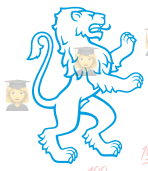

Kantonsschule Im Lee

Informatik

Kryptologie

Skript

Judith Beestermöller

Inhaltsverzeichnis

Kapitel 1

Schlüsselaustausch

1.1 Diffie-Hellman-Merkle-Schlüsselaustausch

Wir haben zuletzt gezeigt, dass Alice mit dem One-Time-Pad verschlüsselte Nachrichten an Bob schicken kann, die von Eve nicht entschlüsselt werden können. Die Voraussetzung hierfür war, dass jede Nachricht mit einem anderen zufällig gewählten Schlüssel verschickt wird. Damit Bob die Nachricht entschlüsseln kann, muss er wissen, welchen Schlüssel Alice verwendet hat.

Aber Moment, damit Alice und Bob One-Time-Pad verwenden können, müssen sie sich auf einen Schlüssel einigen, ohne dass Eve mithört. Das **Schlüsselverteilungsproblem** (auch **Schlüsselaustauschproblem** genannt) beschreibt die grundlegende Herausforderung in der Kryptographie, wie zwei (oder mehr) Kommunikationspartner einen gemeinsamen, geheimen Schlüssel sicher austauschen können.

Das Problem ist ein klassisches Henne-Ei Problem:

1. Um sicher über einen unsicheren Kanal kommunizieren zu können, brauchen Alice und Bob einen gemeinsamen geheimen Schlüssel.
2. Um diesen geheimen Schlüssel auszutauschen, brauchen sie einen sicheren Kanal.

Damit stellt sich die Frage, ob es möglich ist, einen gemeinsamen geheimen Schlüssel auf einem komplett öffentlichen Kanal zu erstellen.

Wir haben bereits einen naiven Schlüsselaustausch mit dem Bin-One-Time-Pad gesehen. Zwar haben bei diesem Schlüsselaustausch Alice und Bob am Ende den selben Schlüssel gehabt, aber Eve konnte anhand der übersendeten Nachrichten ebenfalls den Schlüssel einfach herausfinden.

Der Diffie-Hellman-Merkle Schlüsselaustausch erlaubt es Alice und Bob einen Schlüssel zu generieren, welcher (bis heute!) von Eve nicht effizient geknackt werden kann. Das Verfahren wurde 1976 von Whitfield Diffie und Martin Hellman publiziert. Wichtige Vorarbeiten leistete Ralph Merkle.

Wir werden im nächsten Abschnitt eine weiterentwickelte Version des Schlüsselaustauschs kennenlernen, bei der Eve am Ende den Schlüssel nicht kennt.

Ralph Merkle, Martin Hellman, Whitfield Diffie (left to right) — Source

Abbildung 1.1: Whitfield Diffie, Martin Hellman und Robert Merkle

Wir wollen zunächst die Grundidee des Schlüsselaustauschs anhand von Farbmischungen veranschaulichen. Achten Sie auf die Farbmengen in untenstehender Abbildung 1.2.

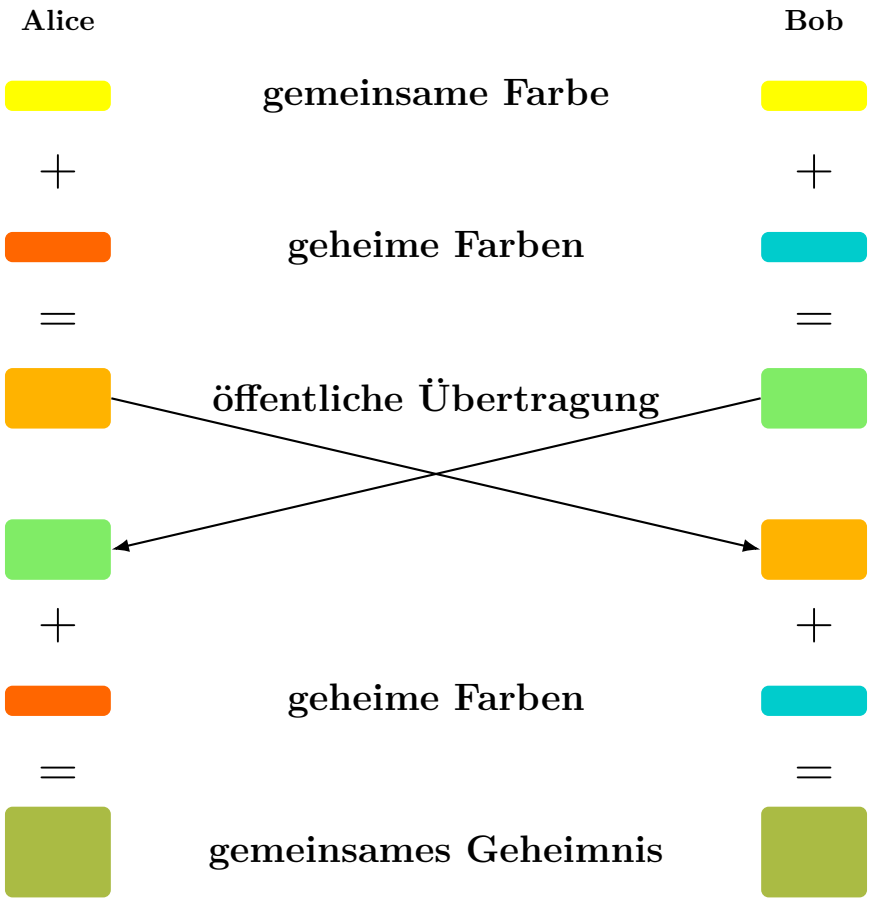

Abbildung 1.2: Dieses Schema zeigt eine Abstraktion, wie das Diffie-Hellmann-Merkle Protokoll funktioniert.

Abbildung 1.2 zeigt eine Abstraktion, wie das Diffie-Hellmann-Merkle Protokoll funktioniert. Zu Beginn einigen sich Alice und Bob auf eine Ausgangsfarbe. Diese ist nicht geheim. Zusäzlich wählt jeder eine eigene Farbe, welcher nur er kennt. Alice mischt die öffentliche Farbe mit ihrer geheimen Farbe und schickt sie an Bob. Ebenso mischt Bob die gemeinsame Farbe mit seiner geheimen Farbe und schickt diese an Alice. Sowohl Alice als auch Bob mischen die erhaltene Farbe wieder mit ihrer eigenen Farbe. Das Endergebnis ist bei beiden gleich und entspricht dem Schlüssel, den sie von nun an verwenden können.

Aufgabe 1.1

Welche Eigenschaft der Farbmischung nutzen Alice und Bob, damit beide am Ende die gleiche geheime Farbe erhalten? Wie würden wir diese Eigenschaft in der Mathematik nennen? Welche mathematischen Operationen kennen Sie, die diese Eigenschaften haben?

Lösungsvorschlag zu Aufgabe 1.1

Alice und Bob nutzen, das Faktum, dass die Reihenfolge der Farben in der Farbmischung irrelevant ist für die Endfarbe. In der Mathematik nennen wir eine Operation **kommutativ**, wenn wir die Operanden vertauschen können. Beispiele für kommutative Operationen sind die Addition und die Multiplikation.

Damit Eve nicht in der Lage ist, die geheime Farbe zu erkennen, muss die Operation für Eve irreversibel sein. Das heisst, es muss für Eve unmöglich sein, den Prozess Rückgängig zu machen. Zum Glück dies ist im konkreten Beispiel der Fall der Fall: Mischen wir gelbe und blaue Farbe zu grün so ist es extrem schwierig, aus der grünen Farbe wieder die reinen gelben und blauen Pigmente herauszutrennen. Wäre dies nicht der Fall, so könnte Eve ganz einfach Alice und Bobs geheime Farben herausfinden und damit auch die geheime gemeinsame Farbe berechnen könnte.

Aufgabe 1.2

Mischen Sie zwei Farben und versuchen Sie die Ursprungsfarben wiederherzustellen. Schaffen Sie es, wenn Sie die Farben am Computer mischen und Sie die RGB-Werte der Farben kennen?

Lösungsvorschlag zu Aufgabe 1.2

Wenn wir zwei Farben zu gleichen Anteilen mischen, so gilt

$$(R_F, G_F, B_F) = (\frac{R_1 + R_2}{2}, \frac{G_1 + G_2}{2}, \frac{B_1 + B_2}{2}),$$

wobei (R_F, G_F, B_F) das Ergebnis der Mischung und (R_1, G_1, B_1) und (R_2, G_2, B_2) die Ursprungsfarben sind. Wenn nur das Endergebnis bekannt ist, so können wir die Ursprungsfarben nicht wiederherstellen, sofern $(R_F, G_F, B_F) \notin \{(0,0,0), (255,255,255)\}$

Aufgabe 1.3

Können wir aus Aufgabe 1.2 schliessen, dass das Schema, welches in Abbildung 1.2 dargestellt wird, von Eve nicht geknackt werden kann?

Lösungsvorschlag zu Aufgabe 1.3

Nein, da die gemeinsame Farbe Eve bekannt ist, kann sie sehr einfach die geheimen Farben von Alice und Bob herausfinden und damit auch die Geheimfarbe.

Das eigentliche Diffie-Hellman-Merkle Protokoll verwendet keien Farben, aber weisst die oben besprochenen Eigenschaften auf.

Vorgehen 1.1 (Protokoll DIFFIE-HELLMAN-MERKLE (DHM))**:**
myprocedure:Diffie

Ausgangssituation: Alice und Bob haben sich zuvor öffentlich auf eine grosse Primzahl p und eine positive natürliche Zahl g geeinigt. Dabei ist g kleiner als p.

Ziel: Alice und Bob möchten gemeinsam mit einer öffentlichen Kommunikation einen Schlüssel s_{AB} vereinbaren. Diesen Schlüssel darf keine Drittperson in Erfahrung bringen.

1. Alice wählt zufällig eine positive ganze Zahl a mit $a < p$ und hält diese geheim. Dann berechnet sie mit dieser geheimen Zahl:

$$x := g^a \mod p$$

   und sendet x an Bob.
2. Bob wählt zufällig eine positive ganze Zahl b mit $b < p$ und hält diese geheim. Dann

berechnet er die Zahl

$$y := g^b \mod p$$

und sendet y an Alice.

3. Alice erhält y von Bob und berechnet mit ihrer geheimen Zahl a die Zahl

$$s_{AB} := y^a \mod p.$$

4. Bob berechnet mit dem erhaltenen x und seiner geheimen Zahl b die Zahl

$$s_{BA} := x^b \mod p.$$

Mithilfe der Rechengesetze der Modulo-Operation kann bewiesen werden, dass tatsächlich

$$s_{AB} = s_{BA}$$

gilt und somit Alice und Bob dieselbe Zahl berechnet haben. Diese Zahl s_{AB} ist der gemeinsame Schlüssel.

Aufgabe 1.4

Führen Sie das DHM Verfahren selber mit Ihrer/Ihrem Sitznachbarn/in aus. Verwenden Sie

$$p := 19 \quad \text{und} \quad g := 8$$

(Sie können auch eigene Werte wählen) als öffentlich bekannte Schlüssel.

Lösungsvorschlag zu Aufgabe 1.4

Sei $a = 4$ und $b = 7$

$$\Rightarrow x = 11,\ y = 8,\ S_{AB} = S_{BA} = 11$$

Aufgabe 1.5

Versuchen Sie das Kommunikationsprotokoll DHM zu knacken, indem Sie für die gegebenen Werte p, g, x und y jeweils die geheimen Zahlen a und b berechnen und daraus dann den vereinbarten Schlüssel s_{AB}.

(a) $g = 4, p = 13, x = 12, y = 3$
(b) $g = 5, p = 7, x = 6, y = 2$

Lösungsvorschlag zu Aufgabe 1.5

(a) $a = 3, b = 2$ und $s_{AB} = 12^2 \mod 13 = 1 = 3^4 \mod 13 = S_{BA}$
(b) $a = 3, b = 4$ und $s_{AB} = 6^4 \mod 7 = 1 = 2^3 \mod 7 = S_{BA}$

Die Funktion $r = g^x \mod p$ wird diskrete Exponentialfunktion genannt und ist auch für grosse Exponenten (auch mit mehr als 100-Bit) für den Computer in unter einer Sekunde berechenbar. Die Inversefunktion (Berechnung von x bei gegebenem $r, g,$ und$p$) heisst diskreter Logarithmus. Die diskrete Logarithmus Funktion ist bis heute höchst aufwändig zu berechnen.

Aufgabe (Challenge) 1.6

Beweisen Sie, dass

$$S_{AB} = S_{BA}.$$

Lösungsvorschlag zu Aufgabe 1.6

Wir zeigen, dass

$$g^{a \cdot b} \mod p = (g^a \mod p)^b \mod p.$$

Aus der Defintion von

$$x = g^a \mod p$$

folgt

$$\exists m \in \mathbb{Z} : mp + x = g^a.$$

Somit ist

$$g^{ab} = (mp + x)^b \overset{(1)}{=} \sum_{k=0}^{b} \binom{b}{k} (mp)^k x^{b-k}.$$

(1) Hier haben binomischen Lehrsatz angewendet.
Der einzige Summand, der kein Vielfaches von p ist, ist x^b.

$$\begin{aligned} g^{a \cdot b} \mod p &= (mp + x)^b \mod p \\ &= \left(\sum_{k=0}^{b} \binom{b}{k} (mp)^k x^{b-k} \right) \mod p \\ &= x^b \mod p \\ &= (g^a \mod p)^b \mod p \end{aligned}$$

Daher folgt

$$\begin{aligned} S_{AB} &= (g^a \mod p)^b \mod p = g^{a \cdot b} \mod p \\ &= g^{b \cdot a} \mod p = (g^b \mod p)^a \mod p = S_B A. \end{aligned}$$

□

1.2 Lernziele Diffie-Hellman-Merkle

- ☐ Ich weiss, was das Schlüsselaustauschproblem ist.
- ☐ Ich weiss, wie das Diffie-Hellman-Merkle Protokoll einen Schlüsselaustausch implementiert.
- ☐ Ich kann für gegebene $g, p, a,$ und p den geheimen Schlüssel mittels des Diffie-Hellman-Merkle Protokolls berechnen.
- ☐ Ich kann erklären, warum Kommutativität für das Diffie-Hellman-Merkle Protokoll wichtig ist.