Elliptische krommen cryptografie

Quirijn Meijer (4205197)

03 Juli 2015

Inhoud

1 Gebruiken van cryptografie

Cryptografie ontleent zijn belang aan de noodzaak gevoelige over te dragen informatie voldoende te beschermen van onbevoegde partijen, zodanig dat enkel verzender en ontvanger het bericht in kunnen zien. Om dit te bereiken wordt het bericht versleuteld door de verzender, waarna de ontvanger deze kan ontsleutelen. Het algoritme dat hiervoor gebruikt wordt moet zo gekozen worden dat zij garandeert dat eenieder anders dan de bestemde ontvanger het onderschept bericht niet kan ontsleutelen. Er wordt vooralsnog aangenomen dat dit geheel onmogelijk maken een onmogelijkheid in zichzelf is. In realiteit worden om deze reden de algoritmen zo ontworpen dat een bepaalde mate van veiligheid gegarandeerd kan worden. Voor vele algoritmen houdt deze mate van beveiliging verband met de sleutel die gekozen wordt. Hierdoor kan de beveiliging van een boodschap naar behoeven gekozen worden. Dit betekent echter niet dat een dergelijke sleutel een pijler is voor de veiligheid van ieder willekeurig algoritme. De komende hoofdstukken in dit verslag zullen de theorie benodigd om op veilige wijze een gemeenschappelijke sleutel vast te stellen uit de doeken doen. Voor dit gebeurt volgt nog enkele achtergrondinformatie.

Het dagelijks leven biedt vele voorbeelden van cryptografie. Op het internet wordt bij vrijwel iedere vorm van identificatie het verkeer versleuteld. Specifieke voorbeelden zijn het inloggen op websites, het doen van aankopen via het internet, of internetbankieren. Een voorbeeld buiten het internet om is het opnemen van geld bij een geldautomaat.

De Enigma machine, gebruikt door de Wehrmacht tijdens de tweede wereldoorlog, verdient een eervolle vermelding. Deze machine werd gebruikt om de oorlogsmachine op afstand te coördineren. Het breken van de encryptie van de Enigma met behulp van de Bombe is een klassiek voorbeeld van de samenkomst van cryptografie en de computer.

2 Het trapdoor principe

Een groot deel van de efficiëntie van een cryptografisch systeem berust op de eenvoud waarmee informatie versleuteld en ontsleuteld kan worden wanneer de benodigde parameters bekend zijn, en de moeilijkheid van de ontsleuteling wanneer deze deels of niet bekend zijn. Het doel van het versleutelen van informatie is immers het afschermen van de informatie voor partijen die niet specifiek toegang tot de informatie verleend zijn. Dit mag echter geen hinder vormen voor de vertrouwde partijen. Een cryptografisch systeem moet zodoende beschikken over de eigenschap dat zij eenvoudig toepasbaar is, maar lastig omkeerbaar door kwaadwillenden. Een functie die deze eigenschappen bezit wordt een trapdoor-functie genoemd Dit is een metafoor voor een werkelijk valluik: één richting volgen moet eenvoudig zijn, de tegengestelde richting niet. De trapdoor-functie in dit verslag zal het Diffie-Hellman protocol zijn, welke zich baseert op de theorie van elliptische krommen over eindige velden van priem orde. Het achterliggend probleem dat de veiligheid van dit protocol waarborgt is het elliptische kromme discreet logaritmisch probleem.

3 De theorie van elliptische krommen

Een elliptische kromme $\mathrm{K}(\mathbb{R})$ wordt gedefiniëerd door alle paren (x, y) in $\mathbb{R}$ die voldoen aan de volgende vergelijking:

$$\mathrm{K}(\mathbb{R}) : y^2 = x^3 + ax + b$$

voor $a, b \in \mathbb{R}$, met als randvoorwaarde dat de discriminant

$$\Delta_{\mathrm{K}} = -16(4a^3 + 27b^2)$$

ongelijk is aan 0. Deze voorwaarde garandeert dat de kromme niet-singulier is. Als conventie wordt vervolgens een afzonderlijk punt in oneindigheid toegevoegd. De punten op deze krommen kunnen nu onderling opgeteld worden, met als resultaat een som van de punten die zich wederom op de kromme bevindt. Evenzo kan een scalaire vermenigvuldiging met dezelfde eigenschap gedefiniëerd worden. Een belangrijke observatie is dat wanneer de punten op de kromme niet langer genomen worden uit $\mathbb{R}$, maar uit een eindig lichaam $\mathbb{F}_p$ van priem orde p, deze eigenschappen behouden blijven. De resulterende grafiek van de kromme zal van aangezicht veranderen en begrensd worden in het vlak. Onder deze restricties is het mogelijk de verzameling punten $\mathrm{K}(\mathbb{F}_p)$ tezamen met de operatie van optelling van punten te nemen om een groep $\mathbf{G} = [\mathrm{K}(\mathbb{F}_p), +]$ te vormen. Merk op dat niet iedere kromme aan de voorwaarden om een welgedefiniëerde groep te vormen hoeft te voldoen, maar de voor cryptografische doeleinden voorgeschreven krommen dit wel doen. Merk tevens op dat, omdat $\mathbf{G}$ priem orde heeft, de groep cyclisch en daardoor abels is. Een opsomming van deze groep is als volgt:

- Voor alle punten P, Q op de kromme $\mathrm{K}(\mathbb{F}_p)$ geldt dat de som $P + Q$ op de kromme ligt. De groep $\mathbf{G}$ is gesloten onder de groepsoperatie.

- De groepsoperatie is associatief. Ofwel, voor $P, Q, R \in \mathbf{G}$ geldt $P + (Q + R) = (P + Q) + R$.

- Het toegevoegde punt in oneindig wordt gerelateerd aan het eenheidselement $e_{\mathbf{G}}$.

- Voor iedere $P \in \mathbf{G}$ bestaat een element $P^{-1} \in \mathbf{G}$ zodat $P + P^{-1} = P^{-1} + P = e_{\mathbf{G}}$.

Deze groepseigenschappen zijn niet vanzelfsprekend, maar behoeven een te uitgebreid bewijs voor dit verslag. Het volstaat te concluderen dat een groep bestaat welke correspondeert met de kromme $\mathrm{K}(\mathbb{F}_p)$.

4 Het Diffie-Hellman protocol

Het Diffie-Hellman protocol is een systeem dat de uitwisseling van cryptografische sleutels tussen twee partijen beveiligt. Hier op volgend kan deze sleutel gebruikt worden om de communicatie tussenbeide te beveiligen.

Er wordt aangenomen dat de variabelen (a, b, p) die een elliptische kromme $\mathrm{K}(\mathbb{F}_p)$ definiëren publiek bekend zijn, en dat verzender en ontvanger overeenstemmen deze kromme te gebruiken. Daarnaast is een specifiek genererend element k van de groep $\mathbf{G}$ behorend bij deze kromme bekend bij beide partijen. De communicatie vindt vervolgens plaats zoals voorgeschreven door het volgende stappenplan.

1. De eerste partij kiest een getal $\lambda \in [1, p-1]$ en zendt de tweede partij het punt k^λ toe. De verzender beschikt nu over een sleutel (λ, k^λ) waarin λ de zogeheten privé-sleutel is, en k^λ de publieke sleutel.

2. De tweede partij kiest een getal $\mu \in [1, p-1]$ en stuurt de publieke sleutel k^μ als reactie.

3. De tweede partij berekent het punt $(k^\lambda)^\mu = k^{\lambda\mu}$.

4. De eerste partij berekent het punt $(k^\mu)^\lambda = k^{\mu\lambda}$, welke dankzij de commutativiteit van de groep $\mathbf{G}$ gelijk is aan $k^{\lambda\mu}$. Dit punt zal in het vervolg met C aangeduid worden..

Beide partijen beschikken nu over hetzelfde punt C. Omdat alleen de punten k^λ en k^μ gepubliceerd zijn is het voor een derde partij die een van beide onderschept onmogelijk C te berekenen zonder dat μ danwel λ bij deze partij bekend is. Deze partij kan pogen een van beiden uit de publieke sleutels te winnen, om hiermee C te berekenen. Het volgend hoofdstuk verklaart waarom deze aanpak geen vruchtbare onderneming is.

5 Het discreet logaritmisch probleem

Gegeven een punt l uit de groep $\mathbf{G}$, en een genererend element $k \in \mathbf{G}$. Het discreet logaritmisch probleem is de naam gegeven aan het probleem ν te vinden zo dat $l = k^{\nu}$. De naam is vanzelfsprekend afgeleid uit het feit dat voor deze combinatie geldt dat $\nu = \log_k(l)$. Het Diffie-Hellman protocol baseert zich op de aanname dat geen voldoende efficiënte algoritmen bestaan om dit getal ν te vinden. Voorbeelden van algoritmen die een oplossing aan dit probleem kunnen bieden, maar niet efficiënt genoeg zijn, zijn de *brute force*-aanpak en het *baby step, giant step*-algoritme. De classificatie van deze algoritmen zijn respectievelijk $\mathcal{O}(p)$ en $\mathcal{O}(\sqrt{p})$, waaruit blijkt dat voor afdoende grote p de tijd benodigd om een oplossing te vinden aanzienlijk is. Ter illustratie: Curve25519, een veelgebruikte kromme, gebruikt het priemgetal $p = 2^{255} - 19$. Zoals de naam doet vermoeden is een brute force aanval weinig elegant, in de zodanigheid dat voor iedere $x \in [1, p]$ gecontroleerd wordt of x voldoet aan $k^x = l$. Is dit het geval, dan kan voor alle gebruiken geconcludeerd worden dat $x = \nu$ en wordt de bewerking afgebroken. De classificatie verraade reeds dat in het ergste geval alle $2^{255} - 19$ mogelijke waarden voor x gecontroleerd worden. Deze onderneming kan met de hedendaags beschikbare computatiekracht jaren in beslag nemen.

6 Implementatie in Python

7 Aanvallen op de encryptie

8 Prestaties

Bronnen

Tate, Silverman (1994). Rational Points on Elliptic Curves (gecorrigeerd). New York City, New York: Springer-Verlag.

http://en.wikipedia.org/wiki/Cryptography

http://en.wikipedia.org/wiki/Elliptic_curve

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Discrete_logarithm