Diffie-Hellman-Algorithmus (sicherer Schlüssel-Tausch)

K 6

Aufgabe:

Lies den folgenden Text genau durch und betrachte den illustrierten Rechenweg.

Spiele den Diffie-Hellmann-Algorithmus zu dritt durch. Der Hacker soll versuchen, die Kommunikation der anderen beiden zu knacken, indem er den geheimen Schlüssel errechnen kann.

Zeit: 30‘ **Sozialform:** GA

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. 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 einfach «Hacker» - den Schlüssel erfährt.

Hinweis:
*Der Diffie-Hellman-Algorithmus arbeitet mit der Modulo-Funktion. Falls du dich nicht sicher im Umgang damit fühlst, bearbeite bitte zuerst die entsprechende Aufgabe **M1 Modulo**.*

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) Der Hacker kennt also p, g, **A** und **B**, aber nicht **a** und **b**. Den geheimen Schlüssel **K** können Alice und Bob berechnen, der Hacker nicht. (Ein Beispiel gibt es auf der nächsten Seite.)

Privater Raum *Alice*	**Öffentlicher Raum** *Hacker*	**Privater Raum** *Bob*
		
Wähle a, a < p	Der Hacker kennt den 1. Schlüssel p, g	Wähle b, b < p
Berechne **A** $A = g^a \bmod p$	Der Hacker kennt den 2. Schlüssel ← B	Berechne **B** $B = g^b \bmod p$
Berechne **K** $K = B^a \bmod p$	A →	Berechne **K** $K = A^b \bmod p$

Beispiel

Alica und Bob vereinbaren einen Schlüssel; p = 23, g = 9

Privater Raum *Alice*	Öffentlicher Raum *Hacker*	Privater Raum *Bob*
		
	Der Hacker kennt den 1. Schlüssel **p = 23, g = 9**	
Alice wählt a, a < p **a = 5**		Bob wählt b, b < p **b = 3**
Alice berechnet **A** $A = g^a \bmod p$ $A = 9^5 \bmod 23$ $A = 59´049 \bmod 23$ **A = 8**		Bob berechnet **B** $B = g^b \bmod p$ $B = 9^3 \bmod 23$ $B = 729 \bmod 23$ **B = 16**
	Der Hacker kennt den 2. Schlüssel B = 16 ← A = 8 →	
Alice berechnet **K** $K = B^a \bmod p$ $K = 16^5 \bmod 23$ $K = 1´048´576 \bmod 23$ **K = 6**		Bob berechnet **K** $K = A^b \bmod p$ $K = 8^3 \bmod 23$ $K = 512 \bmod 23$ **K =6**

Der von Alice und Bob berechnete geheime Schlüssel in diesem Beispiel ist 6. Um den Schlüssel zu finden, müsste der Hacker nur alle Zahlen ausprobieren, die kleiner als **p**, hier also 23, 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.

Der Diffie-Hellman-Schlüsselaustausch ist ein Protokoll zur Schlüsselvereinbarung. Es handelt sich um das erste der sogenannten asymmetrischen Kryptoverfahren (auch Public-Key-Kryptoverfahren), das veröffentlicht wurde und ermöglicht, dass zwei Kommunikationspartner über eine öffentliche, abhörbare Leitung einen gemeinsamen geheimen Schlüssel in Form einer Zahl vereinbaren können, den nur diese kennen und ein potenzieller Lauscher nicht berechnen kann. Unterschiedliche Varianten des Diffie-Hellman-Merkle-Verfahrens werden heute für die Schlüsselverteilung in den Kommunikations- und Sicherheitsprotokollen des Internets eingesetzt, beispielsweise in den Bereichen des elektronischen Handels. Dieses Prinzip hat damit eine wichtige praktische Bedeutung.

Auftrag

Bildet eine Dreiergruppe und spielt den Diffie-Hellman-Algorithmus durch. Eine/r von euch ist Alice, eine/r Bob und der oder die Dritte ist der Hacker. Alice und Bob tauschen den Schlüssel aus und der Hacker versucht den Schlüssel (K) herauszufinden, um die geheime Nachricht lesen zu können. Führt den Algorithmus mit p = 11 und g = 3 ein- bis dreimal mit verschiedenen Rollen aus. **Notiert euer Ergebnis**. Hat der Hacker den Schlüssel herausgefunden?

Benutze die Python 3 IDLE als Rechner!

```
>>> 59049 % 23
8
>>> 729 % 23
16
>>> 1048576 % 23
6
>>> 512 % 23
6
```

Aufgabe für echte Hacker!°

Erstelle ein Programm in Python, welches dir automatisch alle Zahlen, Zwischenergebnisse und Schlüssel berechnet. Die nötigen Variablen für die Eingabe sind (p, g, a), resp. (p, g, b)

Primzahlen

2,	3,	5,	7,	11,	13,	17,	19,	23,	29,	31,	37,	41,	43,
47,	53,	59,	61,	67,	71,	73,	79,	83,	89,	97,	101,	103,	107,
109,	113,	127,	131,	137,	139,	149,	151,	157,	163,	167,	173,	179,	181,
191,	193,	197,	199,	211,	223,	227,	229,	233,	239,	241,	251,	257,	263,
269,	271,	277,	281,	283,	293,	307,	311,	313,	317,	331,	337,	347,	349,
353,	359,	367,	373,	379,	383,	389,	397,	401,	409,	419,	421,	431,	433,
439,	443,	449,	457,	461,	463,	467,	479,	487,	491,	499,	503,	509,	521,
523,	541,	547,	557,	563,	569,	571,	577,	587,	593,	599,	601,	607,	613,
617,	619,	631,	641,	643,	647,	653,	659,	661,	673,	677,	683,	691,	701,
709,	719,	727,	733,	739,	743,	751,	757,	761,	769,	773,	787,	797,	809,
811,	821,	823,	827,	829,	839,	853,	857,	859,	863,	877,	881,	883,	887,
907,	911,	919,	929,	937,	941,	947,	953,	967,	971,	977,	983,	991,	997,
1009,	1013,	1019,	1021,	1031,	1033,	1039,	1049,	1051,	1061,	1063,	1069,	1087,	1091,