Simon Hauser, Manuel Sailer

Diffie-Hellman-(Merkle)-Schlüsselaustausch

1. Grundlagen

Definition:

Bei Diffie-Hellman handelt es sich um ein asymmetrisches, kryptografisches Schlüsselaustauschverfahren, welches von den Wissenschaftlern Whitfield Diffie und Martin Hellman entwickelt und veröffentlicht wurde (wichtige Vorarbeit von Ralph Merkle, deshalb oft auch Diffie-Hellman-Merkle-Schlüsselaustausch). Ziel dieses Verfahrens ist die Ermittlung eines gemeinsamen Sitzungsschlüssels, welcher zur Ver- und Entschlüsselung von Daten verwendet wird.

Besonderheit:

Bei herkömmlichen Schlüsselaustauschverfahren der modernen Kryptografie muss während der Aushandlung der Verschlüsselung der geheime Sitzungsschlüssel ebenfalls übertragen werden, da ansonsten die Ver- und Entschlüsselung der Daten nicht realisiert werden kann.

⇒ Angreifer können den Sitzungsschlüssel während der Übertragung ermitteln.

Die Besonderheit des Diffie-Hellman-Verfahrens ist, dass hier nicht wie bei anderen Schlüsselaustauschverfahren der geheimen Sitzungsschlüssel übertragen wird, sondern nur das Ergebnis einer Rechenoperation. Anhand dieses Ergebnisses berechnen sich die jeweiligen Kommunikationspartner den Sitzungsschlüssel, welcher zur Ver- und Entschlüsselung von Daten verwendet wird. (es handelt sich also eigentlich um ein Schlüsselaustauschverfahren)

Verwendung:

Das Diffie-Hellman-Schlüsselaustauschverfahren bildet die Grundlage für das Protokoll Secure Shell (SSH2, OpenSSH), IPSec und TLS mit Forward Secrecy / Perfect Forward Secrecy. Einsatz findet der Diffie-Hellman-Schlüsselaustausch vor allem beim Internetkommunikationsprotokoll HTTPS (HyperText Transfer Protocol Secure). Bei der Verschlüsselung von E-Mails kommt es nicht zum Einsatz, da eine Interaktion beider Kommunikationspartner vorausgesetzt wird. Dafür findet Diffie-Hellman aber bei der Transportverschlüsselung mit STARTTLS Anwendung.

2. Vorgehensweiße bei diesem Verfahren

Die Vorgehensweiße beim Diffie-Hellman-Schlüsselaustausch wird mit Hilfe von Bob und Alice veranschaulicht. Bob und Alice stehen für die Kommunikationspartner, welche mittels Diffie-Hellman eine geheimen Sitzungsschlüssel zur Ver- und Entschlüsselung der Daten ermitteln.

Schema:

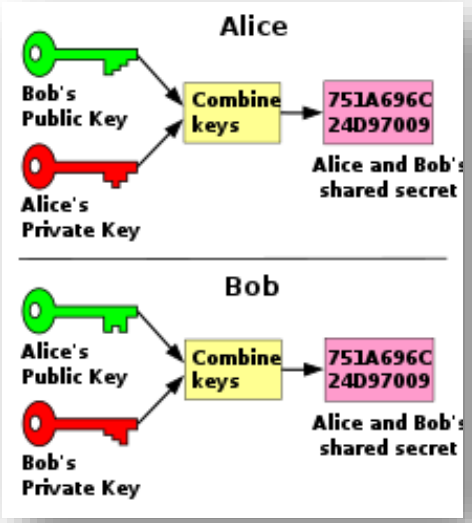

Abbildung 1
Source: Diffie-Hellman-Schlüsselaustausch – Wikipedia, 06.03.2022

Funktionsweiße:

1. Alice und Bob müssen sich auf eine Primzahl p und eine natürliche Zahl g einigen (in der Praxis vorgegeben). g sollte idealerweise ein Generator der zyklischen Gruppe Z_p sein, aber das Verfahren funktioniert auch, wenn g einen anderen Wert kleiner p annimmt. Beide Werte dürfen bekannt sein und können über einen unsicheren Kanal übertragen werden.
2. Im nächsten Schritt wählt Bob eine Zahl b und Alice eine Zahl a. Die gewählten Zahlen müssen jeweils kleiner sein als die Primzahl p (Intervall [1, p-1]). Bei diesen Zahlen handelt es sich um die **Private Keys.**
3. Anschließend führen sowohl Alice als auch Bob folgende Berechnung durch und ermitteln somit die jeweiligen **Public Keys**:

   Alice: **g^a modulo p = A**

   Bob: **g^b modulo p = B**

4. Nach der Berechnung werden die Public Keys (= Ergebnisse der Rechenoperation) zwischen Alice und Bob ausgetauscht
5. Im letzten Schritt führen Alice und Bob dieselbe Rechenoperation wie zuvor durch, allerdings mit dem übertragenen Public Key des jeweils anderen.

   Alice: **B^a modulo p = geheimer Sitzungsschlüssel**

   Bob: **A^b modulo p = geheimer Sitzungsschlüssel**

Die Ergebnisse dieser Rechenoperationen sind identisch und bildet somit den geheimen Sitzungsschlüssel, welcher in weiterer Folge in einem symmetrischen Verschlüsselungsverfahren zur Ver- und Entschlüsselung von Daten verwendet werden kann.

In der nachfolgenden Grafik wird das Diffie-Hellman-Schlüsselaustauschverfahren veranschaulicht.

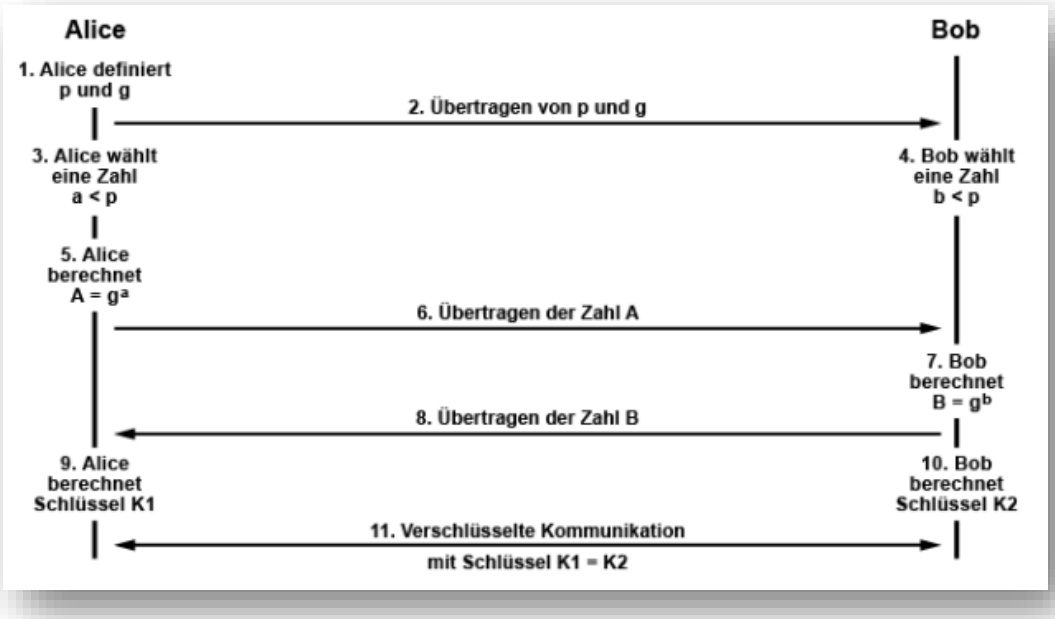

Abbildung 2

Source: Diffie-Hellman-Merkle-Schlüsselaustausch (elektronik-kompendium.de), 05.03.2022

Bsp. zu Diffie-Hellman:

1. Sowohl Alice als auch Bob wissen:

   p = 11, g = 7

2. Bob und Alice wählen eine Zahl (Private Keys):

   Alice: a = 3

   Bob: b = 6

3. Berechnung durchführen (Public Key):

   Alice: $A = 7^3$ modulo 11 = 2

   Bob: $B = 7^6$ modulo 11 = 4

4. Übertragung der Public Keys:

   Alice übertragt 2, Bob überträgt 4

5. Berechnung durchführen (geheimer Sitzungsschlüssel):

   Alice: 4^3 modulo 11 = **9**

   Bob: 2^6 modulo 11 = **9**

   ⇒ geheimer Sitzungsschlüssel

3. Sicherheit bei diesem Verfahren

Beim Diffie-Hellman-Schlüsselaustauschverfahren handelt es sich um ein diskretes Logarithmusverfahren. Die Sicherheit bei solchen Verfahren basiert auf der Tatsache, dass diskrete Exponentialfunktionen in gewissen zyklischen Gruppen eine Einwegfunktion bilden. Das bedeutet, dass in einer primen Restklassengruppe die diskrete Exponentialfunktion für große Exponenten effizient berechenbar ist, deren Umkehrung, der diskrete Logarithmus, jedoch nicht. Es gibt bestimmte Algorithmen zu Berechnung des diskreten Logarithmus, aber je größer die Parameter werden, desto unmöglicher wird die Berechnung

⇨ hohe Sicherheit

Problem:

Das Diffie-Hellman-Verfahren hat von mathematischer Sicht her eine hohe Sicherheit, es hat allerdings einen Schwachpunkt. **Man-in-the-Middle-Attacken**. Wenn es einem Angreifer gelingt, sich zwischen die beiden Kommunikationspartner zu schalten, dann ist das gesamte Schlüsselaustauschverfahren unbrauchbar und der Angreifer kann die verschlüsselten Daten abfangen, verändern und weiterleiten.

Man-in-the-Middle-Attacke:

Bei einer Man-in-the-Middle-Attacke fängt ein Angreifer die gesendeten Nachrichten der Kommunikationspartner ab und ersetzt deren Daten durch andere Daten. Will also z.B. ein Kommunikationspartner den berechneten Public Key übertragen, fängt der Angreifer diesen ab, ermittelt selbst einen anderen Public Key und leitet den falschen Public Key an den anderen Kommunikationspartner weiter. Somit erfolgt die Schlüsselvereinbarung nicht zwischen den Kommunikationspartnern, sondern jeweils zwischen einem Kommunikationspartner und dem Angreifer. Die gesamte Kommunikation erfolgt also somit über den Angreifer.

Nachfolgende Grafik veranschaulicht einen Man-in-the-Middle-Angriff:

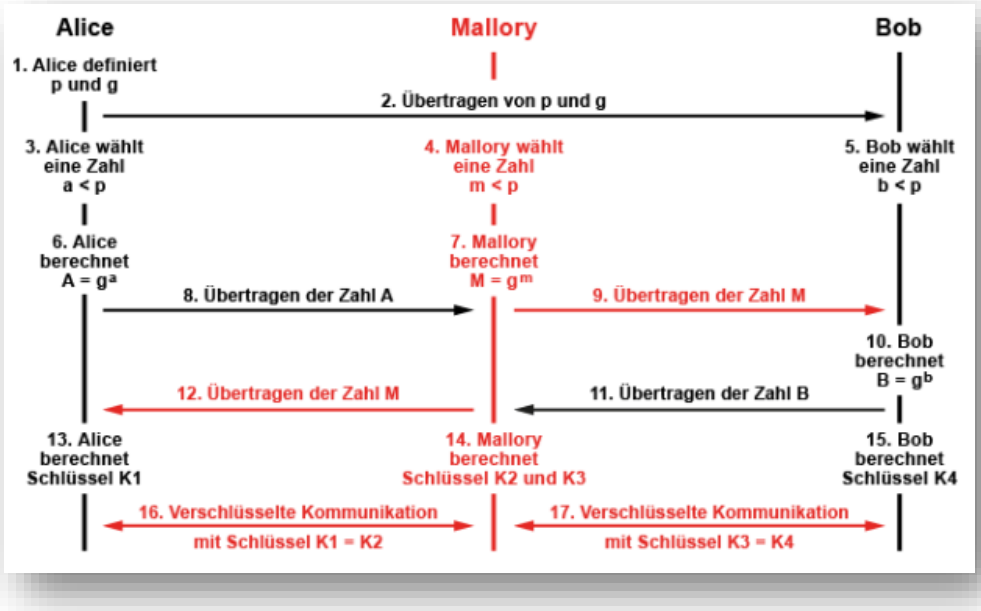

Abbildung 3

Source: Diffie-Hellman-Merkle-Schlüsselaustausch (elektronik-kompendium.de), 05.03.2022

Lösung dieses Problems:

Damit Man-in-the-Middle-Angriffe ausgeschlossen werden können, müssen die ausgetauschten Nachtrichten bei einer externen Authentifizierungsstelle verifiziert werden. Hierfür benötigt man ein funktionierendes und vertrauenswürdiges Authentifizierungsverfahren mit digitalen Signaturen (RSA) und Message Authentication Codes.

4. Mathematischer Hintergrund

Einwegfunktion:

Einwegfunktionen sind mathematische Funktionen, welche komplexitätstheoretisch leicht berechenbar sind, deren Umkehrung allerdings nicht.

Diskrete Exponentialfunktion:

Berechnung:

b^x modulo m

Eine diskrete Exponentialfunktion liefert den Rest bei der Division von b^x durch m. Die Umkehrfunktion der diskreten Exponentialfunktion ist der diskrete Logarithmus. Die diskrete Exponentialfunktion ist für sehr große Exponenten effizient berechenbar, der diskrete Logarithmus allerdings nicht --> diskrete Exponentialfunktion ist eine Einwegfunktion

Gruppentheorie:

Eine Gruppe ist ein Paar (G,*), bestehend aus einer Menge G und einer assoziativen Verknüpfung * auf G, die ein neutrales Element hat und für die jedes Element von G ein inverses Element besitzt. Wenn für eine Gruppe zusätzlich das Kommutativgesetz gilt, spricht man von einer abelschen Gruppe. Eine Untergruppe (U,*) einer Gruppe (G,*) ist eine Teilmenge U von G, die bezüglich der Verknüpfung * selbst wieder eine Gruppe ist.

Beispielsweise bildet die Menge der ganzen Zahlen mit der Addition als Verknüpfung die (abelsche) Gruppe (Z, +)

Prime Restklassengruppe und Primitivwurzel:

Die prime Restklassengruppe ist die Gruppe der primen Restklassen bezüglich eines Moduls n. Sie wird als Z_n^* oder $(Z/nZ)^x$ notiert. Die primen Restklassen sind genau die multiplikativ invertierbaren Restklassen und sind daher endliche abelsche Gruppen bezüglich der Multiplikation.

Diffie-Hellman:

In der Kryptographie sind vor allem jene Zahlen n von Interesse, für die alle Zahlen zwischen 1 und n-1 ein inverses Element modulo n haben. Dies ist genau dann der Fall, wenn n eine

Primzahl ist (deshalb p statt n). Die Zahlen zwischen 1 und p-1 bilden also zusammen mit der Modulo-Multiplikation die Gruppe Z_p^*.

Eine weitere Aussage, die sich beweisen lässt:

Nimmt man ein beliebiges Element a aus Z_p^* und betrachtet die Menge $\{a, a^2, a^3, ...a^{p-1}\}$, dann erhält man eine Untergruppe (mit a als Generator der Untergruppe). Jede Untergruppe von Z_p^* hat mindestens einen Generator, und damit auch Z_p^* selbst. Die Gruppe Z_p^* ist also zyklisch.

Eine zyklische Gruppe ist also eine Gruppe, deren Elemente als Potenz eines ihrer Elemente dargestellt werden können.

Beispiel: Z_{13}^* ist eine zyklische Gruppe mit 2 als Generator, denn jede Zahl von 1 bis 12 lässt sich als Potenz von 2 darstellen

$1 = 2^{12}$ modulo 13

$2 = 2^1$ modulo 13

$3 = 2^4$ modulo 13

$4 = 2^2$ modulo 13

$5 = 2^9$ modulo 13

$6 = 2^5$ modulo 13

...

$12 = 2^6$ modulo 13

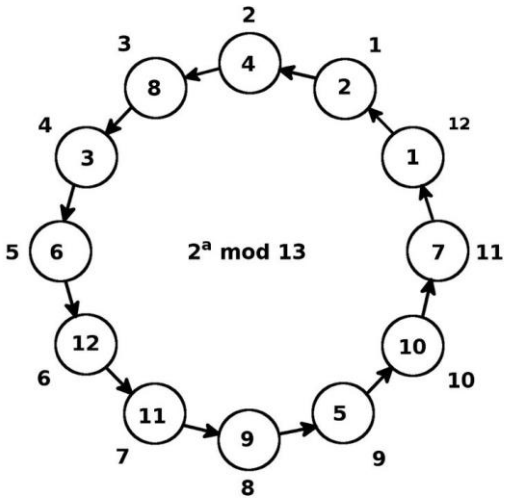

Abbildung 4
Source: Diffie-Hellman-Schlüsselaustausch – Wikipedia, 06.03.2022

Es lässt sich nun leicht nachvollziehen, dass die Gleichung $a^x = b$ modulo p immer lösbar ist, wenn a ein Generator von Z_p^* ist, wobei dann b ein Element Z_p^* ist (außer 0). Der diskrete Logarithmus existiert also in Z_p^* immer dann, wenn die Basis ein Generator von Z_p^* ist. Stellt man die Zahlen in einem Kreis (Zyklus) der Potenzen dar, scheinen sie willkürlich verteilt zu sein. Dies gibt zumindest eine Vorstellung davon, weshalb der diskrete Logarithmus so aufwändig (bzw. fast unmöglich) zu bestimmen ist.

Literaturverzeichnis:

Diffie-Hellman-Merkle-Schlüsselaustausch (elektronik-kompendium.de), 05.03.2022

Diffie-Hellman-Schlüsselaustausch – Wikipedia, 06.03.2022