Diffie-Hellman-Algorithmus

Schlüsselaustausch

Um einen Klartext zu verschlüsseln und auch anschließend zu entschlüsseln, brauchen Sender und Empfänger denselben Schlüssel. Dieser ist meist eine Zahl. Sender und Empfänger müssen den Schlüssel **geheim** austauschen können, das heißt, ohne dass ein Dritter ihn erfährt.

Lange galt es als unmöglich, im »öffentlichen Raum«, also für jeden mithörbar, einen geheimen Schlüssel auszutauschen. Aber 1976 wurde von Martin Hellman, Whitfield Diffie und Ralph Merkle der **Diffie-Hellman-Algorithmus** entwickelt. Er ermöglicht die Vereinbarung eines gemeinsamen geheimen Schlüssels über eine unsichere Verbindung.

Hinweis: Der Diffie-Hellman-Algorithmus arbeitet mit der Modulo-Funktion. Falls du dich nicht sicher im Umgang damit fühlst, bearbeite bitte zuerst die entsprechende Station.

Mit dem Diffie-Hellman-Algorithmus können also zwei Beteiligte - nennen wir sie Alice und Bob - im öffentlichen Raum einen geheimen Schlüssel vereinbaren, ohne dass eine dritte Person, die alles mithört, - nennen wir sie Eve - den Schlüssel erfährt.

Der Algorithmus

Alice und Bob vereinbaren zu Beginn öffentlich eine Primzahl **p** und eine natürliche Zahl **g**. Dabei muss **g** kleiner sein als **p**. Zum Berechnen von **A** bzw. **B** wählte Alice die Zahl **a**, die nur sie kennt, und Bob wählt die Zahl **b**, die nur er kennt. **A** und **B** werden öffentlich ausgetauscht. (Berechnungen siehe unten)
Eve kennt also **p**, **g**, **A** und **B**, aber nicht **a** und **b**. Den geheimen Schlüssel **K** können Alice und Bob berechnen, Eve nicht. (Ein Beispiel gibt es auf der nächsten Seite.)

privater Raum:	öffentlicher Raum:	privater Raum:
Alice 	Eve 	Bob 
Wähle a, mit a < p Berechne $A = g^a \mod p$ Berechne $K = B^a \mod p$	p und g A → ← B	Wähle b, mit b < p Berechne $B = g^b \mod p$ Berechne $K = A^b \mod p$

Diffie-Hellman-Algorithmus

Schlüsselaustausch

Beispiel

Alice und Bob vereinbaren öffentlich: $p = 13$ und $g = 4$:

privater Raum:	öffentlicher Raum:	privater Raum:
Alice 	 Eve	Bob 
	$p = 13, g = 4$	
Wähle a, mit a < p		Wähle b, mit b < p
$a = 3$		$b = 5$
Berechne $A = g^a \mod p$		Berechne $B = g^b \mod p$
$A = g^a \mod p$ $A = 4^3 \mod 13$ $= 64 \mod 13$ $= 12$		$B = g^b \mod p$ $B = 4^5 \mod 13$ $= 1024 \mod 13$ $= 10$
	$A = 12 \longrightarrow$	
	$\longleftarrow B = 10$	
Berechne $K = B^a \mod p$		Berechne $K = A^b \mod p$
$K = 10^3 \mod 13$ $= 1000 \mod 13$ $= 12$		$K = 12^5 \mod 13$ $= 248832 \mod 13$ $= 12$

Der von Alice und Bob berechnete geheime Schlüssel in diesem Beispiel ist 12. Um den Schlüssel zu finden, müsste Eve nur alle Zahlen ausprobieren, die kleiner als p, hier also 13, sind. Das wäre einfach.
Normalerweise sind die Zahlen aber so groß, dass es auch mit den schnellsten Computern fast unmöglich ist, den Schlüssel durch Ausprobieren zu finden.

Version vom 2019-08-09

BERGISCHE UNIVERSITÄT WUPPERTAL