Public Key Cryptography

de wiskunde van het perfecte kopje koffie

Wieb Bosma

Radboud Universiteit Nijmegen

Bachelordag

2 april 2011

Cryptografie is

> *de wetenschap van het ontwerpen en kraken van systemen om geheime informatie te delen.*

Er wordt meestal gebruikt gemaakt van een bekend systeem met geheime sleutels om de informatie te versluieren. In een klassiek cryptosysteem spreek je samen geheime sleutels af alvorens je kunt beginnen.

Probleem

Hoe wissel je geheime sleutels uit?

Antwoord

Met *public key* cryptosystemen!

Bij een klassiek cryptosysteem kun je denken aan het volgende brandkastmodel:

er zijn inbraakveilige brandkasten in omloop die met een degelijk hangslot afgesloten kunnen worden. Om met iemand anders geheime informatie uit te kunnen wisselen, kies je samen een hangslot met twee identieke sleutels (en niemand anders krijgt dezelfde sleutel).

Bij het verzenden van een bericht stopt de één de geheime informatie in de brandkast, doet het hangslot op slot, en de brandkast wordt naar de ander gebracht, die met de andere sleutel toegang krijgt tot het geheime bericht.

Maar hoe wissel je de geheime sleutels uit?

nog een analogie

Het slimme idee achter een public key cryptosysteem is dit:

degene die de geheime boodschap in de brandkast stopt, hoeft daarna helemaal niet meer in staat te zijn om het slot zelf weer open te maken: de zender heeft helemaal geen sleutel nodig! Denk aan een open hangslot dat je dicht kunt klikken, maar dan niet zonder sleutel weer kunt openen.

Iedereen mag dus de open hangsloten van de ontvanger hebben en kan informatie uitsluitend voor de ontvanger beschikbaar maken door zo'n slot op een brandkast dicht te klikken.

Waar is de wiskunde?

Informatie in de vorm van getallen, electronisch opgeslagen. We zoeken een één-richtingsfunctie: makkelijk toe te passen maar moeilijk ongedaan te maken, tenzij je extra, geheime, informatie kent.

De één-richtingsfunctie fungeert als hangslot, de extra informatie is de sleutel.

Iedereen mag de één-richtingsfunctie toepassen, slechts 1 persoon kan de bewerking ongedaan maken.

Definities

De *natuurlijke getallen* zijn $1, 2, 3, 4, \ldots$.

Een *priemgetal* is een natuurlijk getal $p > 1$ dat alleen deelbaar is door 1 en p zelf.

Een *samengesteld getal* is een natuurlijk getal n met meer delers dan alleen 1 en n.

Voorbeelden

2, 3, 19 en 31 zijn priemgetallen

$6 = 2 \times 3$ en $33 = 3 \times 11$, en $150 = 2 \times 75 = 3 \times 50 = 2 \times 3 \times 5^2$ zijn samengestelde getallen

1 is geen priemgetal en is ook niet samengesteld

Stelling

Er zijn oneindig veel priemgetallen en oneindig veel samengestelde getallen

Paradox

Om met de definitie te bewijzen dat 31 *een priemgetal* is, kun je laten zien dat 31 niet deelbaar is door $2, 3, 4, 5, 6, \ldots, 29, 30$.

Om te bewijzen dat 33 *geen priemgetal* is hoef je alleen maar een echte deler te vinden: inderdaad is 3×11 gelijk aan 33.

Dit is een paradox omdat veel cryptografische systemen juist gebaseerd zijn op de volgende eigenschap:

> *Van een groot getal is gemakkelijk vast te stellen of het een priemgetal of een samengesteld getal is. Maar van een product van grote priemgetallen zijn de delers moeilijk te vinden!*

Dit is niet een echte tegenspraak:

- er zijn veel betere methoden om te zien of een getal een priemgetal is dan testen of het delers heeft; gebruik andere karakteristieke eigenschappen
- het is wel eenvoudig om na te gaan dat een ontbinding klopt $(33 = 3 \times 11)$ maar de beste methoden om de factoren van grote getallen te vinden zijn niet vergelijkbaar veel beter dan het proberen van de mogelijkheden

Conclusie

Het vermenigvuldigen van grote priemgetallen is een goede één-richtingsfunctie

Het vergt wat meer eerstejaarswiskunde om hier een mooie toepassing van te geven.
We gaan over op een andere één-richtingsfunctie: machtsverheffen modulo p.

Machtsverheffen modulo p: we werken alleen met getallen van 0 tot en met $p-1$.
Van een getal groter dan $p-1$ trekken we p af tot het kleiner is geworden.

Voorbeeld $p = 5$

Nu is $2^3 = 8$ groter dan 4, dus we trekken er 5 af en schrijven

$2^3 = 8 \equiv 3$ modulo 5

Laten we dit voor alle machten van 2 modulo $p = 5$ doen:

$2^1 = 2$ modulo 5

$2^2 = 4$ modulo 5

$2^3 = 8 \equiv 3$ modulo 5

$2^4 = 16 \equiv 1$ modulo 5

$2^5 \equiv 2$ modulo 5,

enzovoort, want we zijn rond!

We hebben zo alle getallen 1,2,3,4 tussen 0 en 5 gevonden als macht van 2

Stelling

Bij elke p is (gemakkelijk) een w te vinden zodat modulo p de getallen $w^1, w^2, \ldots, w^{p-1}$ precies alle getallen van 1 tot en met $p-1$ opleveren.

Voorbeeld $p = 31$ en $w = 3$, dan

$3^1 = 3$ modulo 31

$3^2 = 9$ modulo 31

$3^3 = 27$ modulo 31

$3^4 = 81 \equiv 50 \equiv 19$ modulo 31

$3^5 = 3 \times 3^4 \equiv 3 \times 19 \equiv 57 \equiv 26$ modulo 31

en als we door gaan vinden we:

$16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1$

Definitie

Een getal w zodat $w^1, w^2, \ldots, w^{p-1}$ modulo p precies alle getallen $1, 2, \ldots, p-1$ geven, heet een primitieve wortel modulo p.

Merk op dat

- de getallen in een rare volgorde optreden.
- 1 nooit een primitieve wortel modulo p is (behalve voor $p = 2$)
- 3 is een primitieve wortel modulo 31, maar 2 is dat niet:

  $2^1 \equiv 2$ modulo 31

  $2^2 \equiv 4$ modulo 31

  $2^3 \equiv 8$ modulo 31

  $2^4 \equiv 16$ modulo 31

  $2^5 \equiv 32 \equiv 1$ modulo 31

  en daarna herhaalt het zich

Machtsverheffen modulo p is heel eenvoudig.

Omgekeerd, gegeven een getal r modulo p is er geen methode bekend die heel veel efficiënter de macht e vindt waarvoor $w^e \equiv r$ modulo p dan door te proberen.

Voorbeeld

$p = 31$ en $r = 22$, dan vinden we in het lijstje dat $3^{17} \equiv 22$ modulo 31.

Conclusie

Machtsverheffen modulo p is een goede één-richtingsfunctie!

Toepassing: wachtwoord

Kies een priemgetal p van 30 cijfers met een primitieve wortel w.

Laat elke gebruiker van een computersysteem een getal k van 30 cijfers kiezen, het wachtwoord. Sla in een bestand de paren op bestaande uit de login-naam en w^k modulo p. Als de gebruiker zich wil aanmelden, geeft hij de login-naam en het geheime getal k; het systeem controleert dat de opgeslagen waarde gelijk is aan w^k modulo p.

De systeembeheerder kent ook de waarde van k niet, en kan dus het wachtwoord wel controleren maar niet geven!

Toepassing: geheime sleutels delen

Doel: gebruikers A en B worden het eens over een geheime sleutel, zonder bij elkaar te komen en door uitsluitend over een openbaar netwerk te communiceren.

Kies priemgetal p en primitieve wortel w, en maak die openbaar.

- gebruiker A kiest geheime sleutel a (getal tussen 0 en p)
- A stuurt w^a modulo p naar B
- gebruiker B kiest geheime sleutel b (getal tussen 0 en p)
- B stuurt w^b modulo p naar A
- A berekent $(w^b)^a \equiv w^{b\times a} \equiv w^{a\times b}$ modulo p,
- B berekent $(w^a)^b \equiv w^{a\times b}$ modulo p.
- beiden kennen nu het geheime getal $w^{a\times b}$ modulo p.

Een eventuele afluisteraar ziet w^a en w^b maar we weten niet hoe daar $w^{a\times b}$ modulo p uit te halen!

In ieder geval lukt dat niet door te vermenigvuldigen: $w^a \times w^b = w^{a+b}$ en dat is vrijwel nooit hetzelfde als $w^{a\times b}$.

Deel het geheime recept van het perfecte kopje koffie

Zowel koffiedrinker A als B maakt volgens openbaar recept zwarte koffie (p en w).

Koffieliefhebber A voegt precies de juiste (geheime) hoeveelheid melk (a) toe en stuurt daar B een kopje van. En genieter B maakt een kopje met precies de juiste (geheime) hoeveelheid suiker (b) en stuurt dat naar A.

Nu kunnen A en B aan het ontvangen kopje respectievelijk de juiste hoeveelheid melk en suiker toevoegen om beiden hetzelfde perfecte kopje koffie te krijgen!

Een eventuele onderschepper C kan de hand leggen op koffie met precies de juiste hoeveelheid suiker, èn op koffie met precies de juiste hoeveelheid melk, maar hoe brouw je daar het perfecte kopje koffie uit? Niet door de twee kopjes bij elkaar te gooien ...