6 4 Cryptografie

Auteur	Bètapartners
Team	Wikiwijs Maken Auteurs
Laatst gewijzigd	29 oktober 2014
Licentie	CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie
Webadres	https://maken.wikiwijs.nl/45975/

Inhoudsopgave

4 Cryptografie

In dit thema worden de volgende onderwerpen besproken:

- Cryptografie
- Simpele methodes
- RSA
- Versleutelde E-Mail

4.1 Inleiding

Cryptografie houdt zich bezig met het omzetten van een bericht of bestand in geheimtaal. Het voordeel hiervan is dat pottenkijkers niet meer mee kunnen lezen. Alleen de ontvanger, die de beschikking heeft over de juiste sleutel, kan uit het geheimschrift de originele boodschap terugkrijgen. Cryptografie wordt tegenwoordig veel toegepast: bijvoorbeeld in gsm's, pinautomaten, de chipknip of de decoder van de TV. Cryptografie wordt ook gebruikt om bestanden te versleutelen, e-mails te coderen of om afgeschermde websites mee te bekijken. In dit hoofdstuk houden we ons vooral bezig met het versleutelen van e-mailberichten. Welke mogelijkheden zijn er om je e-mailberichten te vertalen in geheimtaal zodat niemand mee kan lezen?

Drie belangrijke begrippen in de cryptografie zijn:
Encryptie : het versleutelen van de informatie door de zender
Decryptie : het weer ontcijferen van de informatie door de ontvanger.
Sleutel : De sleutel wordt gebruikt om de informatie te encrypten en ook om de informatie te decrypten

4.2 Simpele methodes

Julius Caesar was de eerste die op vrij grote schaal gebruik maakte van cryptografie. Hij gebruikte geheimschrift om zijn leger te informeren. De methode die Julius Caesar gebruikte is een van de simpelste vormen van cryptografie en werkt als volgt: Elke letter in een bericht werd in het alfabet drie plaatsen opgeschoven, dus een A werd een D, een B werd een E enzovoort. Een X werd weer een A. Deze methode van Julius Caesar is te makkelijk te kraken en wordt niet meer gebruikt in cryptografie.

In de Tweede Wereldoorlog dachten de Duitsers na over een betere encryptiemethode en kwamen met de Enigma. De Enigma is een soort typemachine die uit drie onderdelen bestaat: drie code-wielen, het toetsenbord en een paneel met lampen waarbij elke lamp bij een letter hoort.

Eerst moest een begininstelling van de enigma gekozen worden. Deze begininstelling werd uit een codeboek gehaald waar voor elke dag een andere instelling stond. Daarna kon de boodschap ingetoetst worden. De drie code-wielen vertaalden elke letter drie keer naar een geheime letter die werd aangegeven op het paneel van lampen.

Het voordeel van deze methode was dat na elke letter de code-wielen draaiden. Een letter W werd dus elke keer in een andere geheime letter vertaald. Het nadeel van deze methode was dat iedereen die de berichten wilden ontcijferen hetzelfde codeboek voor de begininstelling moesten hebben. Deze codeboeken moesten dus verspreid worden over het hele Duitse leger.

Uiteindelijk werd de code van de Enigma toch gekraakt door de Polen en de Britten. Ook de Enigma wordt niet meer gebruikt in hedendaagse cryptografie. Tegenwoordig heb je een betere beveiliging nodig.

Klik hier om naar de bron van de afbeelding te gaan.

Opdracht

Op deze pagina kun je de werking van de enigma-machine bekijken. Wat is het gecodeerde bericht van het woord Hallo?

Verander nu onder de knop settings de volgorde van de codewielen in 123 i.p.v. 312. Wat is nu het

gecodeerde bericht van het woord hallo?

4.3 RSA

De voorbeelden die we tot nu toe gezien hebben zijn voorbeelden van symmetrische cryptografie. Dit betekent dat je dezelfde sleutel nodig hebt voor het encrypten en decrypten van een bericht. Het probleem hiervan is dat je de sleutel moet doorgeven en hierdoor kan deze onderschept worden. De onderschepper kan de berichten dan meelezen.

Tegenwoordig wordt gebruikt gemaakt van asymmetrische cryptografie. Bij asymmetrische cryptografie zijn twee verschillende sleutels nodig: een sleutel om de informatie te encrypten, en een andere sleutel om de informatie te decrypten.

De meest bekende encryptiemethode tegenwoordig is RSA. Deze methode maakt gebruik van asymmetrische cryptografie en van priemgetallen. Dit maakt de RSA methode heel veilig. RSA is genoemd naar de initialen van de uitvinders: Rivest, Shamir en Adleman.

Priemgetallen

RSA maakt gebruik van de eigenschappen van priemgetallen, daarom gaan we eerst in op wat dat precies zijn. Priemgetallen zijn getallen, die alleen door 1 en zichzelf deelbaar zijn. Het getal 9 is geen priemgetal want 9 is deelbaar door 3. Het getal 17 is wel een priemgetal. Er is geen getal denkbaar waar 17 een geheel aantal malen door te delen is.

Er is niet één priemgetal aan te duiden als het grootste. Er bestaat wel het grootste priemgetal dat tot nu toe bekend is. De Duitse oogarts Martin Nowak heeft in maart 2005 het grootste priemgetal tot nu toe ontdekt. Dit priemgetal bestaat uit maar liefst 7.816.230 cijfers. De eerste persoon die een priemgetal van 10 miljoen cijfers vindt, wint 100.000 dollar.

Priemgetallen hebben een speciale eigenschap: elk geheel getal kan worden gemaakt door bepaalde priemgetallen te vermenigvuldigen. Dit kan maar op één manier. Zo kun je het getal 42 maken door de priemgetallen 2,3 en 7 met elkaar te vermenigvuldigen (2 * 3 * 7 = 42). Er is geen andere combinatie van priemgetallen mogelijk die je met elkaar kunt vermenigvuldigen en die 42 oplevert.

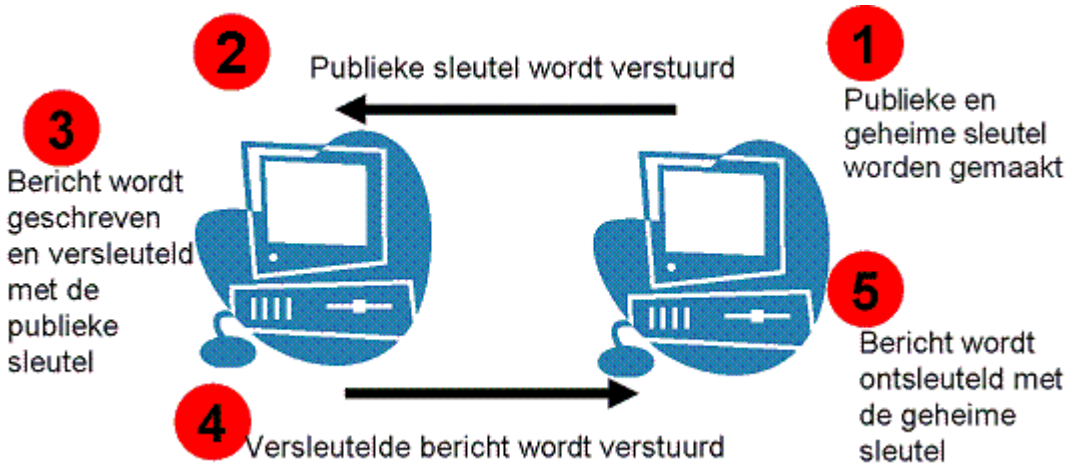
RSA en priemgetallen

RSA maakt gebruik van deze eigenschap van priemgetallen. Zoals we al eerder hebben gezien maakt RSA gebruik van twee sleutels: een publieke sleutel en een geheime sleutel. De publieke sleutel mag iedereen weten en deze sleutel is nodig om een bericht te encrypten. De geheime sleutel moet je goed geheim houden en met behulp van deze sleutel kun je een bericht decrypten. De publieke sleutel kun je maken door twee priemgetallen met elkaar te vermenigvuldigen. Bijvoorbeeld 2027 * 6359 = 12889693. de publieke sleutel is dus nu 12889693. Met deze sleutel kun je een bericht encrypten.

Om het bericht vervolgens te decrypten heb je de getallen 2027 en 6359 nodig.Het is niet makkelijk om erachter te komen welke priemgetallen je met elkaar moet vermenigvuldigen om de publieke sleutel te krijgen. Bij kleine getallen is dit nog wel mogelijk zoals je hebt gezien. Maar bij heel grote getallen is dit niet mogelijk - tenminste met de computers die we tot nu hebben. Als je een bericht veilig wilt versturen heb je een heel grote publieke sleutel nodig.

4.4 Versleutelde E-Mail

Welke stappen moet je nu ondernemen om een beveiligde e-mail te sturen? Hieronder zie je de vijf stappen:



Om publieke en geheime sleutels te genereren kies je twee heel grote priemgetallen. De getallen noemen we P en Q. Aan de hand van deze priemgetallen genereert de computer drie getallen.

1. Getal N : N = P * Q
2. Getal D
3. Getal E

Als je wil weten hoe de getallen D en E gegenereerd worden kijk dan op Wikipedia. Getal N en E zijn je publieke sleutels. Je publieke sleutel is openbaar en iedereen mag deze weten. Getal D is de geheime sleutel. Hoe langer deze sleutel is, hoe betrouwbaarder de codering zal zijn.

Om een bericht veilig te versturen kun je het coderen met behulp van iemand anders zijn publieke sleutel. Hierna kan de ontvanger het bericht decoderen met zijn geheime sleutel. De publieke sleutel van de ontvanger moet dus bekend zijn. De geheime sleutel wordt echter nooit verzonden, wat deze methode behoorlijk veilig maakt.

Opdracht

Maak nu de opdracht "Cryptografie" uit het menu-onderdeel "Opdrachten en Toetsen".

Over dit lesmateriaal

Colofon

Auteurs	Bètapartners
Team	Wikiwijs Maken Auteurs
Laatst gewijzigd	29 oktober 2014 om 13:33
Licentie	De Nederlandse Creative Commons 3.0 licentie waarbij de gebruiker het werk mag kopiëren, verspreiden en doorgeven en afgeleide werken mag maken onder de voorwaarden: Naamsvermelding en Gelijk Delen, zie http://creativecommons.org/licenses/by-sa/3.0/nl/. Meer informatie over de CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie licentie.

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Leerniveaus	VVE, HAVO 4, Praktijkonderwijs, VWO 4
Leerinhoud en doelen	Informatica
Eindgebruiker	leerling/student
Trefwoorden	a1 wetenschap en technologie, a2 maatschappij, e-klassen rearrangeerbaar