

16 Deffie-Hellman

Peter Rutschmann

03.12.2025

Deffie-Hellman

Sichere Website-Verbindung

Wenn Sie die Verbindung zum Webserver öffnen, so handeln der Webserver und Ihr Browser automatisch einen Schlüssel für die sichere Verbindung aus. Sie sehen das in der Adresszeile des Browsers.

Wozu Deffie-Hellman dient.

Nehmen wir an, Alice und Bob möchten geheime Nachrichten austauschen. Doch da ist auch noch Eve, die alle Nachrichten mitlesen kann.

Alice und Bob müssen als Ihre Nachrichten verschlüsseln, damit Eve den Inhalt der Nachrichten nicht verstehen kann. Doch wie vereinbaren Alice und Bob einen gemeinsamen Schlüssel, ohne dass Eve diesen Schlüssel mitbekommt? Hier kommt das Deffie-Hellman Verfahren ins Spiel.

Das Grundprinzip von Deffie-Hellman

Der Diffie-Hellman-Schlüsselaustausch oder Diffie-Hellman-Merkle-Schlüsselaustausch (auch kurz DHM-Schlüsselaustausch oder DHM-Protokoll[1], ursprünglich $ax^{1 \times 2}$) ist ein Schlüsselaustauschprotokoll. Dieses 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. Der dadurch vereinbarte Schlüssel kann anschließend für ein symmetrisches Krypto System verwendet werden. Diffie-Hellman baut dabei auf die Exponentialfunktion in Kombination mit Modulo auf. Computer können mit dieser Formel y sehr schnell berechnen

Verstehen Sie nur Bahnhof?

Aufgabe Filme zu Diffie-Hellman

- Schauen Sie sich diesen Film aufmerksam an. <https://www.youtube.com/watch?v=3QnD2c4Xovk> oder Stichwort: *short version Diffie-Hellman key exchange*
 - Notieren Sie welche Schritte Alice und Bob mit den Farben machen.
 - Erklären Sie danach Ihrem Lernpartner das Verfahren mit den Farben aus dem Film.
-

Das Mathematische Verfahren von Diffie-Hellman

Diffie-Hellman baut auf die Exponentialfunktion in Kombination mit Modulo auf. Computer können anhand der Formel $y = b^x \mod m$ sehr schnell berechnen.

$$y = b^x \mod m$$

Der Ablauf Schritt um Schritt:

- 1) Schritt: Alice und Bob vereinbaren Werte für b und m .
 - $b=7$ und $m=17$.
 - b ist eine sogenannte Basiszahl.
 - m ist eine sogenannte Modulo Zahl.
 - Beide Zahlen müssen Primzahlen sein.
 - **Eve hört mit und kennt diese Zahlen auch.**
- 2) Alice bestimmt eine weitere beliebige Zahl
 - AliceSecretKey = 34
 - Alice berechnet nun mit der Formel $y = b^x \mod m$ ihren öffentlichen Schlüssel
 - * $y = 7^{34} \mod 17 = 15$
 - Alice sendet diesen öffentlichen Schlüssel (15) an Bob.
 - **Eve hört mit und kennt diesen Schlüssel 15 auch.**
- 3) Bob bestimmt auch eine weitere eigene Zahl, behält die aber für sich.
 - BobSecretKey = 19
 - Bob berechnet nun mit der Formel $y = b^x \mod m$ seinen öffentlichen Schlüssel
 - * $y = 7^{19} \mod 17 = 3$
 - Bob sendet diesen öffentlichen Schlüssel (3) an Alice.

- **Eve hört mit und kennt diesen Schlüssel 3 auch.**
- 4) Alice berechnet nun mit dem öffentlichen Schlüssel von Bob und ihrem geheimen Schlüssel den gemeinsamen geheimen Schlüssel.
 - $\text{GemeinsamerSchlüssel} = \text{BobPublicKey}^{\text{AliceSecretKey}} \bmod m$
 - $\text{GemeinsamerSchlüssel} = 3^{34} \bmod 17 = 9$
 - **Da Eve den AliceSecretKey nicht kennt, kann sie den Gemeinsamer-Schlüssel nicht berechnen.**
- 5) Bob berechnet nun mit dem öffentlichen Schlüssel von Alice und seinem geheimen Schlüssel den gemeinsamen geheimen Schlüssel.
 - $\text{GemeinsamerSchlüssel} = \text{AlicePublicKey}^{\text{BobSecretKey}} \bmod m$
 - $\text{GemeinsamerSchlüssel} = 15^{19} \bmod 17 = 9$
 - **Da Eve den BobSecretKey nicht kennt, kann sie den Gemeinsamer-Schlüssel nicht berechnen.**
- 6) Alice und Bob haben nun den gleichen gemeinsamen geheimen Schlüssel (9).
Doch Eve kennt diesen Schlüssel nicht.

Dies funktioniert deshalb, da mathematisch bewiesen werden kann dass:

- 7 Basiszahl
- 17 abgemachte Modulozahl
- 34 Alice secret key
- 15 Alice public key
- 19 Bob secret key
- 3 Bob public key
- 9 gemeinsamer geheimer Schlüssel

A) $\text{Basizahl}^{\text{AliceSecretKey}} \bmod \text{Modulozahl} = \text{AlicePublicKey} \quad 7^{34} \bmod 17 = 15$

B) $\text{Basizahl}^{\text{BobSecretKey}} \bmod \text{Modulozahl} = \text{BobPublicKey} \quad 7^{19} \bmod 17 = 3$

C) $\text{AlicePublicKey}^{\text{BobSecretKey}} \bmod \text{Modulozahl} = \text{geheimer Key} \quad 15^{19} \bmod 17 = 9$
Nun kombiniere ich die Schritte A) und C) für den Beweis: $(7^{34})^{19} \bmod 17 = 9$
 $7^{(34 \cdot 19)} \bmod 17 = 9$

D) $\text{BobPublicKey}^{\text{AliceSecretKey}} \bmod \text{Modulozahl} = \text{geheimer Key} \quad 3^{34} \bmod 17 = 9$ Nun kombiniere ich die Schritte B) und D) für den Beweis: $(7^{19})^{34} \bmod 17 = 9 \quad 7^{(19 \cdot 34)} \bmod 17 = 9$

Es ist das Gleiche: $7^{(34 \cdot 19)} \bmod 17 = 9 = 7^{(19 \cdot 34)} \bmod 17$