Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 13 (31.1.2025)

Bemerkungen:

(1) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(2) Im Internet gibt es auch Möglichkeiten, schnell $a^d \bmod n$ auszurechnen. Mit nachfolgenden Befehlen erhält man jeweils $2^{693} \bmod 1387$:
   - https://sagecell.sagemath.org: `pow(2,693,1387)` oder `power_mod(2,693,1387)`
   - https://www.alpertron.com.ar/ECM.HTM: `Modpow(2,693,1387)`
   - WolframAlpha: `2^693 mod 1387`
(3) Es gibt keine Hausaufgaben mehr.

Präsenzaufgaben

Aufgabe P49: Um den diskreten Logarithmus von a zur Basis g modulo p zu mit der Pollard-ρ-Methode zu berechnen (mit einer Primitivwurzel g modulo p), wurde in der Vorlesung eine Folge (x_i, e_i, f_i) (mit $x_i \in \{1, \ldots, p-1\}$, $e_i, f_i \in \{0, \ldots, p-2\}$ und $x_i \equiv a^{e_i} g^{f_i} \bmod p$) rekursiv durch $(x_0, e_0, f_0) = (1, 0, 0)$ und

$$(x_{i+1}, e_{i+1}, f_{i+1}) = \begin{cases} (ax_i \bmod p, (e_i+1) \bmod (p-1), f_i), & \text{falls } x_i \equiv 1 \bmod 3, \\ (x_i^2 \bmod p, (2e_i) \bmod (p-1), (2f_i) \bmod (p-1)), & \text{falls } x_i \equiv 2 \bmod 3, \\ (gx_i \bmod p, e_i, (f_i+1) \bmod (p-1)), & \text{falls } x_i \equiv 0 \bmod 3 \end{cases}$$

definiert.
$g = 2$ ist eine Primitivwurzel modulo $p = 101$. Mit der Pollard-ρ-Methode soll der diskrete Logarithmus von $a = 3$ zur Basis $g = 2$ modulo $p = 101$ bestimmt werden. Hier sind die ersten Glieder der zugehörigen Folge $((x_i, e_i, f_i, x_{2i}, e_{2i}, f_{2i}))_{i \geq 0}$:

$(1,0,0,1,0,0), (3,1,0,6,1,1), (6,1,1,24,1,3), (12,1,2,96,1,5), (24,1,3,71,2,6), (48,1,4,81,8,24),$
$(96,1,5,82,9,25), (91,1,6,17,20,50), (71,2,6,73,40,1), (92,4,12,87,82,2), (81,8,24,17,83,3),$
$(61,8,25,73,66,7), (82,9,25,87,34,14), (44,10,25,17,35,15), (17,20,50,73,70,31),$
$(87,40,0,87,42,62), \ldots$

Bestimme damit den diskreten Logarithmus von 3 zur Basis 2 modulo 101.

Aufgabe P50: Sei $p = 181$.

(1) Zeige, dass 2 eine Primitivwurzel modulo p ist.
(2) Bestimme den diskreten Logarithmus von 3 zur Basis 2 modulo p mit der $(p-1)$-Methode.

Datei: ki_u13.tex. Version vom 29.1.2025

Aufgabe P51: (baby-step-giant-step-Methode) Für $p = 307$ ist $g = 5$ eine Primitivwurzel. Definiert man $m = \lceil \sqrt{p-1} \rceil$ und B durch $B(g^i \bmod p) = i$ für $0 \le i \le m-1$, so erhält man folgende Tabelle:

x	1	5	25	125	11	55	275	147	121	298	262	82	103	208	119	288	212	139
$B(x)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Berechne für $a = 3$

$$h_j = ag^{-mj} \bmod p$$

für $j = 0, 1, 2, \ldots$ soweit nötig, um damit und der oben stehenden Tabelle den diskreten Logarithmus von 3 zur Basis 5 modulo 307 zu bestimmen.

Aufgabe P52: (Index-Calculus-Methode) Für $p = 1009$ ist $g = 11$ eine Primitivwurzel modulo p. Insbesondere existieren die diskreten Logarithmen von 2 und 3 zur Basis $g = 11$ modulo $p = 1009$, d.h. es gibt Zahlen $\ell_2, \ell_3 \in \{0, 1, \ldots, p-2\}$ mit $2 \equiv g^{\ell_2} \bmod p$ und $3 \equiv g^{\ell_3} \bmod p$.
Für $b_1 = 32$, $b_2 = 42$, $b_3 = 62$ gibt es Zahlen a_{ij} mit

$$(g^{b_i} \bmod p) = 2^{a_{i1}} \cdot 3^{a_{i2}}$$

(1) Bestimme die Zahlen a_{ij}.
(2) Ersetzt man in den Gleichungen $2^{a_{i1}} \cdot 3^{a_{i2}} \equiv g^{b_i} \bmod p$ die Zahl 2 durch g^{ℓ_2} und 3 durch g^{ℓ_3}, so erhält man durch Vergleich der Exponenten ein Kongruenzgleichungssystem modulo $p-1$ für ℓ_2 und ℓ_3. Stelle das Kongruenzgleichungssystem auf.
(3) Löse das in (2) aufgestellte Kongruenzgleichungssystem und bestimme so die diskreten Logarithmen von 2 und 3 zur Basis 11 modulo 1009.