Diffie-Hellman: Ziel: Alice und Bob wollen sich auf ein geheimes Schlüssel einigen

public   private

Wir suchen uns zuerst eine Primzahl p aus und wählen $\langle g \rangle = \mathbb{Z}_p^*$

Alice: wählt $x_A \in \{0, 1, \dots, p-2\}$

Bob: wählt $x_B \in \{0, 1, \dots, p-2\}$

$\underbrace{y_A = R_p(g^{x_A})}$

Kernidee: mit nur y_A, p und g ist es schwierig x_A zu finden.

$y_B = R_p(g^{x_A})$

$$k_{AB} = R_p(y_B^{x_A}) = R_p(g^{x_B \cdot x_A}) = R_p(g^{x_A \cdot x_B}) = R_p(y_A^{x_B}) = k_{BA}$$

RSA recap   public   private

1. generiere Primzahlen p, q, $n := p \cdot q$
2. wähle e so dass $1 < e < \varphi(n)$ und $\gcd(e, \varphi(n)) = 1$
3. berechne $d := e^{-1}$ (in $\mathbb{Z}^*_{\varphi(n)}$) also d, so dass

$$de \equiv_{\varphi(n)} 1 \iff de = k \cdot \varphi(n) + 1 \text{ für } k \in \mathbb{Z}$$

Garantiert lösbar da $\gcd(e, \varphi(n)) = 1$.

Sender | **Empfänger**

Nachricht $m \in \{1, \dots, n-1\}$

$$\underbrace{c = R_n(m^e)}_{} \xrightarrow{\text{sende } c} \qquad m \overset{(*)}{=} R_n(c^d)$$

Kernidee: diese Gleichung ist schwierig nach m aufzulösen, ohne $\varphi(n) = (p-1)(q-1)$ zu kennen

Beweis von $(*)$:

$$c^d \equiv_n m^{ed} \equiv_n m^{k \cdot \varphi(n) + 1} \equiv_n \Big(m^{\overset{|\mathbb{Z}^*_n|}{\overset{\shortparallel}{\varphi(n)}}}\Big)^k \cdot m \equiv_n 1^k \cdot m \equiv_n m$$

∇ in $\mathbb{Z}^*_n$

$(\Rightarrow R_n(c^d) = m)$

Beweis im Fall $\gcd(n, m) \neq 1$:

$\gcd(n, m) \neq 1 \iff m$ hat p oder q als Faktor $\iff \gcd(n, m) \in \{p, q\}$ $(m \neq p \cdot q)$

aber $m \in \{1, \dots, n-1\} \neq \mathbb{Z}^*_n$ da n nicht prim z.B. $p \in$ ↯, $\gcd(n, p) = p \neq 1$

Zu zeigen: $c^d \equiv_n m^{ed} \equiv_n m$

Idee: $n = p \cdot q$ (teilerfremd) $\to$ $c^d \equiv_p m$, $c^d \equiv_q m$ $\Rightarrow c^d \equiv_{\underbrace{p \cdot q}_{n}} m$

Es gilt: $c^d = m^{ed} \equiv_p m^{k \cdot \varphi(n) + 1} \equiv_p \underbrace{m^{k \overset{\varphi(p)}{\overset{\shortparallel}{(p-1)}}(q-1)}}_{\to 1} \cdot m$

$\equiv_p 1 \cdot m = m$

analog $m^{ed} \equiv_q m$

(siehe Aufgabe 7.7)

$$\Rightarrow c^d \equiv_{\underbrace{p \cdot q}_{n}} m$$

oder

Beweis:

betrachte das Gleichungssystem

$$x \equiv_p m$$
$$x \equiv_q m$$

Da $x = m$, $x = m^{de}$ und alle Lösungen kongruent sind mod n (siehe Beweis von CRT) gilt $m \equiv_n m^{de}$.

Aufgabe 1

Let $c = 7$ be a message encrypted with the public key pair (n, e). Find both the secret key d and the original message m.

To find d we need to solve

$$de = 27d \equiv_{\varphi(n)} 1.$$

We have $\varphi(55) = \varphi(5 \cdot 11) = 4 \cdot 10 = 40$. So we get

$$27d \equiv_{40} 1.$$

We want to find some $k \in \mathbb{Z}$ such that $27d = 40k + 1$. So we can start with 1 and keep adding 40 until we reach something divisible by 27:

$$1 \to 41 \to 81 = 3 \cdot 27 \implies d = 3$$

Now for m we just calculate

$$R_{55}(c^d) = R_{55}(7^3) = R_{55}(49 \cdot 7) = R_{55}(-6 \cdot 7) = R_{55}(-42) = 13 = m.$$

Generators bestimmen:

z.B. $\mathbb{Z}_7^*$ 1. Teiler von $|\mathbb{Z}_7^*| = 6$: (1,) 2, 3, 6

2.

Potenz \ $\mathbb{Z}_7^*$	2	3	4	5	6
2	4	2	2	4	1
3	1	6	1	6	
6		1		1	

$\to \mathrm{ord}(6) = 1$

$\to$ generators: 3 und 5

\# Nullteiler vom Ring $\mathbb{Z}_n$ berechnen

$a \in \mathbb{Z}_n \setminus \{0\}$ ist ein Nullteiler $\overset{\text{def.}}{\Longleftrightarrow} \exists b \in \mathbb{Z}_n \setminus \{0\} \quad a \cdot b \equiv_n 0$

$\Longleftrightarrow R_n(a \cdot b) = 0$

$\Longleftrightarrow n \mid a \cdot b$

Fall $\gcd(a, n) = 1$: $\to$ keine Primfaktoren zusammen

$\Rightarrow \mathrm{lcm}(a, n) = a \cdot n$

wir wissen alle Primfaktoren von beiden Zahlen in x reinpacken, damit $n \mid x$ und $a \mid x \Rightarrow x = \mathrm{lcm}(a, n) = a \cdot n$

Da $n \notin \mathbb{Z}_n$ gilt dann $a \cdot b \not\equiv_n 0$ für alle $b \in \mathbb{Z}_n \setminus \{0\}$

Fall $\gcd(a, n) = d > 1$:

$\Rightarrow \mathrm{lcm}(a, n) = \frac{a \cdot n}{d}$. Da $d \mid n$ und $d > 1$ ist $\frac{n}{d} \in \mathbb{Z}_n$ und $a \cdot \frac{n}{d} \equiv_n 0$

$\Rightarrow$ a ist ein Nullteiler.

Daher: "Nullteiler von $\mathbb{Z}_n$" $= \{a \in \mathbb{Z}_n \setminus \{0\} \mid \gcd(a, n) \neq 1\}$

$\Rightarrow \#\,\text{Nullteiler} = |\mathbb{Z}_n| - 1 \quad - \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\} = n - \varphi(n) - 1$