Kryptografie und -analyse, Übung 10

Henry Haustein

RSA

(a) $k_s = k_t^{-1} \mod \Phi(n) \Rightarrow k_s = 3^{-1} \mod \Phi(3 \cdot 17) \equiv 3^{-1} \mod 32 \Rightarrow k_s = 11$
$s = 7^{11} \mod 51 = 31$
$3 \overset{?}{=} 12^3 \mod 51 \Rightarrow 45 = 12^3 \mod 51 \Rightarrow$ Signatur nicht gültig

$$m = \left(m^{k_s}\right)^{k_t} \mod n$$
$$m = m^{k_s \cdot k_t} \mod n$$

Wir wissen $k_s \cdot k_t \equiv 1 \mod \Phi(n)$, also $k_s \cdot k_t = l(p-1)(q-1)+1$. Damit

$$\begin{aligned} m^{k_s \cdot k_t} &= m^{l(p-1)(q-1)+1} \mod n \\ &= \left(m^{p-1}\right)^{l(q-1)} \cdot m \mod n \end{aligned}$$

Da p eine Primzahl ist, gilt nach dem kleinen Satz von Fermat ($a^{p-1} \equiv 1 \mod p$) und weil $p \mid n$:

$$1^{l(q-1)} \cdot m = m \mod p$$

(b) $k_{dp} = k_e^{-1} \mod (p-1) = 3^{-1} \mod 2 \equiv 1$
$k_{dq} = k_e^{-1} \mod (q-1) = 3^{-1} \mod 10 \equiv 7$
u, v mit $up + vq = 1 \Rightarrow EEA(3, 11) \Rightarrow u = 4, v = -1$
$\Rightarrow y_p = c^{k_{dp}} \mod p = 19^1 \mod 3 \equiv 1$
$\Rightarrow y_q = c^{k_{dq}} \mod q = 19^7 \mod 11 \equiv 2$
$CRA(y_p, y_q) = upy_q + vqy_p = 3 \cdot 4 \cdot 2 + (-1) \cdot 11 \cdot 1 = 13 = m$
Probe: $13^3 \mod 33 \equiv 19$

(c) Angreifer beobachtet c, will m ermitteln, bekommt n, k_e, wählt $r \in \mathbb{Z}_n^*$, berechnet $r^{-1} \mod n$, berechnet $c' = c \cdot r^{k_e} \mod n$ und lässt sich das vom Empfänger entschlüsseln $\Rightarrow m' = (c')^{k_d} \mod n$. Angreifer berechnet

$$\begin{aligned} m' \cdot r^{-1} \mod n &= (c')^{k_d} \cdot r^{-1} \mod n \\ &= (m^{k_e} \cdot r^{k_e})^{k_d} \cdot r^{-1} \mod n \\ &= m \cdot r \cdot r^{-1} \mod n \\ &= m \end{aligned}$$

(d) $r^{-1} \mod 33 \equiv 5$
$c' = 5 \cdot 20^3 \mod 33 \equiv 4$
$m' = 4^7 \mod 33 \equiv 16$
$m = 16 \cdot 5 = 14$

(e) Wer faktorisieren kann, zerlegt $n = p \cdot q$ und berechnet dann $k_d = k_e^{-1} \mod \Phi(n)$.

Kryptosysteme auf Basis elliptischer Kurven

(a) Diskriminante $\neq 0$

$$\begin{aligned} D &= 4a^3 + 27b^2 \mod p \\ &= 4 \cdot 4^3 + 27 \cdot 7^2 \mod 11 \\ &= 6 \mod 11 \end{aligned}$$

Für $x = 0$:

$$z = 0^3 + 4 \cdot 0 + 7 \mod 11 \equiv 7$$

Ist $7 \in QR_{11}$? $\Rightarrow z^{\frac{p-1}{2}} \mod p \stackrel{?}{\equiv} 1$. $7^5 \mod 11 \equiv -1 \Rightarrow$ es gibt keinen Punkt mit $x = 0$ auf dieser Kurve.
Für $x = 5$:

$$z = 5^3 + 4 \cdot 5 + 7 \mod 11 \equiv 9$$

Ist $9 \in QR_{11}$? $\Rightarrow z^{\frac{p-1}{2}} \mod p \stackrel{?}{\equiv} 1$. $9^5 \mod 11 \equiv 1 \Rightarrow$ es gibt einen Punkt mit $x = 0$ auf dieser Kurve $P(5, 3)$ (und auch $Q(5, 8)$).
Punkt-Kompression: $(5, 3) \rightarrow (5, 3 \mod 2) = (5, 1)$ und $(5, 8) \rightarrow (5, 8 \mod 2) = (5, 0)$
Punkt-Dekompression:

$$\begin{aligned} z &= 6^3 + 4 \cdot 6 + 7 \mod 11 \equiv 5 \\ y &= \sqrt{5} \mod 11 \equiv 4 \end{aligned}$$

Da $4 \not\equiv 1 \mod 2$, ist $(6, 1) \rightarrow (6, -4) = (6, 7)$.

(b) $827 = 1100111011_2 \Rightarrow$ 10 Punktverdopplungen, 7 Punktadditionen
nichtadjazenter Form: $[1, 0, -1, 0, 1, 0, 0, 0, -1, 0, -1]_2 \Rightarrow$ 11 Punktverdopplungen, 5 Punktadditionen/-subtraktionen (online Tool zur Umwandlung Dezimal $\rightarrow$ NAF: https://codegolf.stackexchange.com/questions/235319/convert-to-a-non-adjacent-form)

(c) $Q_A = 2 \cdot (1, 1) \mod 11$

$$\begin{aligned} s &= \frac{3x^2 + a}{2y} = \frac{3 \cdot 1^2 + 4}{2 \cdot 1} = \frac{7}{2} \\ x_Q &= s^2 - 2x = \frac{49}{4} - 2 = \frac{41}{4} \\ y_Q &= -y + s(x - x_Q) = -1 + \frac{7}{2}\left(1 - \frac{41}{4}\right) = -\frac{267}{8} \end{aligned}$$

$Q_B = 3 \cdot (1, 1) \mod 11 = (1, 1) + \left(\frac{41}{4}, -\frac{267}{8}\right) \mod 11$

$$\begin{aligned} s &= \frac{\Delta y}{\Delta x} = \frac{-\frac{267}{8} - 1}{\frac{41}{4} - 1} = -\frac{275}{74} \\ x_Q &= \left(-\frac{275}{74}\right)^2 - \frac{41}{4} - 1 = \frac{3505}{1369} \\ y_Q &= -1 - \frac{275}{74}\left(1 - \frac{3505}{1369}\right) = \frac{243047}{50653} \end{aligned}$$

gemeinsamer Schlüssel $k_{AB} = 2 \cdot \left(\frac{3505}{1369}, \frac{243047}{50653}\right)$

$$s = \frac{3x^2 + a}{2y} = \frac{3 \cdot \left(\frac{3505}{1369}\right)^2 + 4}{2 \cdot \frac{243047}{50653}} = \frac{44351719}{17985478}$$

$$x_k = s^2 - 2x = \left(\frac{44351719}{17985478}\right)^2 - 2 \cdot \frac{3505}{1369} = \frac{310700466634601}{323477418888484}$$

$$y_k = -y + s(x - x_k) = -\frac{243047}{50653} + \frac{44351719}{17985478}\left(\frac{3505}{1369} - \frac{310700466634601}{323477418888484}\right) = -\frac{4964433566291413215147}{5817896000915613435352}$$