RSA codering

De RSA-code was het eerste algoritme dat codering mogelijk maakte via een publieke sleutel, zodat (vaak onveilig) contact tussen verzender en ontvanger overbodig werd. Het algoritme werd ontworpen in 1977 door Ron Rivest, Adi Shamir en Leonard Adleman op het Massachusetts Institute of Technology (MIT). De letters RSA staan voor de eerste letters van hun familienaam.

In deze nota bespreken we de wiskundige principes achter de RSA code.

Notatie. Voor elke drie gehele getallen r, s, t met $t \neq 0$ schrijven we

$$r = s \bmod t$$

indien t een (gehele) deler is van $r - s$. Met andere worden, $r = s \bmod t$ als en slechts als de rest bij deling van r door t gelijk is aan de rest bij deling van r door t.

Voorbeelden.

1) $40 = 7 \bmod 3$ want $40 - 7$ is deelbaar door 3.

2) $3 = -2 \bmod 5$ want $3 - (-2)$ is deelbaar door 5.

3) $-16 = 0 \bmod 4$

4) $77 \neq 1 \bmod 8$

Definitie. Voor elk natuurlijk getal $n > 1$ noteren we de verzameling van alle natuurlijke getallen kleiner dan n door $\mathbb{Z}_n$. In symbolen

$$\mathbb{Z}_n = \{a \in \mathbb{N} \mid 1 \leq a < n\}$$

Op deze verzameling definiëren we een optelling en een vermenigvuldiging die geërfd wordt door de optelling en vermenigvuldiging op de gehele getallen $\mathbb{Z}$

$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

$$(a, b) \mapsto a + b \stackrel{\text{def}}{=} (a + b) \bmod n \qquad \text{met } a + b \text{ in het rechterlid de gewone optelling in } \mathbb{Z}$$

$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$

$$(a, b) \mapsto a \cdot b \stackrel{\text{def}}{=} a \cdot b \bmod n \qquad \text{met } ab \text{ in het rechterlid de gewone vermenigvuldiging in } \mathbb{Z}$$

De verzameling $\mathbb{Z}_n$ voorzien van deze optelling en vermenigvuldiging heet een ring, notatie $\mathbb{Z}, +, \cdot$

Voorbeelden.

1) In $\mathbb{Z}_2 = \{0, 1\}$ is $1 + 1 = 2 \bmod 2 = 0$

2) In $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ is $2 \cdot 3 = 0$

3) In $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ is $2^7 = 2 \cdot 2^6 = 2 \bmod 5 \cdot 2^6 \bmod 5 = 2 \cdot 128 \bmod 5 = 2 \cdot 3 \bmod 5 = 1$

3) In $\mathbb{Z}_{50}$ is $49^{18} = 49^{18} \bmod 50 = (49 \bmod 50)^{18} = (-1 \bmod 50)^{18} = (-1)^{18} \bmod 50 = 1 \bmod 50 = 1$

Definitie. Voor $n \in \mathbb{N}$ noteren we met $\varphi(n)$ het aantal natuurlijke getallen kleiner dan n die relatief priem[1] zijn met n. Met andere woorden

$$\varphi(n) = \{a \in \mathbb{N} \mid 1 \leq a \leq n \text{ en } \text{ggd}(a, n) = 1\}$$

[1] Twee natuurlijke getallen a, b heten relatief priem indien hun grootste gemene deler gelijk is aan 1, notatie $\text{ggd}(a, b) = 1$.

Lemma 1. Er geldt

1. Voor een priemgetal p is $\varphi(p) = p - 1$.
2. Voor een priemgetal p en een $e \in \mathbb{N}_0$ is $\varphi(p^e) = (p-1)p^{e-1}$.
3. Voor twee natuurlijke getallen a, b is die relatief priem zijn is $\varphi(ab) = \varphi(a)\varphi(b)$.
4. Als n een natuurlijk getal is met priemontbinding

$$n = p_1^{e_1} p_2^{e_2} \dots p_l^{e_l} = \prod_{i=1}^{l} p_i^{e_i}$$

dan is

$$\varphi(n) = \prod_{i=1}^{l} (p_i - 1) p_i^{e_i - 1}$$

Bewijs. (1) en (2) zijn elementair, (3) vergt wat inspanning maar volgt gemakkelijk uit de Chinese Reststelling[2] en (4) volgt uit (2-3). □

Stelling (Fermat[3], 1640) Voor elk priemgetal p en geheel getal a geldt

$$a^p = a \bmod p$$

Omdat de stelling triviaal is in geval p een deler is van a, is de stelling equivalent met: Voor elk priemgetal p en geheel getal a relatief priem met p geldt

$$a^{p-1} = 1 \bmod p$$

Het bewijs van deze stelling van Fermat volgt uit de algemere

Stelling (Euler, 1736). Voor elk natuurlijk getal n en geheel getal a relatief priem met n geldt

$$a^{\varphi(n)} = 1 \bmod n$$

Bewijs. Een zeer eenvoudig bewijs met behulp van groepentheorie gaat als volgt. Op de verzameling

$$G = (\mathbb{Z}_n)^* = \{d \in \mathbb{N} \mid 1 \leq d \leq n \text{ en } (d, n) = 1\}$$

kan men een vermenigvuldiging definiëren

$$\cdot : G \times G \to G$$

$$(a, b) \mapsto a \cdot b \stackrel{\text{def}}{=} ab \bmod n$$

waarbij ab de gewone vermenigvuldiging is van a en b in $\mathbb{Z}$. De verzameling G voorzien van deze vermenigvuldiging heet een groep, notatie $G, \cdot$
Voor elke groep $H, \cdot$ geldt de eigenschap

$$\forall h \in H : h^{\#H} = e_H$$

met e_H het neutraal element voor de vermenigvuldiging in H. Voor onze groep G wordt dit

$$\forall a \in G : a^{\#G} = e_G$$

en omdat $\#G = \varphi(n)$ is

$$\forall a \in \mathbb{Z} : 1 \leq a \leq n \text{ en } (a, n) = 1 \Rightarrow a^{\varphi(n)} = 1 \bmod n$$

□

Bewijs van de Kleine Stelling van Fermat. Stel $n = p$. Uit het Lemma 1 volgt $\varphi(n) = p - 1$. De Stelling van Euler bewijst het gestelde. □

---

[2] De (eerste versie van de) Chinese Reststelling drukt uit dat elk stelsel vergelijkingen van de vorm $x = a \bmod n$, $x = b \bmod m$ met $\text{ggd}(n, m) = 1$ een oplossing x heeft (en geeft een algoritme om de oplossingen te vinden). In moderne taal formuleert men de Chinese Reststelling stelling als volgt: $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ als groepen (en eigenlijk ook als ringen).

[3] Ook wel de "Kleine Stelling van Fermat" genoemd. Fermat had de gewoonte om zijn bewijzen voor zijn stellingen niet kenbaar te maken maar veeleer andere wiskundigen via briefwisseling uit te dagen. Fermat stuurde zijn "kleine stelling" op naar de Bessy in 1640, met onderschrift "Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long." Leibniz, 1683 was de eerste die erin slaagde de Kleine Stelling van Fermat te bewijzen. Een ander - en wellicht het meest bekende - voorbeeld is de zogenaamde "Laatste Stelling van Fermat" die onbewezen bleef tot Wiles die in 1994 aantoonde.

1. Voorbereiding: sleutels maken

De ontvanger (vb. bank) zal als voorbereiding twee sleutels aanmaken: een publieke sleutel (die gepubliceerd wordt in een tijdschift of op internet) en een geheime sleutel (die de ontvanger voor zichzelf houdt). Het aanmaken van deze twee sleutels verloopt in drie stappen.

Stap 1. Kies twee (bij voorkeur grote) priemgetallen p en q en bereken $n = pq$.

Stap 2. Kies een natuurlijk getal e zodat

$$1 < e < n \quad \text{en} \quad \text{ggd}(e, \varphi(n)) = 1$$

gebruik makend van Lemma 1 (1),(3) kunnen we dit vertalen in

$$1 < e < n \quad \text{en} \quad \text{ggd}(e, (p-1)(q-1)) = 1$$

De publieke[4] sleutel is het paar (e, n).

Stap 3. Bereken het[5] natuurlijk getal d waarvoor

$$1 < d < \varphi(n) \quad \text{en} \quad de = 1 \bmod \varphi(n)$$

Merk op dat

$$de = 1 \bmod \varphi(n) \Rightarrow de - 1 = k\varphi(n) \text{ voor een } k \in \mathbb{Z} \qquad (*)$$

De geheime[6] sleutel is het paar (d, n).

2. Een bericht coderen

De verzender[7] (vb. klant bij bank) ontbindt eerst het bericht in leestekens, en elk leesteken wordt omgezet in een getal (bijvoorbeeld, $A = 1$, $B = 2$, etc). Dus om een bericht veilig te versturen volstaat het om getallen veilig te versturen.

Noem M het getal[8] dat je wil versturen. De publieke sleutel is (e, n) dus je kan het getal

$$C = M^e \bmod n$$

berekenen. Dit getal C is de code die je verstuurt.

3. Een bericht decoderen

De ontvanger (vb. bank) ontvangt de code C. Om de code te decoderen gebruikt de ontvanger de geheime sleutel (d, n) en berekent het getal

$$C^d \bmod n$$

Een kleine rekenoefening leert

$$\begin{aligned}
C^d \bmod n &= (M^e \bmod n)^d \\
&= M^{de} \bmod n \qquad \text{(definitie vermenigvuldiging in } \mathbb{Z}_n) \\
&= M^{1+k\varphi(n)} \bmod n \\
&= \left(M M^{k\varphi(n)}\right) \bmod n \\
&= M \bmod n \cdot \left(M^{\varphi(n)} \bmod n\right)^k \qquad \text{(definitie vermenigvuldiging in } \mathbb{Z}_n) \\
&= M \bmod n \qquad \text{(Stelling van Euler)} \\
&= M \qquad (\text{want } M < n)
\end{aligned}$$

Om de Stelling van Euler toe te passen gingen we er in de voorlaatste stap wel van uit dat M en n onderling ondeelbaar zijn. Maar zelfs als dit niet zo is kun je aantonen dat deze overhang klopt.

---

[4] De letter e staat voor het woord "encryptie" (code schrijven).

[5] Dat d bestaat en uniek is, volgt uit het feit dat $(\mathbb{Z}_n)^*, \cdot$ een groep is en dus elk element een uniek invers heeft voor de bewerking. Op zijn beurt volgt dit uit de Stelling van Bezout-Bachet: Voor elke twee gehele getallen a, b is $\text{ggd}(a, b) = c$ als en slechts als er gehele getallen k, l bestaan waarvoor $ak + bl = c$.

[6] De letter d staat voor het woord "decoderen" (code omzetten).

[7] of diens computer

[8] Belangrijk is wel dat M kleiner is dan n.

Voorbeeld.

1. Kies twee priemgetallen en bereken $n = pq$. We kiezen $p = 61$ en $q = 53$. Dus $n = 3233$. Dus $\varphi(n) = (p-1)(q-1) = 3120$.
2. Kies e zodat $1 \leq e \leq n$ en $\text{ggd}(e, \varphi(n)) = 1$. Dus moet $1 \leq e \leq 3233$ en $\text{ggd}(e, 3120) = 1$. We kiezen $e = 17$. De publieke sleutel is $(e, n) = (17, 3233)$.
3. Bereken d waarvoor $1 \leq d \leq n$ en $de = 1 \bmod \varphi(n)$. Dus moet $1 \leq d \leq 3233$ en $17d = 1 \bmod 3120$. De computer[9] berekent $d = 2753$. De geheime sleutel is $(d, n) = (2753, 3233)$.
4. De verzender wil bijvoorbeeld $M = 123$ verzenden. We coderen als volgt
$$C = M^e \bmod n = 123^{17} \bmod 3233 = 855$$
5. De ontvanger ontvangt $C = 855$ en wil dit decoderen. De ontvanger decodeert als volgt
$$C^d \bmod n = 855^{2753} \bmod 3233 = 123 = M$$
en hij vindt de oorspronkelijke boodschap M terug.

Tot slot: waarom is RSA zo goed?

Omdat het enorm moeilijk te kraken is. Om de code te kraken zonder in het bezit te zijn van de geheime sleutel moet je d zien te vinden, het natuurlijk getal waarvoor

$$1 < d < \varphi(n) \quad \text{en} \quad de = 1 \bmod \varphi(n)$$

Je kent e (die is publiek), dus moet je enkel nog $\varphi(n) = (p-1)(q-1)$ zien te achterhalen. Daarvoor dien je n (die is ook publiek) te ontbinden in priemfactoren p en q. En dat is nu net ontzettend moeilijk als p en q grote getallen zijn...

K. De Naeghel, 21 mei 2007.

[9] Alternatief: je kan aantonen dat je $d = e^{\varphi(\varphi(n))-1} \bmod \varphi(n)$, op die manier kun je d berekenen