

---

# Fortgeschrittene Techniken der Kryptographie

Jürgen Fuß

Episode 5: Diskrete Logarithmen in Gruppen

HAGENBERG | LINZ | STEYR | WELS



UNIVERSITY  
OF APPLIED SCIENCES  
UPPER AUSTRIA

## Definition

Eine **Gruppe** ist ein Quadrupel  $(\mathbb{G}, \circ, \perp, \hat{\circ})$ , wobei  $\mathbb{G}$  irgendeine Menge ist,  $\circ$  eine Funktion von  $\mathbb{G} \times \mathbb{G}$  nach  $\mathbb{G}$ ,  $\hat{\circ}$  eine Funktion von  $\mathbb{G}$  nach  $\mathbb{G}$  und  $\perp \in \mathbb{G}$ , und die folgenden Gesetze erfüllt sind:

1. Für alle  $a, b, c \in \mathbb{G}$  gilt:  $(a \circ b) \circ c = a \circ (b \circ c)$ . ↗
2. Für jedes  $a \in \mathbb{G}$  gilt:  $a \circ \hat{a} = \perp$  und  $\hat{a} \circ a = \perp$ . ↗
3. Für jedes  $a \in \mathbb{G}$  gilt:  $\perp \circ a = a$  und  $a \circ \perp = a$ . ↗

Die Funktion  $\circ$  wird auch als **Verknüpfung** oder **Gruppenoperation** bezeichnet. Das Element  $\perp$  der Gruppe wird ihr **neutrales Element** genannt. Das Element  $\hat{a}$  heißt **inverses Element** von  $a$ .

Gilt außerdem  $a \circ b = b \circ a$  für alle  $a, b \in \mathbb{G}$ , so heißt  $(\mathbb{G}, \circ, \perp, \hat{\circ})$  **abelsche Gruppe**.

# Rückblick: Ordnung eines Elements einer Gruppe

## Definition

Ist  $g$  ein Element der Gruppe  $(\mathbb{G}, \circ, \perp, \wedge)$  und  $\alpha \in \mathbb{N}$ , so schreiben wir

$g^\alpha$  statt  $\underbrace{g \circ g \circ \cdots \circ g}_{\alpha \text{ mal}}$ ,

$g^{-\alpha}$  statt  $\underbrace{\hat{g} \circ \hat{g} \circ \cdots \circ \hat{g}}_{\alpha \text{ mal}}$  (insbes.  $\hat{g} = g^{-1}$ ) und definieren

$$g^0 := \perp$$

$$g^{-\alpha} = \frac{1}{g^\alpha}$$

Die kleinste natürliche Zahl  $\omega$ , so dass  $g^\omega = \perp$  heißt (sofern es so eine Zahl gibt) die **Ordnung von  $g$**  und wird mit  $\text{ord}(g)$  bezeichnet. Gibt es keine solche Zahl, so sagen wir, die Ordnung von  $g$  ist unendlich.

$$\underline{\text{ord}([2]_7) = 3}$$

$$([2]_7 \cdot [2]_7 \cdot [2]_7) \cdot [2]_7 = [4]_7 \cdot [4]_7 = [1]_7$$

$$[3]_7^2 = [2]_7, \quad [3]_7^3 = [6]_7, \quad [3]_7^4 = [4]_7, \quad [3]_7^5 = [8]_7, \quad [3]_7^6 = [1]_7,$$

# Potenzrechenregeln

## Satz

Ist  $(\mathbb{G}, \circ, \perp, \wedge)$  eine Gruppe und  $g \in \mathbb{G}$  und sind  $\alpha, \beta \in \mathbb{Z}$ , dann gelten die bekannten Potenzrechenregeln

$$\underbrace{g \circ g \circ \dots \circ g}_{\alpha} \quad \underbrace{\circ g \circ g \circ \dots \circ g}_{\beta} \quad \leftarrow g^{\alpha} \circ g^{\beta} = g^{\alpha+\beta} \quad \checkmark$$
$$(g^{\alpha})^{\beta} = g^{\alpha \cdot \beta} \quad \checkmark$$
$$g^{\alpha} \circ g^{\alpha} \circ \dots \circ g^{\alpha} \quad \underbrace{\wedge}_{\alpha}$$

$$g^4 \circ g^{-2} \rightarrow g^{4+(-2)} = g^2$$

$$\cancel{g \circ g \circ g \circ g} \circ \cancel{g \circ g \circ g \circ g} \quad \underbrace{\perp}_{g}$$

Ist  $g$  ein Element der Ordnung  $\omega$ , so gilt darüber hinaus

$$\alpha = q \cdot \omega + r \quad 0 \leq r < \omega$$
$$g^{\alpha} = g^{\alpha \text{ mod } \omega}.$$
$$\boxed{g^{\alpha} = g^{q \cdot \omega + r} = g^{q \cdot \omega} \circ g^r = \underbrace{(g^{\omega})^q}_{\perp} \circ g^r = \underbrace{g^r}_{\perp}} \quad r = \alpha \text{ mod } \omega$$

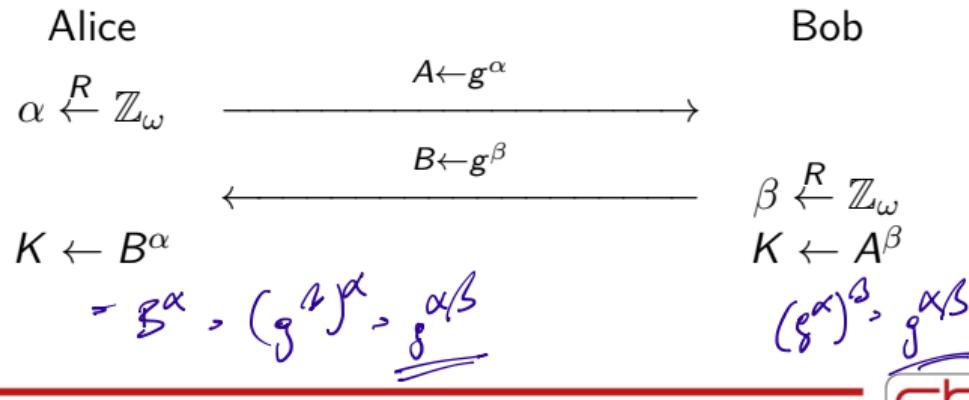
$$g \circ g \circ g \circ g \quad \underbrace{\perp}_{g}$$

# Diffie-Hellman mit Gruppen

## Diffie-Hellman-Schlüsselaustausch in einer Gruppe $\mathbb{G}$

Setup: Alice und Bob einigen sich auf eine Gruppe  $\mathbb{G}$  und auf ein Element  $g \in \mathbb{G}$  mit der Ordnung  $\omega$ . Diese Parameter (**Domain Parameter**) sind öffentlich.

### Key Agreement:



## Diskrete Logarithmen und mehr

# Probleme: DLP

## Definition (DLP)

Es seien  $\mathbb{G}$  eine Gruppe,  $g \in \mathbb{G}$  ein Element der Ordnung  $\omega$  und  $\alpha, \beta \in \mathbb{Z}_\omega$ . Weiterhin seien  $A := g^\alpha$  und  $B := g^\beta$ .

Das **diskrete Logarithmusproblem (DLP)** lautet:

$$(\mathbb{G}, B \rightarrow B^\alpha = K)$$

**Gegeben:**  $\mathbb{G}, g, A$

**Gesucht:**  $\alpha$

Die Zahl  $\alpha$  wird **diskreter Logarithmus von A zur Basis g (in der Gruppe  $\mathbb{G}$ )** genannt.

$$\left| \begin{array}{l} 3^{44} = 23 \\ 3^\alpha = 23 \text{ mod } 50 \end{array} \right.$$

$$(\mathbb{Z}_{50}, +, -, \cdot)$$

$$g = 3$$

$$5 \cdot 3 \Rightarrow 3^5 = 3+3+3+3+3 = 15$$

$$10 \cdot 3 \Rightarrow 3^{10} = 30$$

$$\frac{30}{3} = 10$$

$$\alpha \cdot 3 = 23 \text{ mod } 50$$

$$\alpha = \underline{23 \cdot 3^{-1}} = 23 \cdot 17 = 391 = 67$$

50	1	0		
3	0	1		
2	1	-16	1	
1	-1	17		

## Definition (CDH)

Es seien  $\mathbb{G}$  eine Gruppe,  $g \in \mathbb{G}$  ein Element der Ordnung  $\omega$  und  $\alpha, \beta \in \mathbb{Z}_\omega$ . Weiterhin seien  $A := g^\alpha$  und  $B := g^\beta$ .

Das **Computational Diffie-Hellman Problem (CDH-Problem)** lautet:

**Gegeben:**  $\mathbb{G}, g, A, B$

**Gesucht:**  $g^{\alpha+\beta}$ .

$$g^\alpha \circ g^\beta = g^{\alpha+\beta}$$

## Definition (DDH)

Es seien  $\mathbb{G}$  eine Gruppe,  $g \in \mathbb{G}$  ein Element der Ordnung  $\omega$  und  $\alpha, \beta \in \mathbb{Z}_\omega$ . Weiterhin seien  $A := g^\alpha$  und  $B := g^\beta$ .

Das **Decisional Diffie-Hellman Problem (DDH-Problem)** lautet:

Es seien  $g_0 := g^{\alpha\beta}$ ,  $g_1 \xleftarrow{R} \mathbb{G}$  und  $b \xleftarrow{R} \{0, 1\}$ .

**Gegeben:**  $\mathbb{G}, g, A, B, g_b \leftarrow$

**Gesucht:**  $b$ .

1. Wählt man als Gruppe  $(\mathbb{Z}_p^*, \cdot, 1, -1)$ , so erhält man das bekannte DH-Verfahren. Die DL-, CDH- und DDH-Probleme gelten – zumindest für geeignete Parameter – als praktisch nicht lösbar.  
Damit das DLP jedoch ausreichend schwierig ist, müssen **sehr große Primzahlen**  $p$  verwendet werden. Außerdem werden auch Elemente  $g$  mit **sehr großer Ordnung**  $\omega$  benötigt. Somit müssen sehr große Potenzen berechnet werden, was ineffizient sein kann.  
Wir beschäftigen uns noch eingehender mit der Berechnung von diskreten Logarithmen (insb. in diesen Gruppen).

2. Wählt man als Gruppe  $(\mathbb{Z}_n, +, 0, -)$ , so lassen sich diskrete Logarithmen ganz einfach berechnen. In diesem Fall lautet das Problem:

**Gegeben:**  $n, g, A = \underbrace{(g + \cdots + g)}_{\alpha\text{-mal}} \bmod n$

**Gesucht:**  $\alpha$

Offenbar ist  $A = \alpha \cdot g \bmod n$ . Mit dem erweiterten Euklidschen Algorithmus lässt sich der Kehrwert von  $g$  modulo  $n$  berechnen und damit  $\alpha = A \cdot g^{-1} \bmod n$ .

3. Weitere interessante Gruppen – die elliptischen Kurven – werden wir noch kennenlernen. Für diese Gruppen stellt sich das DLP als noch etwas schwieriger heraus als für  $\mathbb{Z}_p^*$ . Als Konsequenz können dort bei gleicher Sicherheit kleinere Parameter verwendet werden, was die Verfahren bedeutend schneller macht.

# Der Ordnung auf der Spur

# Mehr Ordnung

Es sei wiederum  $\mathbb{G}$  eine Gruppe. Sind  $g, h, h' \in \mathbb{G}$  und ist  $g \circ h = g \circ h'$ , so ist  $h = h'$ ; dies ist einfach zu erkennen, man braucht nur die erste Gleichung (links und rechts) mit  $\widehat{g}$  zu verknüpfen.

$$\begin{aligned} g \circ h &= g \circ h' \\ (\widehat{g} \circ g) \circ h &= (\widehat{g} \circ g) \circ h' \\ =\perp &= \perp \\ h &= h' \end{aligned}$$

Dies bedeutet aber, dass aus zwei verschiedenen Gruppenelementen  $h, h'$  durch Verknüpfung mit  $g$  wiederum verschiedene Gruppenelemente werden.

# Ordnung und Ordnung

Ist  $\mathbb{G}$  eine endliche abelsche Gruppe der Ordnung  $n$  mit den Elementen  $\underline{g_1, g_2, \dots, g_n}$ , und ist  $\underline{g} \in \mathbb{G}$ , so sind auch  $g \circ g_1, \dots, g \circ g_n$  verschiedene Elemente – und damit alle Elemente – der Gruppe  $\mathbb{G}$ . Betrachtet man nun das Ergebnis der Verknüpfung aller Elemente von  $\mathbb{G}$ , so erhält man

$$\begin{aligned} g_1 \circ g_2 \circ \dots \circ g_n &= (\underline{g} \circ g_1) \circ (\underline{g} \circ g_2) \circ \dots \circ (\underline{g} \circ g_n), \\ g_1 \circ g_2 \circ \dots \circ g_n &= \underline{g^n} \circ (g_1 \circ g_2 \circ \dots \circ g_n). \end{aligned}$$

Verknüpfen mit  $(g_1 \circ g_2 \circ \dots \circ g_n)^{-1}$  ergibt

$$\perp = \underline{g^n}.$$

$$\begin{array}{c} (\mathbb{Z}_7^*, \cdot, ^{-1}, 1) \\ n=6 \\ g^6 = 1 \pmod{7} \end{array}$$

# Ordnungen und Ordnungen

Dieses Resultat gilt allgemeiner nicht nur in abelschen Gruppen.

## Satz

Ist  $\mathbb{G}$  eine endliche Gruppe, dann gilt für jedes Element  $g \in \mathbb{G}$

$$g^{|\mathbb{G}|} = \perp.$$

## Satz

Es seien  $\mathbb{G}$  eine endliche Gruppe,  $g \in \mathbb{G}$  ein Element der Ordnung  $\omega$  und  $\alpha \in \mathbb{N}$ . Dann gilt:

1. Die Elemente  $g, g^2, \dots, g^\omega$  sind alle verschieden.
2. Ist  $\underline{g^\alpha = \perp}$ , dann gilt  $\omega \mid \alpha$ , und umgekehrt.
3. Die Ordnung  $\omega$  von  $g$  ist ein Teiler von  $|\mathbb{G}|$ .

$$g^\omega = \perp$$

$$g^\alpha = \perp \quad \alpha \in \mathbb{N}, \quad \omega \leq \alpha < \beta \leq \omega$$

$$\perp = g^{\beta-\alpha} \neq$$

$$\begin{aligned} \alpha &= q \cdot \omega + r \\ \alpha &\leq q \cdot \omega \end{aligned}$$
$$\perp = g^\alpha = g^{q \cdot \omega + r} = (g^\omega)^q \circ g^r = g^r = \perp$$
$$r = 0$$

# Erzeugende Elemente, zyklische Gruppen

Es kann passieren, dass die Ordnung eines Elements  $g$  einer Gruppe  $\mathbb{G}$  gleich der Ordnung  $n$  der Gruppe ist. In diesem Fall sind die Potenzen  $g, g^2, \dots, g^n$  alle verschieden und somit genau die  $n$  verschiedenen Elemente von  $\mathbb{G}$ .

Aus gutem Grund heißt  $g$  dann **erzeugendes Element** von  $\mathbb{G}$ . Die Gruppe  $\mathbb{G}$  heißt in diesem Fall **zyklische Gruppe** (Die Potenzen von  $g$  durchlaufen „zyklisch“ alle Elemente der Gruppe.).

Um zu überprüfen, ob ein Element  $g$  einer Gruppe  $\mathbb{G}$  die Ordnung  $\omega$  hat, ist folgender Satz nützlich, den wir (für die Gruppen  $\mathbb{Z}_p^*$ ) schon aus der LVA „Grundlagen der Kryptographie“ kennen.

### Satz

Es sei  $\mathbb{G}$  eine Gruppe und  $g \in \mathbb{G}$ . Weiterhin sei  $\omega \in \mathbb{N}$ . Dann gilt:

$$\omega = 12$$

$$= 2^2 \cdot 3$$

$$\Rightarrow 2, 3$$

1. Ist  $g^\omega \neq \perp$ , dann ist  $\text{ord}(g) \neq \omega$ .
2. Gibt es einen Primfaktor  $p$  von  $\omega$ , so dass  $g^{\omega/p} = \perp$ , dann ist  $\text{ord}(g) \neq \omega$  (sondern maximal  $\omega/p$ ).
3. Andernfalls (wenn 1. und 2. nicht zutreffen) ist  $\text{ord}(g) = \omega$ .

$$\begin{aligned} g^{12_2} &= g^c = \perp ? \\ g^{12_3} &, g^u = \perp ? \end{aligned}$$

# Ordnungen von Potenzen eines Elements

Ist die Ordnung eines Elements bekannt, so lassen sich die Ordnungen von Potenzen dieses Elements bestimmen. Auch das kennen wir bereits aus den „Grundlagen der Kryptographie“.

## Satz

Ist  $\underline{g \in \mathbb{G}}$  ein Element der Ordnung  $\omega$  und ist  $\alpha \in \mathbb{N}$ , dann ist die Ordnung von  $g^\alpha$  gleich

$$\text{ord}(g^\alpha) = \frac{\omega}{\text{ggT}(\alpha, \omega)}.$$

$$\text{ord}(g) = 24$$

$$\text{ord}(g^{10}) = \frac{24}{\text{ggT}(10, 24)} = \frac{24}{2} = 12$$

$$\text{ord}(g^6) = 6 = \frac{24}{4}$$

# Wie viele Erzeuger?

## Satz

Es sei  $p \in \mathbb{P}$ . Es sei  $d$  ein positiver Teiler von  $p - 1$ .

- Dann gibt es genau  $\varphi(d)$  Elemente der Ordnung  $d$  in  $\mathbb{Z}_p^*$ .
- Insbesondere gibt es genau  $\varphi(p - 1)$  erzeugende Elemente in  $\mathbb{Z}_p^*$ .

$$p = 127$$

$$p-1 = 126 = 2 \cdot 3^2 \cdot 7$$

$$\varphi(126) = 126 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right)$$
$$126 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 36$$

$$\begin{array}{r} 126 \\ 63 \\ 21 \\ 7 \\ 1 \end{array} \Big| \begin{array}{r} 2 \\ 3 \\ 2 \\ 7 \\ 1 \end{array}$$

$$\Pr[\text{erz. ET}] = \frac{36}{126} = \frac{18}{63} = \frac{2}{7}$$

$$\left. \begin{array}{l} g^{\frac{126}{2}} \neq 1 \\ g^{\frac{126}{3}} \neq 1 \\ g^{\frac{126}{7}} \neq 1 \end{array} \right\} \Rightarrow \text{ord. El.}$$

$$\text{ord}(h) = 7$$

$$h = \underbrace{g^{\alpha}}_{18} = \overbrace{\frac{126}{2 \cdot 3^2}}^{18} = \underline{\underline{7}}$$

ggT( $\alpha, 126$ )