Kryptografie und -analyse, Übung 9

Henry Haustein

Grundlagen

(a) $\mathbb{Z}_{77}^* = \{a \in \mathbb{Z}_{77} \mid \mathrm{ggT}(a, 77) = 1\}$. Offensichtlich $\mathrm{ggT}(20, 77) = 1$ und $\mathrm{ggT}(14, 77) = 7$ und $20^{-1} = 27$ mit WolframAlpha (`20^-1 mod 77`)

(b) Satz von Lagrange: Wenn H Untergruppe von G, dann $\mathrm{ord}(H) \mid \mathrm{ord}(G)$, damit haben die Untergruppen von $\mathbb{Z}_{13}^*$ die Ordnungen 1, 2, 3, 4, 6 und 12 (die Ordnung von $\mathbb{Z}_{13}^*$ ist $\Phi(13) = 12$).

(c) Primfaktorzerlegung von Gruppenordnung: $12 = 2^2 \cdot 3$. Für $a_1 = 5$:

- $b = a_1^{\frac{n}{p_1}} = 5^{\frac{12}{2}} = 5^6 \equiv 12 \mod 13$
- $b = a_1^{\frac{n}{p_2}} = 5^{\frac{12}{3}} = 5^4 \equiv 1 \mod 13$

Für $a_2 = 6$:

- $b = a_2^{\frac{n}{p_1}} = 6^{\frac{12}{2}} = 6^6 \equiv 12 \mod 13$
- $b = a_2^{\frac{n}{p_2}} = 6^{\frac{12}{3}} = 6^4 \equiv 9 \mod 13$

$\Rightarrow a_1 = 5$ ist kein Generator, $a_2 = 6$ ist ein Generator.

(d) Binärdarstellung des Exponenten: $22 = 10110_2$. $z_0 = 1$, $z_1 = 5$, $z_2 = 3$, $z_3 = 1$, $z_4 = 5$, $z_5 = 3$

Diskreter Logarithmus/ElGamal

(a) $x = \log_5(9) \mod 11$ und $x = qm + r$
$m = \lceil \sqrt{|G|} \rceil = \lceil \sqrt{\Phi(11)} \rceil = \lceil \sqrt{10} \rceil = 4$
Babystep-Liste: $B = \left\{\left(i, y(g^i)^{-1} \mod p\right), 0 \le i < m\right\}$ mit $y = 9 \equiv -2$, $g = 5$ und $p = 11$. $B = \{(0,9), (1,4), (2,3), (3,5)\}$
Giantstep-Liste: $G = \{(j, (g^m)^j \mod p), 0 \le j < m\} = \{(0,1), (1,9), (2,4), (3,3)\}$
erstes zusammengehörendes Element: (0,9) und (1,9) $\Rightarrow x = 1 \cdot 4 + 0 = 4$
Probe: $5^4 \equiv 9 \mod 11$

(b) $k_e = g^{k_d} = 5^3 \equiv 6 \mod 17$
$c_1 = g^r = 5^2 \equiv 8 \mod 17$
$c_2 = m \cdot k_e^r = 4 \cdot 6^2 \equiv 8 \mod 17$
$m = (c_1^{k_d})^{-1} \cdot c_2 = (6^3)^{-1} \cdot 16 \equiv 12^{-1} \cdot 16 \equiv 10 \cdot 16 \equiv 7 \mod 17$
$k_d = \log_g(k_e) \mod p$

(c) $m_2 = m_1 \cdot c_{1,2}^{-1} \cdot c_{2,2} = 4 \cdot 7^{-1} \cdot 2 = 4 \cdot 8 \cdot 2 \equiv 9 \mod 11$

(d) $k_t = g^{k_s} = 2^3 \equiv 8 \mod 11$
Berechnung r^{-1} mit $rr^{-1} \equiv 1 \mod (p-1) \Rightarrow r^{-1} = 3$ $s_1 = g^r = 2^7 \equiv 7 \mod 11$

$s_2 = r^{-1}(m - k_s s_1) = 3 \cdot (4 - 3 \cdot 7) = -51 \equiv 9 \mod 10$
$v_1 = k_t^{s_1} \cdot s_1^{s_2} = 8^7 \cdot 7^9 \equiv 2 \cdot 8 \equiv 5 \mod 11$
$v_2 = g^m = 2^4 \equiv 5 \mod 11 \Rightarrow v_1 = v_2$