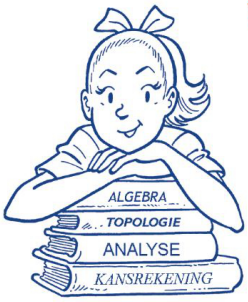
WISKUNNEND WISKE

DE VERBIJSTERENDE VERCIJFERING

FINALE 2020 - RODE DRAAD B



Herhaal dat we a mod n noteren voor de rest van a bij deling door n. We noemden a **inverteerbaar** modulo n als er een geheel getal b bestaat zodat $a \cdot b \bmod n = 1$. Dit geheel getal b bestaat als en slechts als $\text{ggd}(a, n) = 1$.

We hebben nu genoeg achtergrond om uit te leggen hoe RSA werkt. De eerste stap is het genereren van een **publieke sleutel** die iedereen kan gebruiken om boodschappen te **vercijferen** en een **geheime sleutel** die de bezitters ervan toelaat om vercijferde berichten terug te **ontcijferen**.

Hiervoor gebeurt het volgende: We bedenken twee oneven priemgetallen p en q en hun product pq noemen we n. Dan kiezen we een getal e tussen 1 en $(p-1)(q-1)$ dat **inverteerbaar** is modulo $(p-1)(q-1)$. De inverse van e modulo $(p-1)(q-1)$ noemen we d. Iedereen mag weten wat n en e zijn, maar slechts één persoon mag weten wat p, q en d zijn.

Je zou kunnen denken dat het kinderspel is om p of q uit n te halen. In de praktijk zijn p en q getallen van tientallen cijfers lang en er zijn nog **geen** klassieke computeralgoritmen gekend die **snel** willekeurig grote getallen kunnen ontbinden in priemfactoren!

We veronderstellen nu dat we een bericht m kunnen voorstellen als een getal tussen 0 en $n-1$. Om m te **vercijferen** berekenen we $c = m^e$ mod n. **Ontcijferen** gebeurt door c^d mod n te berekenen. En geloof het of niet, $c^d = (m^e)^d = m$ mod n.

Een snelle manier om berichten te vercijferen is door gebruik te maken van het **herhaald kwadrateren**. Stel dat ik bijvoorbeeld $m = 2$ wil vercijferen met $n = 21$ en $e = 11$. Ik schrijf 11 in haar binaire vorm, in dit geval 1011 (want $11 = 1 + 2 + 0 \cdot 4 + 8$). Ik tel het aantal cijfers van de binaire vorm, noem dit aantal k en ik kwadrateer m dus $k - 1$ keer. In dit geval moet ik 2 dus 3 keer kwadrateren:

1. $2^2 = 4$ mod 21
2. $2^4 = 4^2 = 16$ mod 21
3. $2^8 = 16^2 = 256 = 4$ mod 21

Aangezien $11 = 1 + 2 + 8$ volgt ook dat

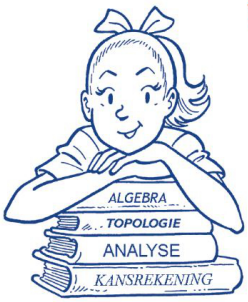
$$2^{11} = 2^{1+2+8} = 2^1 2^2 2^8 = 2 \cdot 4 \cdot 4 = 32 = 11 \text{ mod } 21$$

Dus de **vercijfering** van $m = 2$ met $n = 21$ en $e = 11$ is $c = 11$.

WISKUNNEND WISKE

DE VERBIJSTERENDE VERCIJFERING

FINALE 2020 - RODE DRAAD B



Opdracht (40 minuten)

Zij $n = 33$, $e = 9$. We stellen de letters van A tot Z (in alfabetische volgorde) voor door de getallen van 0 tot en met 25 (van klein naar groot). Verder hebben we:

Teken	.	?	!	-	(	)	:
Getal	26	27	28	29	30	31	32

Een spatie vercijferen we ook gewoon met een spatie.

Vercijfer de boodschap SUSKE EN WISKE letter per letter met RSA.

VUB