1

$N = 109$ 052|083|051|006|101|073|054|082|022

$e = 47$ $b = 1$

$E(m) = m^e \pmod N$ $d = 23$

$D(c) = c^d \pmod N$

$m^{\varphi(N)} = 1 \pmod N$

$D(E(m)) = m^{ed} \pmod N$

$ed \equiv 1 \pmod{\varphi(N)} \Rightarrow m^{ed} = m^{1+k\varphi(N)} \pmod N$

$d = e^{-1} \pmod{\varphi(N)}$ $= m \cdot m^{k\varphi(N)} \pmod N$

$d = 47^{-1} \pmod{108}$ $= m \pmod N$

$d \cdot 47 + k \cdot 108 = 1$

$d \cdot 47 + k \cdot 108 = \gcd(108, 47)$ $(=1)$

$108 = 2 \cdot 47 + 14$

$47 = 3 \cdot 14 + 5$

$14 = 2 \cdot 5 + 4$

$5 = 4 + 1$

	108	47	
108	1	0	
47	0	1	$\times 1$
14	1	-2	$\times 3$ $-$
5	-3	7	$=$
4	7	-16	
1	-10	23	

$1 = -10 \cdot 108 + 23 \cdot 47$

d

2

Euler-Fermat

$\forall m \in \mathbb{Z}_N^*, \quad m^{\varphi(N)} \equiv 1 \pmod{N}$

Maar b.v. $N = p \cdot q \Rightarrow m^{ed} \equiv m \pmod{N}$

$\forall m < N$ (dus ook $m \notin \mathbb{Z}_N^*$)

Waarom?

$\mathbb{Z}_N = \{a \in \mathbb{N} \mid a < N\}$

$\mathbb{Z}_p$ en $\mathbb{Z}_q$ $\quad \mathbb{Z}_p \times \mathbb{Z}_q = \{(a,b) \mid a \in \mathbb{Z}_p, b \in \mathbb{Z}_q\}$

$3 \cdot_{\mathbb{Z}_{11}} 5 = 4$ $\quad (3,5) \cdot_{\mathbb{Z}_p \times \mathbb{Z}_q} (7,11)$

$= ([3 \cdot 7 \bmod p], [5 \cdot 11 \bmod q])$

$|\mathbb{Z}_p| = p$

$|\mathbb{Z}_q| = q$

$|\mathbb{Z}_p \times \mathbb{Z}_q| = pq$

$|\mathbb{Z}_N| = N = pq$

} zelfde grootte

werpt (misschien) de vraag op:
kunnen we tussen elementen mappen?

Ja. Het blijkt dat de groepen zgn. isomorf zijn ($Z_N \simeq Z_p \times Z_q$).

DEFINITION 8.23 *Let $\mathbb{G}, \mathbb{H}$ be groups with respect to the operations $\circ_{\mathbb{G}}, \circ_{\mathbb{H}}$, respectively. A function $f : \mathbb{G} \to \mathbb{H}$ is an* isomorphism from $\mathbb{G}$ to $\mathbb{H}$ *if:*

1. *f is a bijection, and*
2. *For all $g_1, g_2 \in \mathbb{G}$ we have $f(g_1 \circ_{\mathbb{G}} g_2) = f(g_1) \circ_{\mathbb{H}} f(g_2)$.*

If there exists an isomorphism from $\mathbb{G}$ to $\mathbb{H}$ then we say that these groups are isomorphic *and write $\mathbb{G} \simeq \mathbb{H}$.*

Neem de functie $f: Z_N \to Z_p \times Z_q$, gedef. als

$$f(m) = ([m \bmod p], [m \bmod q]).$$

Deze functie voldoet aan bovenstaande eisen en is een isomorfisme van Z_N naar $Z_p \times Z_q$.

We bewijzen de bijectiviteit (de andere eigenschap mag je zelf bewijzen ;))

Stel, $\exists x, x'$ waarvoor $f(x) = (x_p, x_q) = f(x')$.
Dan geldt $x' \equiv x_p \equiv x \pmod p$
$x' \equiv x_q \equiv x \pmod q$
Dan geldt $p \mid (x'-x)$ en $q \mid (x'-x)$. Maar dan $N \mid (x'-x)$,
en dus $x' \equiv x \pmod N$, dus is f injectief.

$|Z_N| = |Z_p \times Z_q|$ + injectiviteit $\Rightarrow$ bijectiviteit.

Nu kunnen we bewijzen dat

$\forall m < N,\ m^{ed} \equiv m \pmod N$.

Bewijs:

We onderscheiden 2 gevallen.

Geval 1: $\gcd(m, N) = 1$.

$$m^{ed} = m^{1 \pmod{\varphi(N)}} \pmod N \quad \text{↓ Euler-Fermat}$$
$$= m \pmod N$$

Geval 2: $\gcd(m, N) > 1$.

Dan geldt $p \mid m$ of $q \mid m$. WLOG kiezen we $m = kp$.

Er geldt $m \equiv 0 \pmod p$, en dus

$$m^{ed} \equiv 0^{ed} \equiv 0 \equiv m \pmod p$$

en

$$m^{ed} = m^{1+k\varphi(N)} = m^{1+k\varphi(p)\varphi(q)} \equiv m \pmod q$$

$$([m \bmod p], [m \bmod q]) = f(m)$$

$$\overset{\text{(injectiviteit)}}{=}$$

$$\| \qquad \| \qquad \| \qquad \| \qquad \|$$

$$([m^{ed} \bmod p], [m^{ed} \bmod q]) = f(m^{ed})$$