FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
10.01.2024

Musterlösung zum 11. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Man erhält in $\mathbb{Z}_{13}$:

x	1	2	3	4	5	6	7	8	9	10	11	12
1^x	1	1	1	1	1	1	1	1	1	1	1	1
2^x	2	4	8	3	6	12	11	9	5	10	7	1
3^x	3	9	1	3	9	1	3	9	1	3	9	1
4^x	4	3	12	9	10	1	4	3	12	9	10	1
5^x	5	12	8	1	5	12	8	1	5	12	8	1
6^x	6	10	8	9	2	12	7	3	5	4	11	1
7^x	7	10	5	9	11	12	6	3	8	4	2	1
8^x	8	12	5	1	8	12	5	1	8	12	5	1
9^x	9	3	1	9	3	1	9	3	1	9	3	1
10^x	10	9	12	3	4	1	10	9	12	3	4	1
11^x	11	4	5	3	7	12	2	9	8	10	6	1
12^x	12	1	12	1	12	1	12	1	12	1	12	1

Also sind 2, 6, 7 und 11 die einzigen Primitivwurzel modulo 13.

Übung 2

Aus der Tabelle zu Übung 1 sieht man, dass in $\mathbb{Z}_{13}^\times$ gilt:

a) $2^5 = 6 \quad \Rightarrow \quad \log_2 6 = 5.$

b) $6^7 = 7 \quad \Rightarrow \quad \log_6 7 = 7.$

c) $2^{11} = 7 \quad \Rightarrow \quad \log_2 7 = 11.$

Übung 3

Beobachtet man mit den Werten aus Übung 2 die Gleichung:

$$\log_2 6 \cdot \log_6 7 \;=\; 5 \cdot 7 \;=\; 35 \;\neq\; \log_2 7 \;=\; 11$$

erkennt man, dass die Gleichung in $\mathbb{Z}_{13}^{\times}$ so nicht ohne weiteres stimmt.

Es gilt aber

$$7 \;=\; 6^7 \;=\; (2^5)^7 \;=\; 2^{35} \bmod 13,$$

d.h. $5 \cdot 7 = 35$ ist eine Lösung zu $2^x = 7 \bmod 13$.

Dies gilt allgemein:

$$a^{\log_a b \cdot \log_b c} \;=\; \left(a^{\log_a b}\right)^{\log_b c} \;=\; b^{\log_b c} \;=\; c \bmod p.$$

Da der Exponent $\log_a b \cdot \log_b c$ größer als $(p-1)$ werden kann, aber $a^{k(p-1)} = 1$ ist, muss man für das eindeutige Logarithmieren im Exponent modulo $(p-1)$ rechnen. Die Formel lautet richtig:

Ist p eine Primzahl und sind a, b Primitivwurzeln modulo p, dann gilt in $\mathbb{Z}_p^{\times}$:

$$\log_a b \cdot \log_b c \;=\; \log_a c \bmod (p-1)$$

Übung 4

Alice berechnet A und schickt es öffentlich an Bob:

$$A \;=\; g^{\alpha} \bmod p \;=\; 5^{12} \bmod 37 \;=\; 10.$$

Bob berechnet B und schickt es öffentlich an Alice:

$$B \;=\; g^{\beta} \bmod p \;=\; 5^{23} \bmod 37 \;=\; 20.$$

Sie berechnen den gemeinsamen geheimen Schlüssel K:

$$K \;=\; B^{\alpha} \;=\; A^{\beta} \;=\; 26.$$

Übung 5

Nein. In $(\mathbb{Z}_m, +)$ ist der diskrete Logarithmus einfach: Zur Bestimmung des diskreten Logarithmus von c zur Basis a muss man das x finden, so dass sich bei x-facher Anwendung von a auf sich selbst c ergibt. Die x-facher Anwendung von a auf sich selbst ist $x \cdot a$, d.h., man muss die Gleichung $x \cdot a \;=\; c \bmod m$ lösen, was mit dem euklidischen Algorithmus leicht möglich ist.

Übung 6

a) Ja, sonst wäre der diskrete Logarithmus leicht zu berechnen.

b) Nein. Zu gegebenem n_0 hat $n = n_0 + p - 1$ den gleichen Wert:

$$f(n) \;=\; g^{n_0+p-1} \bmod p \;=\; g^{n_0} \cdot g^{p-1} \bmod p \;=\; g^{n_0} \cdot 1 \bmod p \;=\; f(n_0).$$

c) Nein, da nicht kollisionsresistent.