Fachhochschule Wedel
Seminararbeit

Fachrichtung
Wirtschaftsingenieurwesen

Der Diffie-Hellman-Schlüsselaustausch und das elGamal-Verfahren

Erstellt von:	Carolin Engel (Mat-Nr. 101193) wing101193@fh-wedel.de
Erarbeitet im	6. Semester
Abgegeben am:	24. Mai 2017
Betreuender Dozent:	Prof. Dr. Michael Anders Fachhochschule Wedel Feldstraße 140 22880 Wedel Tel. (04103) 804824 E-Mail: an@fh-wedel.de

Inhaltsverzeichnis

Abkürzungsverzeichnis

DH-Schlüsselaustausch	Diffie-Hellman-Schlüsselaustausch
GCHQ	Government Communications Headquarters
MitM-Angriff	Man-in-the-middle-Angriff
CDH	Computational-Diffie-Hellman-Problem
DDH	Decisional-Diffie-Hellman-Problem

1 Einleitung

In der heutigen Zeit, in der immer mehr Daten durch das Internet verschickt und empfangen werden, wird die Verschlüsselungstechnik immer wichtiger. Neben der Menge der ganzen Daten hat auch die Sensibilität dieser zugenommen. Persönliche Fotos sowie Video-, Sprach- oder Textnachrichten, Bankverbindungsdaten, politische Meinung bis hin zum Kaufverhalten wird alles ungeschützt im Internet preisgegeben. Um einen Zugriff durch Dritte zu vermeiden, ist es wichtig seine Daten zu schützen. Es kann auf alternative Nachrichtenkanäle gewechselt werden, jedoch besteht auch hier die Möglichkeit, dass die Daten abgefangen oder weitergeleitet werden können.

Eine deutlich bessere Lösung ist die Verschlüsselung der eigenen Daten und den passenden Schlüssel nur wenigen autorisierten Personen zur Verfügung zu stellen.

Durch eine Verschlüsselung werden unsere Daten geschützt, wenn sie durch das Internet geschickt werden und schützen so unsere Privatsphäre. Lange Zeit war eine starke Verschlüsselung den Regierungen vorbehalten, doch heute kann sie jeder Anwender nutzen. Auch wenn viele sagen, sie haben keine Geheimnisse und so auch nichts zu verbergen, was von Interesse sei, im Grunde meinen sie nur, dass sie nicht glauben, dass sich jemand die Mühe macht und auf seinem Laptop nach etwas Wertvollem zu suchen.[1]

Diese Arbeit wird sich mit dem Diffie-Hellmann Schlüsselaustausch (DH-Schlüsselaustausch) und elGamal-Verfahren als Möglichkeiten zur Verschlüsselung befassen.

[1] (CryptoCD, 2017)

2 Grundlagen zur Verschlüsselung

Bei der Verschlüsslung, auch Chiffrierung genannt, werden Informationen umgewandelt, damit sie nicht von Unautorisierten gelesen werden können. Durch das Verschlüsseln wird ein Klartext in einen Geheimtext umgeformt, der durch Entschlüsseln wieder in den ursprünglichen Klartext überführt werden kann. In der Regel wird für das Verschlüsseln bzw. Entschlüsseln ein Schlüssel genutzt. So kann ein Dritter den verschlüsselten Text nicht lesen, solange er den benötigten Schlüssel nicht besitzt. Für den Moment kann er nur versuchen den unverständlichen Text zu entziffern.

Es gibt viele verschiedene Ver-/Entschlüsselungsmethoden. Sie reichen bis in das Römische Reich zurück, in dem die Herren ihren Sklaven Nachrichten auf den rasierten Kopf tätowieren und warteten bis deren Haare wieder nachgewachsen waren, damit nur der richtige Empfänger die Nachricht lesen sollte.

Der eigentliche Algorithmus ist nicht das Wichtigste, um die Sicherheit gewährleisten zu können. Das Wichtigste ist, den Schlüssel geheim zu halten, sodass nur vertrauenswürdige Teilnehmer ihn kennen. Wie in dem Fall mit den Römern: Wenn außenstehende Wissen, dass der Schlüssel ein Rasierer ist, ist die Nachricht leicht zu bekommen.[2]

Die Verschlüsselungsverfahren werden in symmetrische und asymmetrische Kryptosysteme eingeteilt.

Symmetrischen Verschlüsselungen sind Systeme, bei denen beide Kommunikationspartner den gleichen Schlüssel verwenden. Wie in dem Beispiel mit den Römern, der Rasierer ein Schlüssel wäre um an die Nachricht zu gelangen. [3]

In der digitalen Welt sind Schlüssel meistens nur noch aneinander gereihte Ziffern. Nachteil dieses Verfahrens ist, dass ein Schlüssel vorher über einen sicheren Kanal oder persönlich ausgetauscht werden muss. Dafür hat dieses Verfahren eine die hohe Geschwindigkeit.

Erst seit den 1970er Jahren sind asymmetrische Schlüsselaustauschprotokolle bekannt. In diesem kryptografischen Verfahren benötigen die Teilnehmer nicht mehr einen gemeinsamen geheimen Schlüssel. Jeder Teilnehmer besitzt einen öffentlichen Schlüssel und einen privaten Schlüssel. Mit dem öffentlichen Schlüssel kann jeder Teilnehmer einen Klartext in einen Geheimtext chiffrieren und nur die Person, die die Nachricht erhalten soll, kann den Geheimtext mit seinem privaten Schlüssel wieder in einen Klartext umwandeln.

[2] (Malenkovich, 2013)
[3] (Cvrk, kein Datum)

Dieses Verfahren dauert aufgrund seines aufwändigeren Verfahren deutlich länger, als symmetrische Verschlüsslungsverfahren.

Der Diffie-Hellman-Schlüsselaustausch (DH-Schlüsselaustausch) ist ein asymmetrisches Verfahren, wird aber auch für symmetrische Verschlüsselungsverfahren genutzt. Er kann genutzt werden um über eine öffentliche und abhörbare Leitung einen gemeinsamen geheimen Schlüssel in Form einer Zahl vereinbaren zu können, ohne dass ein Dritter diese Zahl berechnen kann. Dieser Schlüssel kann danach in einem symmetrischen Kryptosystem genutzt werden.

Allerdings hat der DH-Schlüsselaustausch eine größere Bedeutung als erstes asymmetrischen Kryptoverfahren, die auch Public-Key-Verschlüsslungsverfahren genannt werden. [4]

Das elGamal-Verschlüsselungsverfahren ist ebenfalls ein Public-Key-Verschlüsslungsverfahren. Es baut auf der Idee des DH-Schlüsselaustausches auf. Es ist ein weiter entwickeltes Kryptosystem, dass nicht nur einen Schlüssel austauschen kann, sondern auch Nachrichten verschlüsseln kann.

[4] (Cvrk, kein Datum)

3 Diffie-Hellman-Schlüsselaustausch

Das Kerckhoffs‘ Prinzip besagt, dass der Verschlüsselungsalgorithmus nicht geheim gehalten werden muss, sondern nur der Schlüssel. Aber wie wird ein Schlüssel ausgetauscht bevor man eine sichere Leitung hat und auch nicht den Schlüssel persönlich überbringen kann? Mit dieser Problematik beschäftigt sich der DH-Schlüsselaustausch. [5]

3.1 Entstehung

Der DH-Schlüsselaustausch wurde von Whitfield Diffie und Martin Hellman mit der Forschungsarbeit „New Directions in Cryptography“ im Jahre 1976 veröffentlicht. Die Grundlagen leistete Ralph Merkle mit dem nach ihm benannten Merkle Puzzle. Deswegen wird dieses Verfahren auch Diffie-Hellman-Merkle-Schlüsselaustausch genannt.

Mit dieser Forschungsarbeit wurde das erste asymmetrische Kryptoverfahren entwickelt. In der Anfangsphase wurde der DH-Schlüsselaustausch noch ax1x2 genannt. Später stellte sich heraus, dass Mitarbeiter des britischen Government Communications Headquarters (GCHQ) bereits 1974 an einem asymmetrischen Kryptosystem forschten. Das GCHQ hat allerdings auf Grund der Geheimhaltung und des aus der Sicht der Briten wegen fraglichen Nutzens kein Patent angemeldet.

Mit diesem Verschlüsselungsverfahren prägten Whitfield Diffie und Martin Hellman einen neuen Sicherheitsbegriff in der Kryptographie, da noch kein effizienter Algorithmus, um dieses Verfahren zu entschlüsseln, existiert.

3.2 Funktionsweise

Der DH-Schlüsselaustausch basiert auf dem diskreten Logarithmus. Das bedeutet, dass die diskrete Exponentialfunktion eine Einwegfunktion ist. Die diskrete Exponentialfunktion $b^x mod\ m$ ist auch für große Exponenten effizient berechenbar, aber nicht ihre Umkehrung mit dem diskreten Logarithmus.

Zur Veranschaulichung wird die Funktionsweise des Verfahrens an Hand von Farben in Abbildung 1 dargestellt.[6] Alice und Bob sind die beiden Kommunikationspartner und wollen eine gemeinsame geheime Farbe mischen, ohne dass es ein Außenstehender nachmischen kann. Dabei helfen zwei einfache Grundsätze:

- Es ist einfach eine Farbe mit zwei Farben zu mischen
- Es ist praktisch unmöglichen die gemischte Farbe wieder in ihre zwei ursprünglichen Farben zu entmischen.

[5] (mk, 2012)
[6] (Vinck, 2012)

Die Startfarbe auf die sich Alice und Bob geeinigt haben, wird öffentlich bekannt gegeben. In diesem Beispiel ist es gelb. Diese Farbe kann abgefangen werden, aber die Information hilft Dritten nicht, die geheimen Farben zu finden.

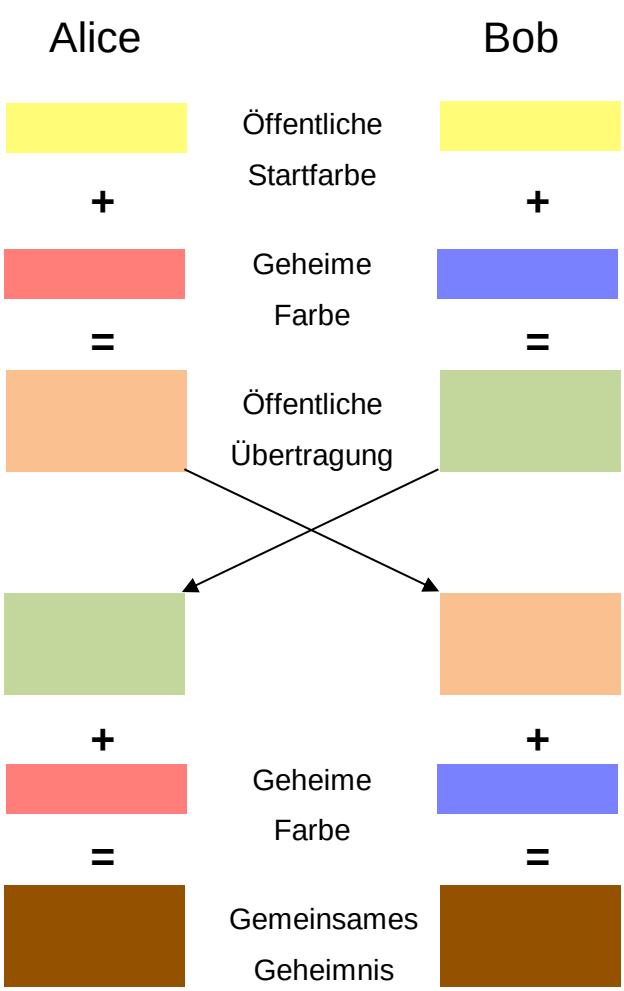

Abbildung 1: Kommunikation beim DH-Schlüsselaustausch mit Farben

Ein Dritter kann nur durch ausprobieren dieses bestimmte Grün erlangen, indem er verschiedene Blau-Töne mit dem öffentlichen Gelb mischt. Es ist aber nicht möglich diese Farbe zu entmischen und dadurch das exakte Blau zu erhalten. Dieses Phänomen nennt man Einwegfunktion Eine solche Funktion kann in einer Rückwärtsbetrachtung nur durch Trial-and-Error gelöst werden.

Zu der öffentlichen Startfarbe suchen sich Alice und Bob jeweils eine geheime Farbe aus, die auf gar keinen Fall öffentlich werden darf. Auch der andere Teilnehmer kennt diese Farbe nicht. Es wird lediglich die gemischte Farbe, also in Bobs Fall das gemischte Grün bzw. bei Alice das Orange, übermittelt. Diese Farbe kann wieder abgefangen werden.

Zu den ausgetauschten gemischten Farben fügen beide Teilnehmer ihre eigene geheime Farbe hinzu. So erhalten beide das exakt das gleiche Braun. Es wird deutlich, dass die Reihenfolge in der die drei Farben gemischt werden irrelevant ist. Am Ende haben beide dieselbe Farbe und so ein gemeinsames Geheimnis. So kann ein Schlüssel ausgetauscht werden. Angreifer erhalten zwar Teilinformationen über die Farben und wissen möglicherweise auch, dass die Farben gemischt sind, kennen also das Verfahren, aber können den Schlüssel trotzdem nicht erhalten. Denn selbst wenn die Startfarbe Gelb bekannt ist und auch das gemischte Orange, lässt sich das rot nicht genau bestimmen. In diesem Farbbeispiel lassen sich die einzelnen Komponenten relativ leicht durchs ausprobieren herausfinden, aber die Funktion zu mischen lässt sich nicht rückgängig machen.

Zur Anwendung von diesem Verschlüsselungsverfahren wird eine mathematische Funktion benötigt. Geeignet ist hierfür die Funktion Modulo, die den Rest einer Division berechnet. Ähnlich wie bei den Farben ist die eine Richtung leicht zu lösen, wie das Mischen der Farben. Der umgekehrte Weg ist nicht zu lösen, da sie nicht eindeutig definiert ist.

Zum Beispiel: 32 mod 5 = 2

Wenn die Zahlen 5 und 2 aus der Gleichung gegeben sind, lässt sich unmöglich eindeutig auf die Zahl 32 schließen. Die Zahlen {2, 7, 12, 17, 22, 27, …} wären genauso möglich um die Gleichung zu lösen.

Um den DH-Schlüsselaustausch anzuwenden einigen sich beide Kommunikationspartner auf eine Primzahl *p* (zum Beispiel 17), die im Beispiel der Farben Gelb entspricht. Primzahlen sind von besonderem Interesse, da sie zwischen 1 und n-1 ein inverses Element Modulo n haben.

Zusätzlich wird ein Generator *g* festgelegt (zum Beispiel *g* = 3). Ein Generator *g* von der Zahl *p* ist eine Zahl, die folgende Bedingung erfüllt.

$$g^i \bmod p = \{1, 2, \ldots, p\text{-}1\} \text{ mit } i = \{1, 2, \ldots, p\text{-}1\}$$

Wenn in die Formel $g^i \bmod p$ die obigen Zahlen ($p = 17$ und $g = 3$) eingesetzt werden ergeben sich die in der Tabelle abgebildeten Werte. Zum Vergleich wurde die Rechnung zusätzlich mit dem Generator $g = 4$ durchgeführt. Mit g = 4 ergeben sich die vier Werte {1; 4; 13; 16}. Bei g = 3 ergeben sich deutlich mehr Möglichkeiten mit den Werten {1, 2, 3, ..., 16}. Das liegt daran, dass *g* = 3 nicht nur ein Generator ist, sondern auch eine sogenannte Primitivwurzel. Primitivwurzeln haben die besondere Eigenschaft, dass sie jedes Element der zyklischen Gruppe als Potenz darstellen können.[7]

i	mit g = 3	mit g = 4
0	1	1
1	3	4
2	9	16
3	10	13
4	13	1
5	5	4
6	15	16
7	11	13
8	16	1
9	14	4
10	8	16
11	7	13
12	4	1
13	12	4
14	2	16
15	6	13
16	1	1

Abbildung 2: Zyklische Gruppe mit Besonderheit von Primitivwurzeln

Wenn Alice und Bob einen Schlüssel mit dem DH-Schlüsselaustausch bestimmen wollen, legt Alice eine Primzahl *p* fest und generiert sich daraus eine Primitivwurzel. Im Beispiel p = 17 und g = 3.

[7] (Morpheus, 2016)

Nun wählt Alice ein *a* zufällig aus dem Bereich {1, 2, …, p-1} aus (zum Beispiel 15) und berechnet mit folgender Formel ihr *A*, dass sie an Bob sendet. Das A entspricht dem Orange in dem Farbbeispiel.

$$A = g^a \bmod p$$

Im Beispiel: $3^{15} \bmod 17 = 6$

Zusätzlich zu *A = 6* versendet Alice auch die Informationen *p = 17* und *g* = 3 an Bob. Alle diese drei Zahlen können von Außenstehenden abgefangen werden, da sie über eine öffentliche Leitung und damit unverschlüsselt an Bob gesendet werden.

Bob überlegt sich ebenfalls eine geheime Zahl *b* aus dem Bereich {1, 2, …, p-1} (zum Beispiel 13) und berechnet mit den von Alice erhaltenen Werten sein *B* durch folgende Formel.

$$B = g^b \bmod p$$

Im Beispiel: $3^{13} \bmod 17 = 12$

Sein berechnetes B=12 sendet er zurück an Alice. Alice und Bob haben jetzt beide alle Werte, die benötigt werden, für die Berechnung des Schlüssels.

Alice berechnet den Schlüssel *K* wie folgt:

$$K = B^a \bmod p$$

Im Beispiel: $12^{15} \bmod 17 = 10$

Bob berechnet den Schlüssel K mit folgender Formel:

$$K = A^b \bmod p$$

Im Beispiel: $6^{13} \bmod 17 = 10$

Die rechts stehende Grafik zeigt welche Zahlen nur ausgetauscht werden und wie ein gemeinsamer Schlüssel errechnet werden kann.

Alice und Bob erhalten die gleiche Zahl bzw. den gewünschten geheimen Schlüssel. Letztendlich haben die beiden ihren Schlüssel über die gleiche

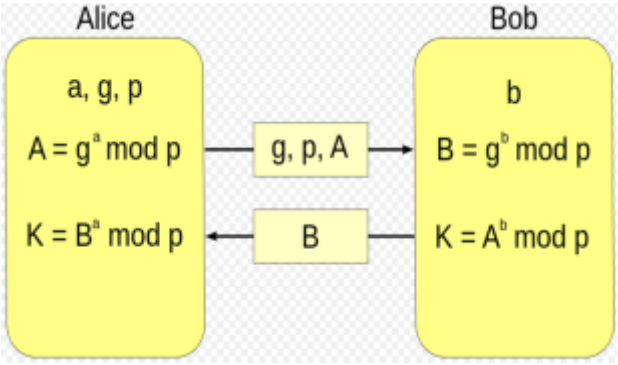

Abbildung 2: Kommunikation beim DH-Schlüsselaustausch

Gleichung berechnet.[8] Zur Berechnung des Schlüssels war die Reihenfolge der mathematischen Schritte irrelevant, ebenso wie bei dem Farbbeispiel. Wenn in die beiden verschiedenen Berechnungen des Schlüssels die Formeln für B und A eingesetzt werden ergeben sich folgende Gleichungen.

$$K = (g^b \bmod p)^a \bmod p = g^{ba} \bmod p$$

$$K = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

Es wird deutlich, dass Alice und Bob die gleiche Rechnung durchgeführt haben. Lediglich in der Reihenfolge der Rechenschritte unterscheiden sie sich.[9] Für die Praxis verwendet man heutzutage Primzahlen mit mehreren hundert Stellen, da bei kleineren Zahlen wie den Beispielzahlen die erstellten Schlüssel zu schnell zu knacken sind. Auch kann eine sogenannte Sophie-Germain-Primzahlen verwendet werden. Eine Primzahl *p* nennt man Sophie-Germain-Primzahl, wenn auch 2p + 1 eine Primzahl ist. Dann wird sie als „sichere Primzahl“ betrachtet. Zum Beispiel ist p = 2 eine Sophie-Germain-Primzahl, da 2p + 1 = 5.[10]

3.3 Verwendung mit mehr als zwei Teilnehmern

Es ist auch möglich einen Schlüssel mit mehr als nur zwei Kommunikationspartnern auszutauschen mit dem DH-Schlüsselaustausch zu nutzen. Im Folgenden Beispiel findet ein Schlüsselaustausch zwischen drei Teilnehmern statt: Alice, Bob und Claus.

Es wird wieder eine zyklische Gruppe als Primzahl *p* festgelegt und die dazugehörige Primitivwurzel *g* generiert. Zusätzlich überlegt sich jeder Teilnehmer eine geheime Zahl *a*, *b* und *c*. Alice berechnet nun wie zuvor ihr *A* und sendet ihr *A* an Bob. Dieser fügt dem *A* seine geheime Zahl *b* an und sendet den daraus resultierenden Wert *B* an Claus. Claus muss diesem Wert noch seine geheime Zahl *c* hinzufügen und erhält so den gehmeinen gemeinsamen Schlüssel.

$$K_C = g^{abc} \bmod p$$

Dies erfolgt ebenso für Alice und Bob, die damit folgende Berechnung erhalten.

$$K_A = g^{bca} \bmod p$$

$$K_B = g^{cab} \bmod p$$

[8] (Cruise, 2012) (Anon., kein Datum)
[9] (Schmeh, 2016)
[10] (Weisstein, Kein Datum)

Es können beliebig viele Teilnehmer an einem DH-Schlüsselaustausch teilnehmen. Bei großen Gruppen wird die in Runden durchgeführte Schlüsselerstellung sehr aufwendig und dauert viel länger. Es bietet sich an große Gruppen in kleinere Gruppen zu unterteilen, die unter sich einen Schlüssel bilden. Die Gruppen tauschen dann ihre Schlüssel aus und bilden damit einen für alle gültigen Schlüssel. So kann die Durchlaufzeit der Schlüsselerstellung deutlich reduziert werden. [11]

[11] (Hellman, 1976)

4 elGamal-Verschlüsselungsverfahren

Da das elGamal-Verschlüsselungsverfahren ein asymmetrisches Kryptosystem ist, wird ein öffentlicher und ein privater Schlüssel benötigt. Mit Hilfe des öffentlichen Schlüssels wird für eine bestimmte Person verschlüsselt und mit dem privaten Schlüssel kann diese Person dann den Geheimtext in einen Klartext entschlüsseln.

4.1 Entstehung

Das elGamal-Verschlüsselungsverfahren oder auch elGamal-Kryptosystem wurde im Jahre 1985 vom Kryptologen Taher Elgamal entwickelt und gehört zu den Public-Key-Verschlüsslungsverfahren. Er beschrieb es in seinem Aufsatz "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms." Es basiert auf dem DH-Schlüsselaustausch. Dieses Verfahren erreichte nie eine ähnlich starke Verbreitung wie das DH-Verfahren. Da es aber keinem Patent unterliegt ist es besonders in Open-Source-Projekten, wie zum Beispiel GnuPG (GNU Privacy Guard), beliebt.

Hauptsächlich unterscheiden sich der DH-Schlüsselaustausch und das elGamal-Verfahren in einer Änderung des Protokolls. Damit ist es nicht nur möglich einen Schlüssel auszutauschen, sondern auch Nachrichten verschlüsselt zu verschicken.

Eine Person erstellt einen öffentlichen Schlüssel, der von einer zweiten Person zum Verschlüsseln benötigt wird. Die erste Person kann die erhaltene verschlüsselte Nachricht durch eine Funktion mit dem eigenen privaten Schlüssel entschlüsseln. Dadurch kann das Verfahren gegenüber dem DH-Schlüsselaustausch die Durchlaufzeit verkürzen.

4.2 Funktionsweise

Beim elGamal-Verschlüsselungsverfahren ist der Anfang des Austausches sehr ähnlich, wie bei dem DH-Schlüsselaustausch.

Bob möchte Alice eine verschlüsselte Nachricht senden. Dazu muss Alice vorher sich einen öffentlichen Schlüssel erstellen.

Alice wählt sich eine große Primzahl *p* (optimaler Weise eine Sophie-Germain-Primzahl). Zur Vereinfachung wird in diesem Beispiel eine niedrige Primzahl gewählt. *p* = 23 ist aber trotzdem eine Sophie-Germain-Primzahl. Zusätzlich generiert sich Alice eine Primitivwurzel *g* = 7 und eine geheime Zahl a = 6, die die Bedingung a $\in$ {2, ..., p-2} erfüllen muss und später als Exponent fungiert. Mit diesen drei Zahlen errechnet sich Alice ihr A = 4, wie in dem DH-Schlüsselaustausch. Die Parameter *p* und *g* werden zusammen mit dem öffentlichen Schlüssel A an Bob unverschlüsselt gesendet oder sind frei zugänglich für Bob, zum Beispiel

auf Alice Homepage. Der Sender benötigt diese Daten um Alice eine Nachricht verschlüsselt zu übermitteln zu können.

Wenn Bob nun eine verschlüsselte Nachricht an Alice versenden möchte, muss dieser sich eine geheime Zahl b aussuchen. Wieder mit der Bedingung b ∈ {2, ..., p-2}, wie zum Beispiel b = 3. Mit dieser Zahl und dem öffentlichen Schlüssel von Alice berechnet sich sein B = 12, wie auch schon im DH-Schlüsselaustausch. Zusätzlich berechnet Bob jetzt noch ein *c* aus dem Klartext *m*. Der Klartext *m* muss zuvor in Zahlen kodiert werden, um ihn verschlüsselt verschicken zu können. Zu beachten ist, dass *m* kleiner als *p* sein muss. Wenn das nicht der Fall ist, muss die Nachricht *m* in mehrere Nachrichten aufgeteilt werden. In diesem Beispiel ist die zu übermittelnde Nachricht *m* = 7. Mit der folgenden Formel berechnet sich der Sender das Chiffrat *c*:

$$c = A^b * m \bmod p$$

Im Beispiel: $c = 4^3 * 7 \bmod 23 = 11$

So hat Bob den Klartext *m* mit dem Schlüssel A^b verschlüsselt. $B = 21$ und $c = 11$ sind zusammen der Schlüsseltext, der an Alice über seine öffentliche Leitung versendet wird.[12] Nun muss Alice nicht erst einen geheimen Schlüssel K, wie zuvor beim DH-Schlüsselaustausch errechnen, sondern kann direkt die Nachricht entschlüsseln.

Aus den Daten *c*, *B*, *A*, *a*, *p*, und *g* lässt sich das inverse *K* berechnen, das multipliziert mit der verschlüsselten Nachricht *c* modulo *p* den Klartext ergibt:

$$B^{p-1-a}\, c \bmod p = m$$

Im Beispiel: $21^{23-1-6} * 11 \bmod 23 = 7$

Einem Außenstehenden wäre das a nicht bekannt, er müsste den Umweg über den diskreten Logarithmus lösen, um von A auf a schließen zu können und obige Formel anwenden zu können.

Der Beweis dieser Formel erfolgt durch Umformen und Anwenden des kleinen Satz von Fermat.[13] Der kleine Satz von Fermat besagt, dass eine beliebige Zahl *d* hoch die Primitivwurzel *p* minus 1 geteilt durch die Primitivwurzel immer einen Rest von 1 ergibt. Unter der Bedingung, dass *d* kein Vielfaches von *p* ist gilt die Formel:

$$d^{p-1} \bmod p = 1$$

[12] (Kreitz, 2007)
[13] (Brünner, 2003)

Ausgehend von der bereits genannten Entschlüsselungsformel wird wie folgt umgeformt und der kleine Satz von Fermat angewendet.

$$m = B^{p-1-a}\, c \bmod p$$

$$= (g^{b} \bmod p)^{p-1-a}\, c \bmod p$$

$$= g^{b\,*\,(p-1-a)}\, c \bmod p$$

$$= g^{b*(p-1)} * g^{-ab} * c \bmod p$$

$$= g^{b*(p-1)} * g^{-ab} * g^{ab} * m \bmod p$$

$$= B^{p-1} * m \bmod p$$

$$= m \bmod p$$

$$= m$$

Wie im letzten Rechenschritt ersichtlich funktioniert diese Rechnung nur für *m* kleiner *p*. Wenn Nachrichten verschickt werden sollen, die *p* übersteigen, dann müssen diese in einzelne kleinere Nachrichten getrennt werden und können dann erst verschlüsselt und versendet werden. [14]

Alice kann durch das Wissen der geheimen Zahl *a* rechnerisch schnell und eindeutig auf den Klartext *m* schließen, da sich die Zahlen wegkürzen. Sie muss keinen Weg finden den diskreten Logarithmus zu lösen. Das müssten Außenstehende versuchen, um an den Klartext *m* zu gelangen, da ihnen die Zahl *a* nicht bekannt ist.[15]

[14] (Morpheus, 2016) (Lang, 2010) (Elgamal, 1985)
[15] (Kröll, 2007) (Buchman, 2010)

5 Sicherheit

5.1 Der Man-in-the-middle-Angriff

Bei dem Man-in-the-middle-Angriff (MitM-Angriff) täuscht ein Außenstehender „in der Leitung“ zwei Kommunikationspartner, indem er ihnen jeweils die Identität des anderen Teilnehmers vorspiegelt.

Der MitM-Angriff ist der größte Schwachpunkt bei dem DH-Schlüsselaustausch und so auch bei dem elGamal-Verschlüsselungsverfahren. Dabei wird der DH-Schlüsselaustausch so manipuliert, dass keine sichere Kommunikation zwischen den beiden Kommunikationspartnern stattfindet. Ein Außenstehender schaltet sich gleich zu Anfang des Schlüsselaustausches zwischen die Übermittlung der Daten. So denken Alice und Bob, dass sie sicher einen Schlüssel austauschen. Der Außenstehende (für dieses Beispiel Mallory) fängt aber die von Alice und Bob gesendeten Nachrichten bei der Schlüsselerstellung ab und ersetzt die Nachrichten durch eigene oder liest nur die Informationen mit. Mallory kommuniziert dadurch mit Alice und parallel dazu mit Bob. Beide denken die erhaltenden Nachrichten sind vom jeweils anderen: Alice denkt, dass die Nachrichten von Bob kommen und Bob glaubt, dass die erhaltenen Nachrichten von Alice gesendet worden sind. Mallory generiert sich, mit den öffentlich zugänglichen und bekannten Zahlen *p* und *g,* eine eigene Zahl Z. Er wählt, wie Alice und Bob zuvor, eine geheime Zahl z, die die Bedingungen erfüllt.[16]

$$Z = g^z \bmod p$$

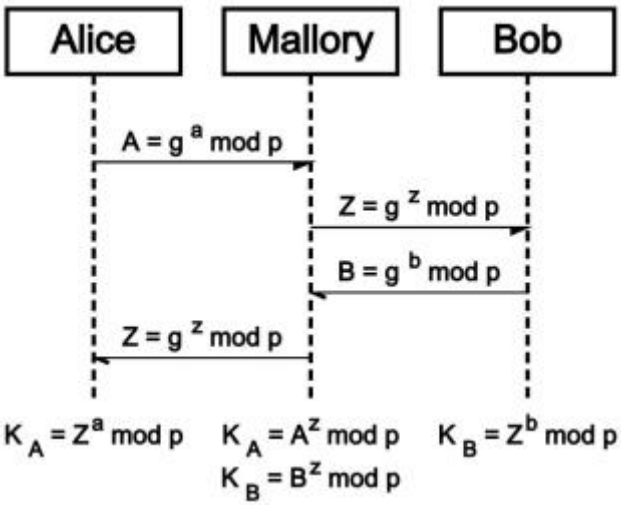

Abbildung 3: MitM-Angriff

Diese Zahl *Z* wird von Bob für das *A* von Alice gehalten und von Alice für das *B* von Bob. Es ergibt sich ein im nachfolgenden Schaubild (Abbildung 4) dargestellter Nachrichtenverkehr zwischen den Dreien:

Mallory führt jeweils einen DH-Schlüsselaustausch mit Alice und Bob ohne das Alice und Bob von Mallory Wissen. Es entstehen zwei verschiedene Schlüssel, die Mallory beide kennt, während Alice und Bob jeweils nur einen kennen. Mallory stellt somit eine Art Nachrichtenüberbringer zwischen Alice und Bob dar. Sie bekommt von Alice Nachrichten, die mit dem Schlüssel K_A verschlüsselt sind. Zur Weiterleitung an Bob entschlüsselt Mallory diese mit dem

[16] (Schmeh, 2016)

entsprechenden Schlüssel und verschlüsselt sie mit K_B, bevor Mallory die Nachrichten weiter an Bob leitet. In die andere Richtung wird bei Nachrichten von Bob an Alice genauso verfahren. Mallory kann dabei die Nachrichten die Alice und Bob übermitteln nicht nur mitlesen, sondern auch diese verändern oder komplett ersetzen.

Es gibt mehrere unterschiedliche Möglichkeiten sich vor einem um MitM-Angriff zu schützen und zu verhindern, dass die eigenen Nachrichten trotz der Verschlüsselung abgefangen werden.

Die Verwendung von Einmalpasswörtern ist eine davon. Über andere Informationskanäle tauschen die Kommunikationspartner Listen mit Einmalpassworten aus und steigern so den Grad der Sicherheit. Es können auch Hardwaregeräte genutzt werden. Diese haben den Vorteil, dass sie das Passwort z.B. alle 30 Sekunden ändern können. Wichtig bei diesem Verfahren ist die Sicherstellung, dass die Geräte oder Listen vom gewünschten Kommunikationspartner und nicht vom Angreifer kommen. Deswegen sollten die Passwörter über einen separaten Informationskanal erhalten worden sein, und nicht über den Kanal, über den verschlüsselt kommuniziert werden soll. Sobald der Angreifer Zugriff auf diese Informationen hat oder sie sogar selbst erzeugen kann, ist dieser Abwehrmechanismus des MitM-Angriffs nutzlos.

Es ist auch die Möglichkeit eine IP-Standortbestimmung durchzuführen. Durch die IP-Adresse lässt sich der geografische Standort eingrenzen und so die ungefähre Position des Kommunikationspartners bestimmen. Diese Information ist aber nur hilfreich, wenn der Standort des anderen Teilnehmers bekannt ist. Ansonsten lässt sich die Übereinstimmung nicht ermitteln. Sollte sich nun eine Person dazwischen schalten wollen und ihre Position weicht von dem bekannten Ort ab, weiß nun der Nutzer, dass die Verbindung nicht sicher ist. Außenstehende können jedoch ihre IP-Adresse verschleiern, wie zum Beispiel mit der Technik des Virtual Private Networks (VPN). Auch kann es sein, dass die Kommunikationspartner ihren Standort mal wechseln. Dieses müssten sie dann jedes Mal dem anderen Mitteilen, damit keine falschen Schlüsse gezogen werden. Eine IP-Standortbestimmung ist nicht aufwendig anzuwenden. Deshalb empfiehlt es sich, sie als zusätzliche Sicherheitsmaßnahme durchzuführen, wenn man weiß wo sein Kommunikationspartner sich ungefähr befindet.

Es kann auch versucht werden einen Digitalen Fingerabdruck mit Hilfe der im Browser verfügbaren Informationen zu erstellen. Beim Aufbau der Kommunikation wird dieser Fingerabdruck mit den Informationen im Browser des Kommunikationspartners verglichen. Diese Variante ist deutlich aufwendiger und dadurch ist kein kurzfristiger Wechsel auf ein anderes Gerät möglich, da dort die benötigten Informationen nicht hinterlegt sind. Außerdem

ist es auch möglich, dass ein Außenstehender die Informationen abfängt, da diese unverändert vom Original-User übertragen werden.

Durch eine Out of Band Authentication wird die Authentifizierung mit zwei unabhängigen Kanal durchgeführt. Das Bankenwesen nutzt diese Methode oft für Online Transaktionen. Dabei wird der Überweisungsauftrag online über einen Rechner durchgeführt. Um die Aktion jedoch durchführen zu können wird ein Sicherheitscode (die Tan) benötigt. Diese erhält der Nutzer über sein Handy, dass vorher authentifiziert wurde. Es können aber auch als zweiten Kanal die E-Mail oder der Post Weg genutzt werden. Durch Verwenden dieses Abwehrmechanismus muss der Angreifer beide Kanäle kontrollieren, was den Aufwand für ihn deutlich erhöht und auch erschwert.[17]

Es gibt viele Mechanismen einen MitM-Angriff möglichst aufwendig und schwierig zu gestalten. Es ist empfehlenswert, eine Kombination aus Abwehrmechanismen zu schaffen und ein konsequentes verschlüsseln aller Verbindungen durchzuführen und die Passwörter regelmäßig zu erneuern. Eine 100-prozentige Sicherheit kann jedoch nicht geschaffen werden. Man kann jedoch mit einer hohen Wahrscheinlichkeit feststellen, ob sich ein Angreifer in die Verbindung eingehackt hat oder ob der Nutzer mit dem gewünschten Kommunikationspartner direkt verbunden ist.

5.2 Das Diffie-Hellman-Problem

Beim Computational-Diffie-Hellman-Problem (CDH) wird angenommen, dass Außenstehende über die öffentliche Leitung die folgenden Daten erfahren: p, g, A und B. Die geheimen Zahlen a und b jedoch nicht, da sie nicht übermittelt werden. Ohne die Kenntnis ist es schwer den Schlüssel K zu berechnen. Es erschwert die Rechnung, wenn die Zahlen sehr groß sind. Daraus ergibt sich die Fragestellung für das CDH: *Wenn ein Element g einer Gruppe und die Werte $A = g^a$ und $B = g^b$ gegeben sind, welchen Wert hat dann $K = g^{ab}$ mit a,b unbekannt ?*

Das Problem ist nur mit einem großen Rechenaufwand zu lösen und somit ist der Schlüssel nur zu erzeugen. Die Problematik baut auf dem Diskretem-Logarithmus-Problem. Solange sich die Einwegfunktion nicht effizient lösen lässt, zählt der DH-Schlüsselaustausch als sicher.

Der Decisional-Diffie-Hellman (DDH) besagt, dass *g, g^a, g^b* und g^{ab} öffentlich ausgetauscht werden. Angreifer können aber nicht die einzelnen Zahlen voneinander unterscheiden. Für Außenstehende ist g^{ab} eine neue Zahl und nicht a und b multipliziert. Darin besteht die Problematik des DDH´s. Wer das CDH lösen kann, ist auch in der Lage das DDH zu lösen.

[17] (Knapp, kein Datum)

Bei der Auswahl von *g* als Primitivwurzel kann das DDH angegriffen werden. Der Angreifer kann prüfen, ob das Kriterium *„Sei P eine Primzahl, sei g eine Primitivwurzel modulo p und seien a,b∈{0,...,p−2}. Dann ist g^{ab} genau dann ein quadratischer Rest modulo p, wenn g^a oder g^b ein quadratischer Rest ist modulo p.“* Er hat damit einen deutlichen Vorteil zum reinen raten.[18]

Wenn man keine Zahlen nimmt lässt sich der DH-Schlüsselaustausch relativ leicht lösen: Die abgefangenen Informationen zwischen Alice und Bob sind: Die Primzahl $p = 17$, den Generator $g = 3$, $A = 6$ und $B = 12$. Mit diesen Informationen können Angreifer folgende drei Gleichungen aufstellen.

$$3^a \bmod 17 = 6 \qquad 3^b \bmod 17 = 12 \qquad 3^{ab} \bmod 17 = K$$

Um den Schlüssel zu berechnen, benötigt diese Person die Werte *a* und *b*. Wobei es beim DDH genügt 3^{ab} zu bestimmen, um an den Schlüssel *K* zu gelangen. Zu den drei Unbekannten *a*, *b* und *K* existieren drei Gleichungen. Durch die Besonderheit von Modulo gibt es mehrere Möglichkeiten um die Gleichungen richtig zu lösen. In einer Beispiel-Betrachtung werden Werte von 0 bis 50 für *a* und *b* geprüft. Die erste Gleichung wird von den Werten 15, 31 und 47 für *a* erfüllt. Die zweite Gleichung von den Werten 13, 29 und 49 für *b*. Diese Werte lassen sich in 9 verschiedenen Kombinationen für *K* verrechnen. Dieses *K* muss dann durch Trial-and-Error getestet werden, bis das passende K gefunden wurde.

Wenn ein möglicher Angreifer weiß, dass der DH-Schlüsselaustausch verwendet wird und er die entsprechenden Regeln beherrscht, dann kann dieser den Algorithmus deutlich schneller lösen. Er weiß, dass *a* und *b* kleiner als *p* sein müssen, welches er abfangen konnte. Jetzt hat der Angreifer jeweils nur noch eine passende Zahl übrig mit $a = 15$ und $b = 13$. Es lassen sich mit diesem Wissen *a* und *b* eindeutig bestimmen und somit lässt sich dann auch *K* eindeutig und schnell bestimmen.

Deshalb ist es wichtig deutlich größere Zahlen zu nehmen, um die Laufzeit der Bestimmung von *a* und *b* zu erhöhen. Wenn die Zahlen weit mehr als 100 Stellen haben, dauert die Berechnung sogar einige Jahre. Bei einer solchen Zeitspanne kann die Entschlüsselung als unmöglich und somit als sehr starke Verschlüsselung betrachtet werden. Die Stärke einer Verschlüsselung basiert immer auf der Dauer, die benötigt wird, um die Verschlüsselung rückgängig zu machen, ohne den Schlüssel zu kennen.

[18] (Morpheus, 2016) (Unbekannt, 2017)

5.3 Sicherheit des elGamal-Verschlüsselungsverfahren

Da das elGamal-Verschlüsselungsverfahren auf dem Prinzip des DH-Schlüsselaustausch basiert, hat es auch ähnliche mathematischen Standardprobleme. Das in Kapitel 4.1 beschriebene Diffie-Hellmann-Problem zu lösen ist äquivalent zum Lösen der elGamal-Verschlüsselung. Zum einen das Diskreter-Logarithmus-Problem, bei dem es noch kein effizientes Verfahren zum Lösen gibt. Ebenso wie das CDH, bei dem es beim elGamalverfahren genügt g^{ab} zu bestimmen, um die Nachricht zu entschlüsseln und auch das DDH erschwert dem Angreifer die gewünschten Informationen zu erhalten, da dieser nicht den Unterschied zwischen den Geheimtexten zweier Klartexte kennt.

Diese Annahmen sind Standardannahmen in der Kryptographie. Deshalb wird vom heutigen Stand aus angenommen, dass das elGamal-Verschlüsselungsverfahren nicht in vertreterbarer Zeit gebrochen werden kann und somit als sicher gilt.[19]

[19] (Lang, 2010) (Kreitz, 2007)

7 Anwendung

Asymmetrische Verschlüsselungsverfahren bzw Public-Key-Kryptosysteme werden heutzutage in vielen Bereichen angewendet. Sie sind ein wahrer Meilenstein in der Kryptographie. Bis zur Entwicklung dieser Verschlüsselungsart mussten beide Kommunikationspartner immer einen gemeinsamen Schlüssel besitzen. Dieser Schlüssel musste vor der Kommunikation über einen anderen Nachrichtenkanal ausgetauscht werden. Da dies ein aufwändiger Vorgang ist, ersetzten Public-Key-Kryptosysteme viele symmetrische Verschlüsselungsverfahren.

Zum Beispiel werden asymmetrische Verschlüsselungen beim Internet-Shopping an mehreren Stellen genutzt. Zum einen beim Einloggen eines Accounts bei einem Portal wie Amazon über eine verschlüsselte Verbindung. Auch die Kreditkarten Informationen und Kundeninformationen sind verschlüsselt auf den Servern der Unternehmen gespeichert. [20]

Auch werden Public-Key-Kryptosysteme heutzutage im E-Mail-Verkehr eingesetzt. Das hierfür verwendete Datenformat ist OpenPGP, das Daten verschlüsseln und digital signieren kann. Die ursprüngliche PGP Version nutzte RSA-Schlüssel. Da diese aber einem amerikanischem Patent unterlag wird in den neueren Versionen der DH-Schlüsselaustausch genutzt. Eines der bekannteren Produkte, die das OpenPGP-Protokoll verwenden, ist das Open-Source-Programm GnuPG. [21]

Eine größere Verwendung haben Public-Key-Verschlüsselungssysteme in dem Protokoll https gefunden. Dieses Protokoll stellt eine sichere Verbindung des Web-Browsers mit einem Server her. Dadurch wird das Abhören der Verbindung verhindert. Die Daten werden verschlüsselt, um einen unbefugten Zugriff zu verhindern und darüber hinaus authentifiziert, um einen Man-in-the-middle-Angriff abzuwehren.

Am meisten werden asymmetrische Verschlüsselungsverfahren in Kombination mit symmetrischen Verschlüsselungsverfahren genutzt, sogenannte hybride Verschlüsselung. Durch die Kombination der beiden Verfahren können die Stärken beider Verfahren ausgenutzt werden. Symmetrische Verschlüsselungsverfahren können auch bei großen Datenmengen Verschlüsselungen schnell erledigen. Der Vorteil der asymmetrischen Verschlüsselungsverfahren liegt darin, dass lediglich der öffentliche Schlüssel benötigt wird und nicht vor dem Beginn der Kommunikation bereits Schlüssel ausgetauscht werden müssen. Hybride Verschlüsselungsverfahren werden unter anderem beim Online-Banking eingesetzt, können aber auch zur E-Mail-Verschlüsselung verwendet werden.

[20] (Baum, 2013)
[21] (Hansen, kein Datum)

8 Fazit

Der DH-Schlüsselaustausch war das erste Public-Key-Kryptosystem. Es ist somit einer der wichtigsten Meilensteine in der Entwicklung der Kryptographie und hat den Grundstein für viele Folgeverfahren gelegt. Mittlerweile findet der DH-Schlüsselaustausch nur noch wenig Anwendung. Auch das elGamal-Verschlüsselungsfahren, das den DH-Schlüsselaustausch für den Nutzer optimiert hat, wird heute nur noch sehr selten verwendet. Die Nachfolgeverfahren sind noch um einiges sicherer und auch häufig schneller, weshalb sie den DH-Schlüsselaustausch und das elGamal-Verfahren größtenteils verdrängt haben.

Trotz der MitM-Gefahr, die die meisten Public-Key-Kryptosysteme betrifft, gelten der DH-Schlüsselaustausch und das elGamal-Verfahren auch heute noch als relativ sichere Verfahren. Das wird auch so lange bleiben, bis ein Algorithmus entwickelt wird, der den Diskreten-Logarithmus effizent lösen kann. Nach Aktuellem Stand (2017) sobald das theoretische Konzept eines Quantencomputers realisiert werden kann.

Mit der größte Vorteil am DH-Schlüsselaustausch und elGamal-Verschlüsseleungeverfahren ist, das keine Patentrechte vorliegen und so für Open Source Programme und Systeme nutzbar sind.

Durch den starken Zuwachs des Datenaustausches im Internet und der damit einhergehende Zuwachs im Austausch von hochsensiblen Daten sind Public-Key-Kryptosysteme in unserer heutigen Welt äußerst wichtig. Ohne die Kryptosysteme würden Funktionen, wie Online Banking, sichere Kommunikation oder Shopping im Internet nicht mehr funktionieren. Zum Erhalt dieser „Selbstverständlichkeiten“ ist die Weiterentwicklung der Public-Key-Kryptosysteme unabdingbar.

Außerdem ist es wichtig nicht nur dann eine Verschlüsselung zu nutzen, wenn wir mit vertraulichen Daten arbeiten. Wenn nur Dissidenten Verschlüsslung nutzen, dann haben Behörden oder Hacker ein leichtes Spiel sie zu identifizieren. Wenn aber viele Menschen eine Verschlüsslung nutzen, kann man ein normales Chat Gespräch nicht von einer privaten und geheimen Unterhaltung unterscheiden.

Dennoch ist es wichtig, uns daran zu erinnern, dass Verschlüsselung nicht auf magische Weise alle Kommunikation sicher und unlesbar macht. Man muss ausreichend Vorrichtungen treffen wie zum Beispiel unter 5.1 beschriebene Gegenmaßnahmen eines MitM-Angriffs und auch vorhandene Schlüssel regelmäßig erneuern.

9 Literaturverzeichnis

Anon., kein Datum *Lehrtext zur Klassischen Kryptographie.* [Online]
Available at: http://homepages.physik.uni-muenchen.de/~milg/quantenkryp/Kryptographie-Lehrtext.pdf
[Zugriff am 2 5 2017].

Baum, F., 2013. *Netzwelt.* [Online]
Available at: https://www.netzwelt.de/news/105101_3-netzwelt-wissen-verschluesselung.html
[Zugriff am 9 5 2017].

Brünner, A., 2003. [Online]
Available at: http://www.arndt-bruenner.de/mathe/Allgemein/fermatklein.htm
[Zugriff am 2 5 2017].

Buchman, J., 2010. *Einführung in die Kryptographie.* 5. Hrsg. s.l.:Springer Verlag.

Cruise, 2012. *YouTube.* [Online]
Available at: https://www.youtube.com/watch?v=YEBfamv-_do
[Zugriff am 30 4 2017].

CryptoCD, D., 2017. *Die CryptoCD.* [Online]
Available at: http://www.vorratsdatenspeicherung.de/CD/CD_1.0/cryptocd/doku/macos/verschluesselung_funktion/verschluesselung_funktion.html
[Zugriff am 25 4 2017].

Cvrk, L., kein Datum. *Kryptowissen.de.* [Online]
Available at: http://www.kryptowissen.de/asymmetrische-verschluesselung.html
[Zugriff am 25 4 2017].

Cvrk, L., kein Datum. *Kryptowissen.de.* [Online]
Available at: http://www.kryptowissen.de/symmetrische-verschluesselung.html
[Zugriff am 25 4 2017].

Elgamal, T., 1985. *A public key cryptosystem and a signature scheme based on discrete logarithms.* s.l.:s.n.

Hansen, M., kein Datum *Unabhängiges Landeszentrum für Datenschutz.* [Online]
Available at: Die ursprüngliche PGP Version nutzte sogenannte RSA-Schlüssel
[Zugriff am 9 5 2017].

Hellman, D. u., 1976. *New Directions in Cryptography,* Stanford University: IEEE Transactions on Information Theory.22.

Knapp, F., kein Datum *Man-in-the-middle: Angriff und Abwehr.* Hochschule Reutlingen: s.n.

Kröll, M., 2007. [Online]
Available at:
http://www.math.tugraz.at/~aistleitner/Proseminar20082009/Kröll/elgamal_beamer_kroell.pdf
[Zugriff am 2 5 2017].

Kreitz, 2007. *Universität Potsdam.* [Online]
Available at: http://www.cs.uni-potsdam.de/ti/lehre/07-Kryptographie/slides/slides-5.2.pdf
[Zugriff am 2 5 2017].

Lang, H., 2010. *Kryptografische Protokolle.* [Online]
Available at: http://www.iti.fh-flensburg.de/lang/krypto/protokolle/elgamal.htm
[Zugriff am 2 5 2017].

Malenkovich, S., 2013. *Kaspersky Lap.* [Online]
Available at: https://blog.kaspersky.de/warum-sie-ihre-daten-verschlusseln-sollten/1088/
[Zugriff am 25 4 2017].

mk, 2012. *HSG.* [Online]
Available at: http://www.hsg-kl.de/faecher/inf/krypto/prinzip/index.php
[Zugriff am 25 4 2017].

Morpheus, T., 2016. *YouTube.* [Online]
Available at:
https://www.youtube.com/watch?v=_E0SGl7aN70&list=PLNmsVeXQZj7pWwFv5APk240hrehtCJae-&index=30
[Zugriff am 15 04 2017].

Schmeh, K., 2016. *Kryptografie.* 6. Hrsg. Heidelberg: dpunkt.verlag.

Unbekannt, 2017. *Wikipedia.* [Online]
Available at: https://de.wikipedia.org/wiki/Kerckhoffs'_Prinzip
[Zugriff am 19 April 2017].

Unbekannt, 2017. *Wikipedia.* [Online]
Available at: https://de.wikipedia.org/wiki/Diffie-Hellman-Schlüsselaustausch#Sicherheit
[Zugriff am 6 5 2017].

Vinck, A. H., 2012. *University of Duisburg-Essen.* [Online]
Available at: https://www.uni-due.de/imperia/md/images/dc/crypto_chapter_5_public_key.pdf
[Zugriff am 30 4 2017].

Weisstein, E. W., Kein Datum. *WolframMathWorld.* [Online]
Available at: http://mathworld.wolfram.com/SophieGermainPrime.html
[Zugriff am 9 5 2017].