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.

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

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

RSA recap   public   private

1. generiere Primzahlen p, q, $n := p \cdot q$
2. wähle e so dass $1 < e < \varphi(n)$ und $ggT(e, \varphi(n)) = 1$
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 $ggT(e, \varphi(n)) = 1$.

Sender   Empfänger

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

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

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

Beweis von $(*)$:

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

in $\mathbb{Z}_n^*$ $(\Rightarrow R_n(c^d) = m)$

Beweis im Fall $ggT(n, m) \neq 1$: aber $m \in \{1, \dots, n-1\} \neq \mathbb{Z}_n^*$ da n nicht prim

$ggT(n, m) \neq 1 \iff m$ hat p oder q als Faktor $\iff ggT(n, m) \in \{p, q\}$ $(m \neq p \cdot q)$ z.B. $p \in \cancel{\mathbb{Z}_n^*}$, $ggT(n, p) = p \neq 1$

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

Idee: $n = \underbrace{p \cdot q}_{\text{teilerfremd}}$ $\to$ $\begin{array}{l} c^d \equiv_p m \\ c^d \equiv_q m \end{array}$ $\Rightarrow$ $c^d \equiv_{\underbrace{p \cdot q}_{n}} m$

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 → ord(6) = 1
3	1	6	1	6	
6		1		1	→ generators: 3 und 5

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

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

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

$\iff n \mid a \cdot b$

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

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

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

$\Rightarrow \operatorname{lcm}(a, n) = \frac{a \cdot n}{d}$. 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 $\mathbb{Z}_n$" $= \{a \in \mathbb{Z}_n \setminus \{0\} \mid \gcd(a, n) \neq 1\}$

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

Modulo Tricks:

Kongruenz zu 1:

$R_{18}(37^{42}) =$ $R_{18}(R_{18}(37)^{42}) = R_{18}(1^{42}) = 1$

$-2\cdot 18$

Der "-" Trick:

modulare Arithmetik sagt uns, dass wir beliebig +3 oder −3 rechnen können.

$R_3(5^{2022}) =$ $R_3(5^{2022}) = R_3((-1)^{2022}) = 1$

da $5^{2022} \equiv_3 (-1)^{2022}$

Fermat's Little Theorem:

Daraus folgt ganz einfach:

Lemma

Für alle $a \in \mathbb{Z}_n^*$:

$$a^{\varphi(n)} \equiv_n 1$$

und für eine Primzahl p, für alle $1 \le a < p$:

$$a^{p-1} \equiv_p 1$$

oder auch $a > p$ mit $p \nmid a$: $R_p(a^x) = R_p(\underbrace{R_p(a)}_{\in \mathbb{Z}_p}{}^x)$

Lemma anwendbar

$R_7(1984^6) =$ 1

Hint: 7 teilt 1984 nicht.

habe ich in der ÜS vergessen

$R_{11}(2^{1408}) =$ $R_{11}(2^{10\cdot 140+8}) = R_{11}((2^{10})^{140}\cdot 2^8) = R_{11}(2^8)$
$= R_{11}(2^{4\cdot 2})$
$= R_{11}(16^2)$
$= R_{11}(5^2)$
$= 3$

1 da $\varphi(11) = 10$

$\boxed{\text{Allgemein gilt } R_n(a^x) = R_n\left(a^{R_{\varphi(n)}(x)}\right)}$

$R_{11}(2^{3^{40}}) =$ $R_{11}\left(2^{R_{10}(3^{40})}\right) = R_{11}(2^1) = 2$

$R_{10}(3^{40}) = R_{10}(9^{20}) = R_{10}((-1)^{20})$
$= 1$

Vom Kahoot:

$R_{16}(49^{42}) = ?$
$= R_{16}(1^{42}) = 1$

$R_5(4^{967} + 6^{1410}) = R_5((-1)^{967} + 1^{1410}) = R_5(-1+1) = 0$

(967) ungerade

$R_{12345}\left(12344^{1234512345^{123451234512345}}\right) = ?$
$= R_{12345}((-1)^{\dots 5 \dots})$ ungerade
$= R_{12345}(-1)$
$= 12344$ $(12345-1)$

Berechne die letzte Ziffer von $123456789^{11^{13}}$

Rest Modulo 10 gibt die letzte Ziffer.

$\to R_{10}(\dots) = R_{10}(9^{11^{13}})$ $(123456789 = 12345678 \cdot 10 + 9)$
$= R_{10}((-1)^{11^{13}})$ ungerade
$= R_{10}(-1)$
$= 9$

Hint: 7919 ist prim

$R_{7919}(3999^{7918}) = ?$
$= 1$ da 7919 prim und $\varphi(p) = p-1$ für p prim

$R_{11}(3^{62}) = ?$
$= R_{11}\left(3^{R_{10}(62)}\right) = R_{11}(3^2) = 9$