



Kantonsschule im Lee

Informatik

Kryptologie

Skript

Judith Beestermöller

© Winterthur, 27. Oktober 2025

Inhaltsverzeichnis

1	Schlüsselaustausch	2
1.1	Diffie-Hellman-Merkel-Schlüsselaustausch	2
1.2	Lernziele Diffie-Hellman-Merkel	6

Kapitel 1

Schlüsselaustausch

1.1 Diffie-Hellman-Merkel-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-Merkel 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 Merkel.

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 Merkel

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

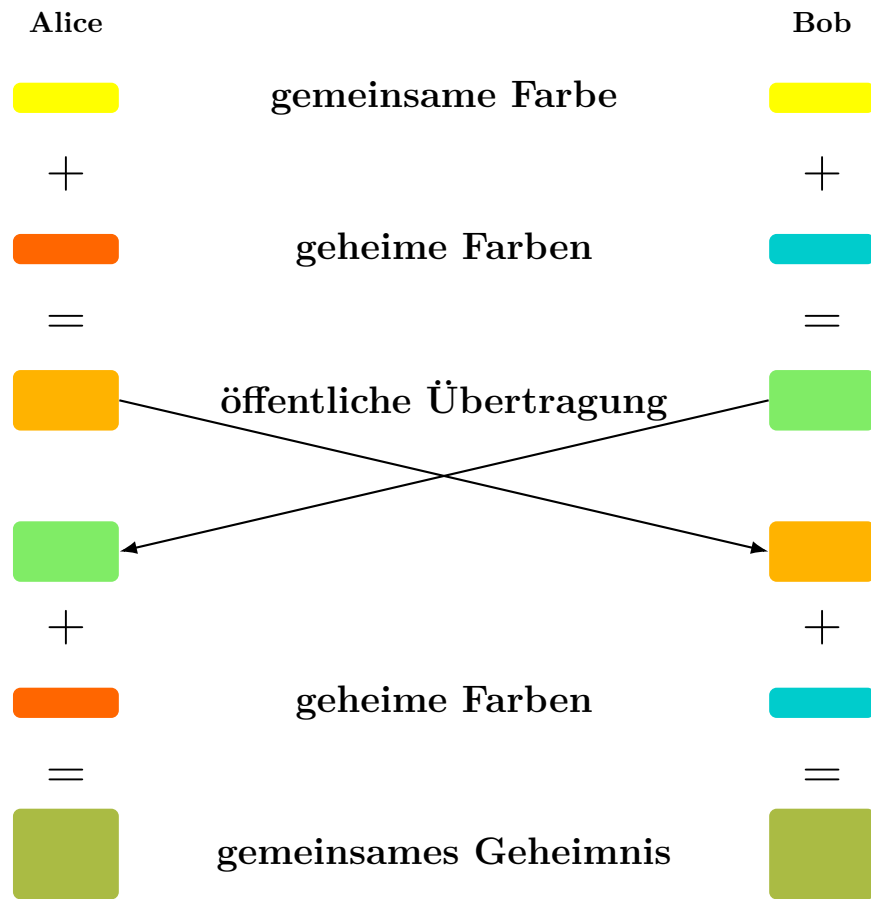


Abbildung 1.2: Dieses Schema zeigt eine Abstraktion, wie das Diffie-Hellmann-Merkel Protokoll funktioniert.

Abbildung 1.2 zeigt eine Abstraktion, wie das Diffie-Hellmann-Merkel Protokoll funktioniert. Zu Beginn einigen sich Alice und Bob auf eine Ausgangsfarbe. Diese ist nicht geheim. Zusätzlich 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?

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: 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?

 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?

Das eigentliche Diffie-Hellman-Merkel Protokoll verwendet keinen Farben, aber weist 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.

 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) $g = 5, p = 7, x = 6, y = 2$

Die Funktion $r = g^x \bmod p$ 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

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

1.2 Lernziele Diffie-Hellman-Merkel

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