikt wordt om transacties op het internet te beveiligen.

Cybersecurity

vertaling	engels
Oorspronkelijk was de veiligheid van netwerken minimaal. Dit was omdat het Arpanet een klein computernetwerk was vooral gebruikt voor militaire doeleinden en universiteiten. Computerbeveiliging werd pas nodig toen bedrijven ook toegang kregen tot het internet in 1995.	*Originally, network security was a relatively minor consideration because the Arpanet was a small computer network of military personnel and university users. The real need for security arose once businesses were allowed on the Internet in 1995.*
Te veel beveiliging gaat ook niet zonder problemen. Een perfect beveiligd internet zou makkelijk ervoor kunnen zorgen dat je niks meer anoniem kan plaatsen. Om fraude tegen te gaan is het belangrijk om te kunnen bevestigen waar het bericht vandaan komt, maar als de oorsprong van een bericht bevestigd kan worden is het bericht niet meer anoniem. Dat is problematisch aangezien het ten koste gaat van privacy en vrijheid van meningsuiting.	*Too much security has its own set of problems. A perfectly secure Internet could easily end up preventing anonymous publishing. To prevent fraud, it's important to be able to verify the source of a message. But if the source of a message can be verified, the message can't be anonymous. That's problematic both for privacy and for freedom of speech.*
Wie wil de computers van andere mensen aanvallen?	*Who Wants to Attack Other People's Computers?*
In het begin van het gebruik van het internet kwamen de meeste online inbraken van tieners die wilde leren over de inhoud van computersoftware om zich slim te voelen en op te scheppen tegen hun vrienden. Meestal deden ze het niet om schade aan te richten maar vaak gebeurden dat toch. Deels door fouten te maken en deels door het afschrikken van systeem managers die hun systemen niet op het internet durfde te plaatsen.	*In the early days of the Internet, most attacks came from teenagers, who wanted to learn about the insides of computer software, feel smart, and show off to their friends. Most of the time, they didn't intend to do any harm, but often they did anyway, partly by making mistakes, and partly by convincing computer system managers that the early open-access network policies were dangerous.*
Dit alles was voordat computersystemen belangrijk werden voor meer mensen dan alleen Dat was voordat computersystemen voor meer	*That was before computer systems on the Internet became important to people other than their owners. Today, people give their credit card numbers to*

mensen belangrijk werden dan alleen de eigenaren van het systeem. Hedendaags geven mensen hun bank informatie aan webwinkels. Computer controle infrastructuur (zoals energiecentrales, telefoonmasten, stoplichten en ziekenhuis apparatuur) kan aangevallen worden door de krijgsmacht van andere landen. (Als voorbeeld, de Verenigde Staten is zowel een voorbeeld van het slachtoffer als de aanvaller) Er zijn nogsteeds tieneres die een beetje lol maken van het kraken van computers maar dat valt in het niets bij het nummer van serieuze cybercriminals.	*online shopping sites, and computers controlling infrastructure (such as power plants, telephone switching systems, traffic lights, and hospital equipment) can be attacked by other countries' military. (The United States has been both the attacker and the attacked in this sort of incident.) There are still teenagers having fun by attacking computers, but today such cases are far outnumbered by serious criminals and cyber-warriors.*
Gemeenschappelijke veiligheids problemen voor gebruikers	*Common Security Issues for Users*
In software zitten foutjes (bugs), ook in professioneel ontworpen software. Mensen kunnen deze bugs gebruiken om bijvoorbeeld computers te laten crashen of spionage software te installeren en je wachtwoorden stelen. Software ontwerpers proberen bugs te voorkomen en te vinden en te veranderen. maar niet elke bug wordt gevonden en verbeterd.(en niet elke netwerkgebruiker update vaak genoeg om zo min mogelijk last te hebben van deze bugs.	*Software has bugs (even finished software written by professionals). And people can use those bugs for bad purposes (such as crashing your computer or implanting spy software to collect everything you type, including passwords). Software developers try to prevent security bugs and fix them when they turn up, but not every software developer distributes fixes promptly. (And not every computer user keeps up with software updates perfectly!)*
De gebruikelijke term voor programma's die je computer negatief beïnvloeden is *malware* . Een vorm van malware is een *virus* . Computervirussen maken kopieën van zichzelf (net als biologische virussen) en proberen zichzelf te verspreiden naar zoveel mogelijk computers. Mensen gebruiken *firewalls* om connecties met andere netwerken zo beperkt mogelijk te houden. mensen gebruiken *antivirus software* om virussen buiten de deur te houden.	*The general name for programs that try to affect your computer badly is malware. One kind of malware is called a virus. Computer viruses make copies of themselves (just as biological viruses do) and try to spread themselves over the network to other computers. People use antivirus software to help prevent these attacks. People also use firewalls to limit connections into or out of their computer. (Both your computer and your router probably run firewall software.)*
Een andere veel voorkomende aanval strategie heet *phishing*: een aanvaller verstuurd een email die lijkt alsof hij van een officiële organisatie |(zoals je kbank) komt. en je misleid om informatie terug te sturen naar de aanvaller (zoals je pincode).	*Another common attack strategy is called phishing: an attacker sends you an email that appears to be from some official organization (such as your bank) and tricks you into giving information to the attackers (such as your bank password).*
Malware is software speciaal gemaakt om schade te doen aan een computer.	*Malware is software that was designed to harm your computer.*

Een **virus** is een type van malware die zichzelf verspreidt en andere computers infecteerd.	*A virus is a type of malware that spreads and infects other computers.*
Antivirus-software is software speciaal gemaakt om bestanden te scannen en bestanden die geïnfecteerd zijn te verwijderen of in "quarantaine" te zetten.	*Antivirus software is software designed to scan the files on your computer and delete or "quarantine" files that are infected with a virus.*
Een **firewall** is een veiligheidssysteem dat controleert of dat connecties tussen computers en servers veilig zijn.	*A firewall is a security system that controls the kinds of connections that can be made between a computer or network and the outside world.*
Phishing ofwel vissen is een veelgebruikte cyberaanval waarbij je wordt misleid om persoonlijke informatie te geven of om malware te downloaden.	*Phishing is a common security attack in which the victim is tricked into giving up personal information or downloading malware.*
Distributed Denial of Service (DDoS) (verdeeld weigeren van functie) aanval	*Distributed Denial of Service (DDoS) Attack*

een Denial of Service (DoS) aanval bestaat uit het zenden van zo veel aanvragen van informatie op een website dat het netwerk het niet meer aankan. DoS beschadigd geen servers en steelt ook geen wachtwoorden; Het zorgt alleen voor een tijdelijke uitschakeling van een server.	*A Denial of Service (DoS) attack consists of sending a lot of requests to a server at the same time (for instance, requests for a web page or some data). This can overload the server's network bandwidth. A DoS attack doesn't destroy data or collect passwords; it just causes a temporary inability to reach the targeted server so other users of that server are denied service.*
*Een vorm van DDoS aanvallen werkt doordat de aanvaller eerst een virus of een ander soort malware naar honderden of duizenden computers ter wereld tegelijk te sturen. Dit netwerk van geïnfecteerde computers heet een *botnet*. De aanvaller stuurt dan een DoS aanval vanaf het botnet. Naast het vergroten van het aantal aanvragen maakt DDoS het ook moeilijker om te kijken wie voor deze aanval heeft gezorgt aangezien de aanvakl van onschuldige mensen lijkt te komen.*	*A variant is the Distributed Denial of Service (DDoS) attack, in which the attacker first uses viruses and other malware to take control of many (sometimes hundreds of thousands of) computers around the world. This network of infected computers is called a botnet. The attacker then launches a DoS attack from all of the victims' computers at the same time. Besides increasing the number of simultaneous server requests, DDoS makes it harder to determine who is at fault, since the attack seems to come from many innocent people.*
De Hiërarchie van de DNS zorgt dat het systeem effectiever is. Als je bijvoorbeeld snap.berkeley.edu bezoekt, dan hoeft je computer alleen te weten waar de edu naam server is. En die server kan snap.berkeley.edu vinden. aanvaller	*The hierarchy of the DNS makes the system more efficient. When you visit snap.berkeley.edu, your computer only has to know where to find an edu name server. That server only has to know where to find the berkeley.edu server. And that server directs your computer to snap.berkeley.edu.*
Er zijn milioenen van deze DNS aanvragen elke	*There are millions of such DNS requests every*

seconden, en als al die requests zouden moeten beginnen met dezelfde stamnaam server zouden die servers constant over vol zijn. In Plaats daarvan herinneren DNS servers de antwoorden van de host naam vragen, en ze bieden deze aan als je een nieuwe aanvraag gaat doen. Desalniettemin kan het zijn dat als het ip adres veranderd in de tussentijd kan het zijn dat je naar een andere of niet bestaande site gaat. Of erger nog, een gefraudeerde DNS kan je ook expres naar een verkeerde site sturen. dit komt omdat DNS niet optimaal beveiligd is.	*second, and if all of those requests had to begin at the same few root domain servers, those servers would be flooded with too many requests. Instead, DNS servers remember (cache) the results of host name queries, and they provide these remembered (non-authoritative) answers for most requests. However, if the IP address of the site you are requesting changes before before the non-authoritative answer is updated, you may be sent to the wrong site. More critically, a fraudulent DNS server may provide deliberately wrong non-authoritative answers. DNS was not designed to be perfectly secure.*
Wat kan jij doen?	*What Can You Do?*
Er zijn geen perfecte oplossingen die je kan doen om te zorgen dat je nooit slachtoffer wordt van malware. Maar er zijn dingen die je kan doen die erg goed helpen:	*There are no perfect solutions you as an individual person can use to be sure you will never be victimized. But there are things you can do that will help a lot:*
***Blijf bij met de meest recente software updates** Nieuwere software, bijvoorbeeld nieuwere versies van Windows hebben vaak betere online beveiliging.*	*un up-to-date software. The Windows 98 operating system was not sold after 2000, and not supported after 2006. But there are still computers running this obsolete system, including many in the US Department of Defense. [source] Usually, when people keep using obsolete systems, it's because they rely on application software that runs only in the old system.*
***Gebruik goede wachtwoorden** Je hebt andere wachtwoorden voor elke site nodig, en als wachtwoorden makkelijk te onthouden zijn zijn ze ook makkelijk op te zoeken. gebruik een wachtwoordmanager, die genereert automatisch gecompliceerde random wachtwoorden en dan hoef je alleen daarvan het wachtwoord te onthouden.*	*Use strong passwords. You need a separate password for every site you use, and if a password is easy for you to remember, it's also easy for criminals to find in the dictionary. The only good solution is to use a password manager, a program that makes up a random password for every site. You just remember one password, the one for the password manager itself. It takes care of your other ones for you.*
***Klik niet op links** van onbekende sites of Mails. check vooral bij Mails de URL code.*	*Don't click links on web sites or (especially) in email, without first double-checking that the actual URL in the link is the same as the one that's shown in the message. (Where does this link to http://google.com really send you?) Two paragraphs up we said to keep your software up-to-date, and often the way you know there's an update is that a window pops up on your screen. Don't click the "update" button — or even the "close" button — unless you're sure it's really a legitimate update.*
***Gebruik geen dubieuze software**. Als een reclame zegt dat je gratis geld of spullen krijgt is er een grote kans dat het malware is.*	*Don't use iffy software. If the advertising says that the program will get you money, or free stuff, or pornography, or cheats for video games, it's very likely to be malware. A particularly sneaky category is fake antivirus software! Check the reviews in magazines to make sure you're getting what you really want.*

Het vertrouwen schade dat internetgebruikers hebben in hun online privacy en veilige online geldzaken.	

Welke van de onderstaande zijn bestaande zwakheden aan het internet volgens expers?	*Which of the following are existing vulnerabilities of the Internet, according to experts?*
Een fysieke aanval op internet kabels.	*A physical attack that involves cutting fiber-optic cables.*
het elektrische systeem online aanvallen die het elektriciteitsnet bestuurt.	*Attacking electrical systems that control the energy grid.*
Goed maar er zijn mischien betere antwoorden,	*Yes, but there may be more!*
Het vertrouwen schade dat internetgebruikers hebben in hun online privacy en veilige online geldzaken.	*Eroding the trust and confidence that the general public has in their online privacy and secure online transactions.*
Alle bovenstaande.	*All of the above*
Je hebt de vraag succesvol beantwoord.	*You have successfully completed this question!*

Wie geeft iets om versleuteling

Origineel	verbetering
de standpunt die iedere groep zal hebben over dit probleem	welke standpunten iedere groep zal hebben over dit probleem
Onze	ons

de	het
de	het
Geeft	geef

Communicatie en Gemeenschap

origineel	verbetering
ga nadenken	ga je nadenken
Maak met de klas een lijst	maak een lijst met de klas.

Cyberpesten

Geen fouten of moeilijke zinnen gevonden.

Censuur

Origineel	Verbetering
een stelling van de hierboven	een van de bovenstaande stellingen
de hele rond.	*de hele wereld rond*

Zoekmachines

Geen incorrecte zinnen of fouten gevonden.

Verleden en Toekomst:

*Banane - **Banen***

Werkomstandigheden:

werknemenrs

werknemers

websitees

websites

existed before the Internet, but technology has helped grow an "on-demand economy." Many on-demand companies do not have regular employees, but hire independent contractors. This gives workers great flexibility about when they work, but costs them benefits like sick pay, health insurance, collective bargaining, job stability, or unemployment insurance if they are fired.

Bestonden voor het internet, maar technologie heeft geholpen met de groei van een "on-demand economie". Veel on-demand bedrijven hebben geen normale werknemers, maar huren zelfstandigen. Dit geeft werkers een enorme flexibiliteit in wanneer ze werken, maar het kost ze wel voordelen als ziekengeld, gezondheidsverzekering, collectief afdingen, baanstabiliteit of werkloosheidsverzekering als ze ontslagen worden.

Research the on-demand economy. Here are some resources to get you started.

Doe onderzoek naar de on-demand economie. Hier zijn wat bronnen om mee te beginnen.

Examples of

Voorbeelden van

A longer article, but with lots of information

Een langer artikel met veel informatie

An example of how, even though drivers aren't employees, Uber monitors them like employees:

Een voorbeeld van hoe, ook al zijn bestuurders geen werknemers, Uber ze monitort als werknemers.

O*n-demand workers know what they're signing up for, so they shouldn't be suing these companies for not getting benefits.*

On-demand werknemers weten waar ze aan beginnen, dus ze moeten deze bedrijven niet aanklagen omdat ze geen voordelen krijgen.

The on-demand economy just helps the rich get richer and the poor get poorer.

De On-demand economie helpt de rijken om rijker te worden en de armen om armer te worden.

It is hard for a traditional company with employees to compete with the on-demand model.

Het is moeilijk voor een traditioneel bedrijf met werknemers om het op te nemen tegen het on-demand model.

Think of an idea for an on-demand company you might launch.

Bedenk een idee voor een on-demand bedrijf dat je kan lanceren.

Computers op werk:

origineel	*verbetering*
betekenen	betekend
zin	zijn
van ver te werken.	op afstand te werken
zegen dat	zeggen:

Hoofdstuk 5: Algoritmes en Simulaties

LES 1 p.1	
project link	projectlink
klik de foto	klik op de foto
kunnen spelen	kunnen gebruiken
houd bij	*houd je bij*
De beste wat ik deed was 12 gissingen.	*Het beste resultaat was 12 keer raden.*
LES 1 p.2	

ga je zien hoe de eigenschappen van een lijst het algoritme voor zoeken in die lijst, kan beïnvloeden.	ga je zien hoe de eigenschappen van een lijst kunnen beïnvloeden hoe het algoritme voor zoeken in die lijst is.
of	óf
in een gesorteerde data	in gesorteerde data
reporteren	rapporteren
de zelfde	dezelfde
over het algemeen	in het algemeen
hebben	hebben.
raad spel	raadspel

en wat	en
that	dat
lijst	lijst,
zijn	zijn.
LES 1 p.3	
dat	of
verschillen./p>	verschillen.
het item	het derde item

de,	de vierde
Deze talen voor menselijk begrip kunnen helpen bij het schrijven van het algoritme in een programmeertaal.	Deze talen kunnen helpen voor menselijk begrip bij het schrijven van het algoritme in een programmeertaal.
predicaat	predikaat
die een lijst als invoer gebruiken en rapporteert een nieuwe lijst met dezelfde elementen als de invoerlijst maar zonder dubbele elementen.	die een lijst als invoer gebruikt en een nieuwe lijst met dezelfde elementen als de invoerlijst, maar zonder dubbele elementen rapporteert.
LES 2, p.1	
new	nieuw
een	één
designprocess	designproces

niet praktisch	onpraktisch
LES 2, pg. 2	
Alleen zul je merken	*Je zult alleen merken,*
is het	*het is*
Les 2 Pg 3	
wil	wilt
Les 3 Pg 1	
manieren sneller	***manieren zijn die***

IK	***Ik***
Les 3 pg 2	***Geen gekke zinnen of fouten gevonden***
Les 3 pg 3	
onredelijketijd	***Onredelijketijd***
Les 4 pg 1	***Geen gekke zinnen of fouten gevonden***
Les 4 pg 2	
probleemis	***probleem is***
Dhe	***De***

function	***functie***
oneindig zich	***zich oneindig***
testtercode	***testercode***
zoals wat	***die***
Les 5 pg 1	
kan	***kunnen***
Les 5 pg 2	
hetleger	***het leger***

een nucleaire oorlog per ongeluk	***per ongeluk een nucleaire oorlog***
Les 5 pg 3	***Geen gekke zinnen of fouten gevonden***