8.8 Schlüsseltausch nach Diffie und Hellman

Das Schlüsselverteilungsproblem sieht aus wie ein Henne-Ei-Problem: Um sicher zu reden, braucht man einen gemeinsamen Schlüssel — und um den auszutauschen, müsste man schon sicher reden können. 1976 zeigten **Whitfield Diffie** und **Martin Hellman**, dass dieser Schluss falsch ist. Zwei Partner können sich auf einen gemeinsamen geheimen Schlüssel einigen, indem sie **ausschließlich öffentlich** miteinander sprechen. Niemand muss das Geheimnis jemals übertragen, weil es erst beim Rechnen entsteht.

Leitidee: Die Idee in einem Bild

Alice und Bob mischen Farben. Beide starten mit demselben, allen bekannten Gelb. Alice gibt heimlich etwas Rot dazu, Bob heimlich etwas Blau; die Mischungen tauschen sie offen aus. Nun gibt Alice ihr Rot in Bobs Mischung, Bob sein Blau in Alices — beide halten am Ende denselben Braunton in der Hand. Ein Beobachter hat Gelb, Orange und Grün gesehen und kommt damit nicht weiter: Mischen ist leicht, Entmischen ist schwer.

Die Rolle des Mischens übernimmt in der Mathematik das **Potenzieren mit Rest**. Öffentlich vereinbart werden eine Primzahl p und eine Zahl g mit $1 < g < p$, die **Basis**. Beide Werte dürfen alle kennen.

Schritt	Alice	Bob
1	wählt geheim a	wählt geheim b
2	berechnet $A = g^a \bmod p$	berechnet $B = g^b \bmod p$
3	sendet A an Bob	sendet B an Alice
4	berechnet $K = B^a \bmod p$	berechnet $K = A^b \bmod p$

Dass am Ende wirklich dieselbe Zahl herauskommt, ist nichts als ein Potenzgesetz:

$$K = B^a = \left(g^b\right)^a = g^{b \cdot a} = g^{a \cdot b} = (g^a)^b = A^b \pmod p$$

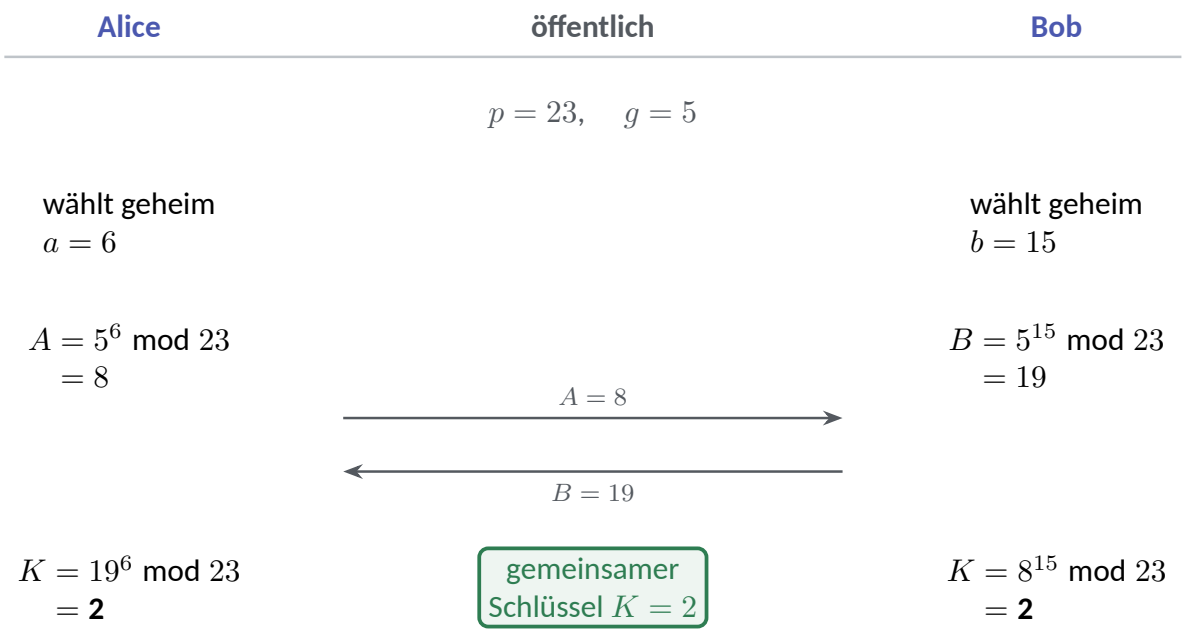
Beispiel: Durchgerechnet mit kleinen Zahlen

Öffentlich: $p = 23$ und $g = 5$.

- Alice wählt $a = 6$ und berechnet $A = 5^6 \bmod 23 = 15\,625 \bmod 23 = 8$.
- Bob wählt $b = 15$ und berechnet $B = 5^{15} \bmod 23 = 19$.
- Sie tauschen $A = 8$ und $B = 19$ offen aus.
- Alice rechnet $K = 19^6 \bmod 23 = 2$.
- Bob rechnet $K = 8^{15} \bmod 23 = 2$.

Beide haben $K = 2$, ohne dass die 2 jemals über die Leitung ging. Die Probe: $5^{6 \cdot 15} \bmod 23 = 5^{90} \bmod 23 = 2$.

Rechnen Sie $5^{15} \bmod 23$ nicht mit dem Taschenrechner aus — 5^{15} hat elf Stellen. Nehmen Sie nach jedem Schritt den Rest: $5^2 = 25 \equiv 2$, also $5^4 \equiv 2^2 = 4$, $5^8 \equiv 4^2 = 16$ und damit $5^{15} = 5^8 \cdot 5^4 \cdot 5^2 \cdot 5^1 \equiv 16 \cdot 4 \cdot 2 \cdot 5 = 640 \equiv 19 \pmod{23}$. In Python genügt `pow(5, 15, 23)`.



Übertragen werden nur p, g, A und B. Wer alles vier mitliest, müsste daraus a oder b zurückrechnen — den *diskreten Logarithmus*. Für kleine Zahlen geht das durch Probieren, für Zahlen mit Hunderten Stellen nicht.

Der Schlüsseltausch nach Diffie und Hellman.

Warum ist das sicher? Ein Lauscher kennt p, g, A und B. Um K zu berechnen, bräuchte er einen der beiden geheimen Exponenten, müsste also aus $A = g^a \bmod p$ die Zahl a zurückgewinnen. Diese Aufgabe heißt **diskreter Logarithmus**. Bei $p = 23$ löst man sie in zwanzig Versuchen; bei einer Primzahl mit 600 Stellen ist kein Verfahren bekannt, das in vertretbarer Zeit zum Ziel kommt. Potenzieren mit Rest ist also eine Einwegfunktion — leicht vorwärts, praktisch unmöglich rückwärts.

Merke

Diffie-Hellman ist **kein Verschlüsselungsverfahren**. Es überträgt keine Nachricht, sondern erzeugt bei beiden Partnern dieselbe Zufallszahl. Verschlüsselt wird danach symmetrisch, etwa mit AES — der ausgehandelte Wert ist der Sitzungsschlüssel. Genau so arbeitet heute jede HTTPS-Verbindung.

Stolperstein

Der Schlüssel entsteht bei jedem Verbindungsaufbau neu und wird danach verworfen. Das hat einen Namen und einen Zweck: **Perfect Forward Secrecy**. Wer den heutigen Datenverkehr mitschneidet und in zehn Jahren den privaten Schlüssel des Servers erbeutet, kann damit nichts anfangen — die Sitzungsschlüssel von damals stehen nirgends mehr.

LK

Der Mittelsmann. Diffie-Hellman sichert zu, dass am Ende *zwei* Partner denselben Schlüssel besitzen. Es sichert nicht zu, **wer** diese beiden sind. Mallory kann sich in die Leitung setzen und mit jeder Seite einen eigenen Schlüsseltausch durchführen:

1. Mallory wählt selbst ein geheimes $m = 3$ und berechnet $M = 5^3 \bmod 23 = 10$.
2. Alice sendet $A = 8$ los. Mallory fängt es ab und schickt Bob stattdessen $M = 10$.
3. Bob sendet $B = 19$. Mallory fängt auch das ab und schickt Alice $M = 10$.
4. Alice rechnet $K_1 = 10^6 \bmod 23 = 6$ — und Mallory rechnet $8^3 \bmod 23 = 6$.
5. Bob rechnet $K_2 = 10^{15} \bmod 23 = 5$ — und Mallory rechnet $19^3 \bmod 23 = 5$.

Mallory hat nun **zwei** Schlüssel: 6 für die Strecke zu Alice, 5 für die Strecke zu Bob. Er entschlüsselt jede Nachricht, liest sie, verschlüsselt sie neu und reicht sie weiter. Alice und Bob bemerken nichts, denn beide Verbindungen sind kryptographisch einwandfrei. Wie sich das abwehren lässt, steht im nächsten Abschnitt.

Arbeitsauftrag 7

26. Führen Sie den Schlüsseltausch mit $p = 13$, $g = 2$, $a = 5$ und $b = 9$ durch. Geben Sie A, B und K an und prüfen Sie, dass beide Seiten dasselbe erhalten.
27. Begründen Sie mit dem Potenzgesetz, warum B^a und A^b denselben Rest lassen müssen.
28. Ein Lauscher kennt $p = 23$, $g = 5$ und $A = 8$. Bestimmen Sie a durch Probieren und notieren Sie, wie viele Versuche Sie gebraucht haben. Was sagt das über die Sicherheit kleiner Primzahlen?
29. Warum darf a nicht 1 sein? Was passiert, wenn Alice und Bob zufällig denselben geheimen Wert wählen?
30. Berechnen Sie $7^{20} \bmod 11$ von Hand, indem Sie nach jedem Schritt den Rest nehmen. Vergleichen Sie mit `pow(7, 20, 11)`.
31. Erklären Sie in drei Sätzen, warum Diffie-Hellman das Schlüsselverteilungsproblem löst, das Problem der Echtheit eines Gegenübers aber nicht.

Gymnasium Ottweiler