FACHHOCHSCHULE WEDEL

Seminararbeit

in der Fachrichtung
Wirtschaftsingenieurwesen
Sommersemester 2018

Seminar Informatik

Thema:

Einführung in die Grundbegriffe der Kryptologie

Eingereicht von: Lukas Kirschnick

Email: wing102754@fh-wedel.de

Erarbeitet im: 3. Semester

Abgegeben am: 18. Mai 2018

Referent (FH Wedel): Prof. Dr. Michael Anders
Fachhochschule Wedel
Feldstraße 143
22880 Wedel
Tel. (0 41 03) 8048-24

Inhaltsverzeichnis

Abkürzungsverzeichnis II
Abbildungsverzeichnis II
Einleitung 1
1. Kryptologie 2
1.1. Kryptographie 3
1.2. Kryptoanalyse 4
1.3. Steganographie 4
2. Grundlagen der Kryptographie 5
2.1. Grundsätze der Kryptographie 5
2.1.1. Kerckhoffs´sches Prinzip 5
2.1.2. Shannon´s Prinzip 5
2.2. Einteilung der Verfahren 6
2.2.1. Symmetrische Verfahren 6
2.2.2. Asymmetrische Verfahren 7
2.2.3. Hybride Verfahren 7
2.3. Anforderungen an die Kryptographie 7
3. Symmetrische Kryptographie 8
4. Asymmetrische Kryptographie 10
5. Kryptographische Hash-Funktionen und digitale Signaturen 12
5.1 Hashfunktionen 12
5.2 Digitale Signaturen 13
6. Fazit 14
Literaturverzeichnis III
Eidesstattliche Erklärung IV

Abkürzungsverzeichnis

v. Chr.:	- vor Christi Geburt
bzw.:	- beziehungsweise
bzgl.	- bezüglich
z.B.:	- zum Beispiel
DES:	- Data Encryption Standard
IDES:	- International Data Exchange System
WPA:	- Wi-Fi Protected Access
WLAN:	- Wireless Local Area Network
AES:	- Advanced Encryption Standard

Abbildungsverzeichnis

Abbildung 1: Bestandteile der Kryptologie 2
Abbildung 2: Kommunikation über einen unsicheren Kanal 8
Abbildung 3: Verschlüsselung mit symmetrischer Kryptographie 9
Abbildung 4: Basisprotokoll zur sicheren Datenübertragung mit asymmetrischer Kryptographie 11
Abbildung 5: Basisprotokoll für den Schlüsseltransport mit asymmetrischer Kryptographie 12

Einleitung

Täglich hat nahezu jeder Mensch bewusst oder unbewusst mit Kryptologie zu tun. Sei es durch das Verschlüsseln oder Entschlüsseln von Texten während des E-Mailverkehrs, beim bargeldlosen Bezahlen oder durch den Umgang mit einem Computer am Arbeitsplatz.

Dies ist jedoch kein Phänomen der Neuzeit, sondern ein kontinuierlicher Prozess, welcher auf großartigen Entwicklungen in der Vergangenheit beruht. Meilensteine wie zum Beispiel ca. 500 v.Chr. mit der SKYTALE und 100-44 v. Chr. mit dem CEASAR-Code, der ENIGMA im Jahre 1923, bis hin zur RSA-Verschlüsselung aus 1978[1].

Aufgrund des Wandels der Gesellschaft von einer Industrie- hin zu einer Informationsgesellschaft, spielt die Kryptologie in der heutigen Zeit eine immer größere Rolle. Wie jede Wissenschaft geht auch die Kryptologie von Grundproblemen aus und versucht diese zu lösen. Hierbei entstehen Fragestellungen wie zum Beispiel:

Wie kann ich mit jemandem vertraulich kommunizieren, sodass kein Unbeteiligter Kenntnis von der übermittelten Nachricht erlangt?

Wie kann ich sichergehen, dass die empfangene Nachricht wirklich von dem ausgewiesenen Sender stammt?

Wie kann ich im Zeitalter der elektronischen Kommunikation meine Privatsphäre schützen[2]?

Diese Seminararbeit soll einen Einblick in die Grundbegriffe der Kryptologie geben und die Notwendigkeit dieser Wissenschaft verdeutlichen. Diese Arbeit gliedert sich in sechs Kapitel. Zunächst erfolgt ein Überblick über den Begriff der Kryptologie. Anschließend wird das Thema der Kryptographie detailliert betrachtet sowie die Grundsätze und einzelnen Verfahren näher erläutert. Abschließend erfolgt ein kurzer Einblick bzgl. Hashfunktionen und digitalen Signaturen, gefolgt von einem Fazit.

[1] Vgl. Stobitzer, Kryptowissen, 2018
[2] Ebd.

1. Kryptologie

Der Begriff Kryptologie setzt sich aus den zwei griechischen Wörtern „kryptós“ und „logos“ zusammen, wobei kryptos gleichbedeutend für verborgen und logos für die Lehre steht. Die Kryptologie ist also die Lehre des Verborgenen bzw. Verbergens.

Die Kryptologie fasst als Oberbegriff zwei Unterthemen zusammen. Zum einen die Kryptographie und zum anderen die Kryptoanalyse.

Bei der Kryptographie geht es darum kryptographische Systeme und Verfahren zu entwerfen und zu implementieren, während es bei der Kryptoanalyse darum geht bestehende kryptologische Systeme und Verfahren auf deren Sicherheit, bzw. auf Stärken und Schwächen zu testen. Im Hinblick auf die Schwächen spielt insbesondere die Sicht des Angreifers eine wichtige Rolle um Sicherheitslücken schnellstmöglich aufzudecken.

Im unteren Schaubild werden die grundsätzlichen Bestandteile der Kryptologie dargestellt. In den folgenden Kapiteln werden die einzelnen Unterthemen genauer erläutert[3].

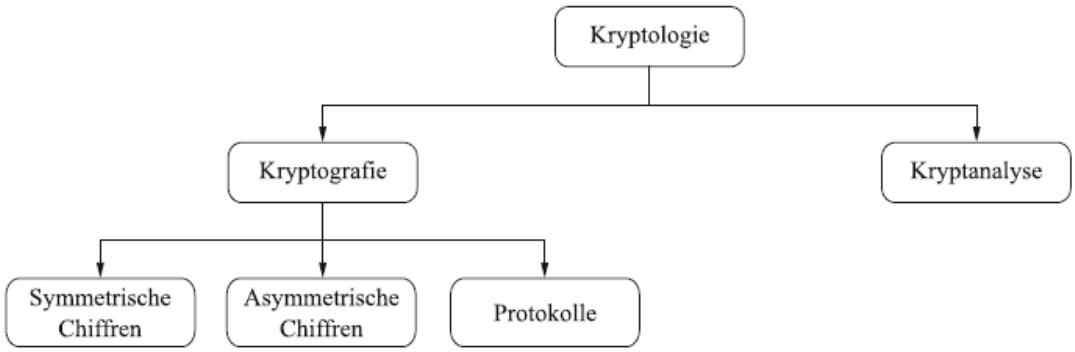

Abbildung 1: Bestandteile der Kryptologie[4]

[3] Vgl. Stobitzer, Kryptowissen, 2018
[4] Vgl. Paar & Pelzl, 2016, Seite 3

1.1. Kryptographie

Der klassische Gegenstand der Kryptographie sind Verschlüsselungsverfahren. Diese Verfahren werden benötigt um Nachrichten oder gespeicherte Daten geheim zu halten. Ein unverschlüsselter Text wird als Klartext bezeichnet und der verschlüsselte Text als Chiffretext oder Chiffrat.

Kryptographie ist die Wissenschaft der Verschlüsselung von Information durch Geheimschriften bzw. Chiffren. Dabei werden meist geheime Schlüssel verwendet. Die Kryptographie umfasst jedoch nicht nur die Anwendung, sondern auch die Entwicklung von Verfahren mit Verschlüsselungen.

Um einen Klartext unkenntlich zu machen, wird dieser chiffriert. Beim Dechiffrieren wird die Verschlüsselung umgekehrt bzw. aufgehoben. Der Schlüssel kontrolliert die Ver- und Entschlüsselung einer Information. Der Schlüssel ist der Informationsträger des Klartextes bzw. der Entschlüsselung des Chiffrats. Für Dritte die nicht im Besitz des Schlüssels sind, ist es in der Regel und in sinnvoller Zeit, nicht möglich den Schlüsseltext zu entschlüsseln und somit den Klartext zu lesen[5].

Für eine problemlose Übertragung und Unversehrtheit des Klartextes gegenüber Dritter ist es sehr wichtig, dass der Schlüssel zwischen Absender und Empfänger über einen sicheren Kanal übermittelt wird. Die Verschlüsselung ist ein Algorithmus, der den Klartext mit Hilfe eines Schlüssels in ein Chiffrat umwandelt. Der Entschlüsselungsalgorithmus erzeugt wiederum mit Hilfe des Schlüssels den Klartext. Die Gesamtheit von Algorithmus, der Menge aller Klartexte und Schlüssel ergeben ein Kryptosystem.

Heutzutage gängige Verfahren der Kryptographie haben meist eine mathematische Basis und sind standardisiert. Die Sicherheit der Verfahren beruht darauf, dass die Verfahren weltweit von Kryptologen untersucht und eventuelle Schwächen öffentlich bekannt gemacht werden[6]. Im folgenden Kapitel wird näher auf die Grundlagen der Kryptographie eingegangen sowie einzelne Verfahren genauer betrachtet.

[5] Vgl. Swoboda, Spitz, & Pramateftakis, 2008, Seite 18 ff.
[6] Ebd.

1.2. Kryptoanalyse

Als Kryptoanalyse oder auch Kryptanalyse bezeichnet man sowohl die Untersuchung von Verschlüsselungsverfahren auf ihre Resistenz gegenüber Sicherheitsangriffen als auch das Herausfinden von geheimen Schlüsseln. Kryptoanalyse wird umgangssprachlich auch Brechen oder Knacken einer Verschlüsselung genannt[7].

1.3. Steganographie

Neben der Verschlüsselung gibt es auch die Möglichkeit, die Existenz einer geheimen Botschaft zu verbergen. Solche Verfahren bezeichnet man als steganographische Verfahren. Ein klassisches Beispiel ist das Schreiben mit Zitronensaft als Tinte, die über der Flamme einer Kerze sichtbar gemacht werden kann. Eine geheime Botschaft kann auch in einem Bild versteckt werden. In digitalen Audio- oder Videodateien lassen sich geheime Botschaften ebenfalls verstecken, indem dafür die niederwertigen Bits der Audio- oder Videodaten genutzt werden, was kaum hörbar oder sichtbar ist.

Wenn die versteckten Daten verschlüsselt wurden, dann können diese nur mit Kenntnis des Schlüssels erkannt werden. Versteckte Daten in Audio- oder Videodateien werden z.B. genutzt, um durch digitale Wasserzeichen unrechtmäßig kopierte Dateien zu verfolgen[8].

[7] Vgl. Paar & Pelzl, 2016, Seite 10
[8] Vgl. Swoboda, Spitz, & Pramateftakis, 2008, Seite 17 f.

2. Grundlagen der Kryptographie

Im folgenden Kapitel werden ausgewählte Grundlagen der Kryptographie dargestellt. Einerseits erfolgt ein Einstieg in die Grundsätze der Kryptographie, wie zum Beispiel die Prinzipien, andererseits erfolgt die Einteilung der Verfahren sowie die Erläuterung der grundsätzlichen Anforderungen.

2.1. Grundsätze der Kryptographie

Um Verschlüsselungsverfahren sicher und erfolgreich zu entwickeln, sollten die folgenden Prinzipien eingehalten werden.

2.1.1. Kerckhoffs´sches Prinzip

Das Prinzip nach August Kerckhoffs besagt, dass die Sicherheit eines Verschlüsselungsverfahrens nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus, sondern auf der Geheimhaltung des Schlüssels beruht. Mit seinen Prinzipien hat Kerckhoffs eine Revolution der Kryptographie eingeleitet. Fortan war es möglich Algorithmen einzusehen und diese öffentlich zu diskutieren und somit zu verbessern[9].

2.1.2. Shannon´s Prinzip

Claude Shannon gilt als der Begründer der modernen Informationstheorie. Er stellte 1949 die Prinzipien der Konfusion und Diffusion auf und definierte zwei grundlegende Operationen, mit denen starke Chiffren realisiert werden können:

- **Konfusion** ist eine Verschlüsselungsoperation, die die Beziehung zwischen Schlüssel und Chiffrat verschleiert. Substitutionstabellen sind heutzutage das gängigste Element, um Konfusion zu erreichen. Sie finden sich sowohl im DES als

[9] Vgl. Paar & Pelzl, 2016, Seite 13

auch im AES wieder, also im sogenannten Data und Advanced Encryption Standard[10].

- **Diffusion** ist eine Verschlüsselungsoperation, bei welcher die Chiffretextzeichen von möglichst vielen Zeichen des Klartextes und des gesamten Schlüssels abhängen sollen. Dadurch wirkt sich ein Angriff auf einen kleinen Teil des abgefangenen Chiffrats, welcher geändert wird, auf die ganze Nachricht aus. Die Änderungen bewirken wiederrum eine unmögliche Entzifferung des Chiffrats durch den Empfänger.

Chiffren, welche lediglich Konfusion oder Diffusion verwenden, wie beispielsweise die im Zweiten Weltkrieg eingesetzte Enigma (Konfusion), sind nicht sicher. Um eine starke Chiffre zu erzeugen, verwenden die meisten modernen symmetrischen Verschlüsselungsverfahren, wie DES oder IDEA, eine Kombination dieser beiden Verfahren, ein sogenanntes Hintereinanderschalten der Konfusion und Diffusion[11].

2.2. Einteilung der Verfahren

Es gibt unterschiedliche Verfahren der Kryptographie. Diese werden aufgrund ihrer verschiedenen Schlüssel in zwei Klassen unterscheiden.

2.2.1. Symmetrische Verfahren

Bei symmetrischen Verfahren wird zur Ver- und Entschlüsselung des Chiffrats, derselbe Schlüssel verwendet. Sender und Empfänger müssen sich auf einen Schlüssel einigen, bevor die Nachricht chiffriert werden kann. Die Schlüsselübertragung sollte immer über eine gesicherte Leitung erfolgen[12].

[10] Vgl. Paar & Pelzl, 2016, Seite 28 ff.
[11] Ebd.
[12] Vgl. Paar & Pelzl, 2016, Seite 3 f.

2.2.2. Asymmetrische Verfahren

Bei asymmetrischen Verfahren wird ein öffentlicher Schlüssel zum Verschlüsseln und ein privater Schlüssel zum Entschlüsseln verwendet. Asymmetrische Verfahren werden häufig als Public-Key Verfahren bezeichnet.

2.2.3. Hybride Verfahren

Hybride Verfahren vereinen die Vorteile der symmetrischen und asymmetrischen Verfahren zu einem Neuen. Sie sind eine Kombination beider Verfahren.

2.3. Anforderungen an die Kryptographie

Das Hauptziel der modernen Kryptographie ist einerseits die Geheimhaltung von Daten. Andererseits sind folgende Punkte von besonderer Bedeutung für die elektronische Kommunikation:

- Vertraulichkeit
- Integrität bzw. Änderungsschutz
- Authentifizierung bzw. Fälschungsschutz und
- Verbindlichkeit bzw. Nichtleugbarkeit

Die Authentifizierung und Vertraulichkeit stellt die Herkunft einer Nachricht sicher. Durch die Integrität wird die Unverfälschtheit einer Nachricht sichergestellt, sodass gewährleistet ist, dass die Nachricht unverändert beim Empfänger eintrifft. Die Verbindlichkeit verhindert, dass ein Sender einer Nachricht diese nachträglich leugnen kann, beispielsweise durch ein Sendeprotokoll[13].

[13] Vgl. Beutelspacher, Schwenk, & Wolfenstetter, 2015, Seite 1 ff.

3. Symmetrische Kryptographie

Mit Hilfe eines einfachen Beispiels kann das Prinzip der symmetrischen Kryptographie optimal veranschaulicht werden. In der folgenden Abbildung 2 sind zwei Benutzer dargestellt, welche über einen unsicheren Kanal kommunizieren möchten. Die beiden Nutzer werden in der Literatur häufig Alice und Bob genannt[14].

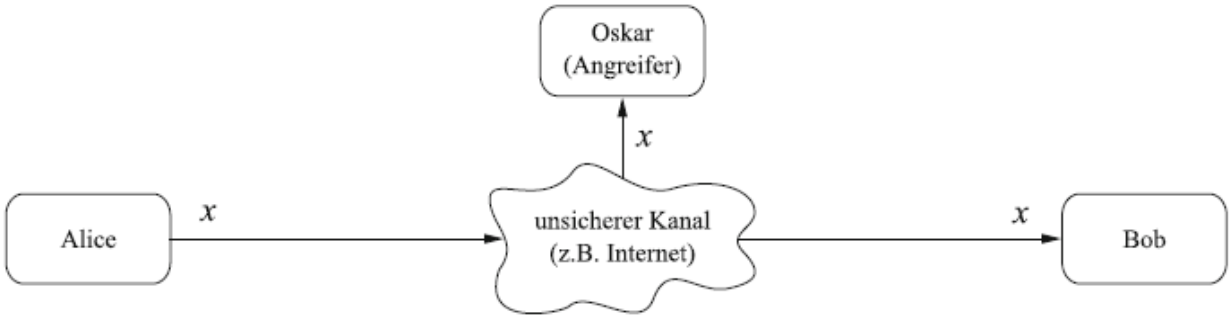

Abbildung 2: Kommunikation über einen unsicheren Kanal[15]

Der Begriff „Kanal“ steht in diesem Fall für die Kommunikationsstrecke, z.B. das Internet, Mobilfunk oder ähnliches, über welches sich digitale Daten übertragen lassen. Ein dritter Gegenspieler namens Oskar versucht sich unbefugten Zugriff zu den Daten zu verschaffen und wird als Angreifer bezeichnet.

Dieses Problem der vertraulichen Kommunikation ist das klassische Einsatzgebiet der symmetrischen Kryptografie. In der folgenden Abbildung 3 verschlüsselt Alice ihre Nachricht x mithilfe eines symmetrischen Verfahrens. Das Ergebnis der Verschlüsselung ist das Chiffrat y, welches anschließend an Bob geschickt wird, der das Chiffrat wiederum entschlüsselt und liest[16].

[14] Vgl. Paar & Pelzl, 2016, Seite 3 f.
[15] Ebd.
[16] Ebd.

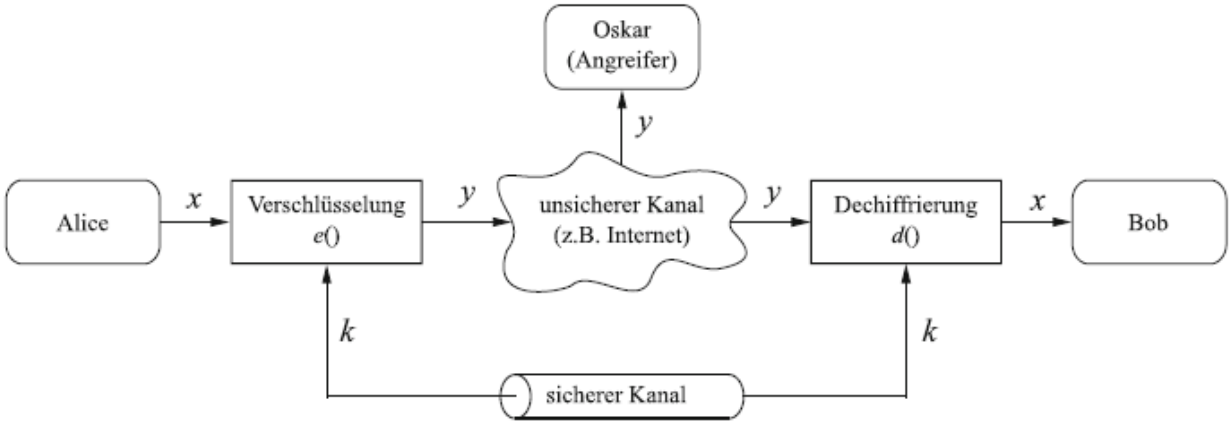

Abbildung 3: Verschlüsselung mit symmetrischer Kryptographie[17]

Wie aus der Abbildung 3 ersichtlich, ist das Entschlüsseln somit die umgekehrte Operation zur Verschlüsselung. Diese Verschlüsselung sorgt dafür, dass die übermittelten Daten für Unbefugte unkenntlich gemacht werden. Somit ergibt das Chiffrat für den Angreifer Oskar lediglich eine ungeordnete Zeichenfolge ohne jeglichen Mehrwert.

Alice und Bob verfügen über den sogenannten Schlüssel, dieser wird über einen sicheren Kanal übertragen und bildet die Grundlage für die symmetrische Kryptografie. Ein einfaches Beispiel für einen sicheren Kanal ist die manuelle Übertragung des Schlüssels auf einem Zettel für die WLAN-Verschlüsselung, als Teil des WPA-Protokolls eines Internetanbieters. Diese Methode wird als sog. „pre-shared key“ bezeichnet.

Der Schlüsselaustausch erfolgt einmalig. Danach können Alice und Bob beliebig oft sicher miteinander kommunizieren. Jedoch hat die Geheimhaltung des Schlüssels oberste Priorität, wobei das so genannte „Schlüsselaustauschproblem“ eine große Rolle spielt[18].

[17] Vgl. Paar & Pelzl, 2016, Seite 6
[18] Vgl. Paar & Pelzl, 2016, Seite 4 f.

Folgende Variablen x, y und k in Abbildung 3 sind in der symmetrischen Kryptografie sehr wichtig:

- x ist der Klartext.
- y ist das Chiffrat oder der Geheimtext, auch Chiffretext und Kryptogramm.
- k ist der Schlüssel.
- e ist die Verschlüsselung oder Chiffrierung.
- d ist die Entschlüsselung oder Dechiffrierung.
- Die Menge aller möglichen Schlüssel wird als Schlüsselraum bezeichnet[19].

4. Asymmetrische Kryptographie

Die Grundlage der asymmetrischen Kryptografie bilden, im Gegensatz zu der symmetrischen Kryptografie, zwei Schlüssel. Ein Schlüssel ist der öffentliche Schlüssel, auch bekannt als „Public-Key“ (kpub), der andere ist der private Schlüssel, der so genannte „Private-Key“ (kpr). Daten, welche mit dem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem privaten Schlüssel entschlüsselt werden. Deshalb muss der private Schlüssel vom Besitzer des Schlüsselpaares geheim gehalten werden. Die asymmetrische Kryptographie wird auch als das „Public-Key-Verfahren“ bezeichnet[20].

Um dieses System genauer zu beleuchten, betrachten wir erneut das Bespiel der Kommunikation zwischen Alice und Bob sowie dem Angreifer Oskar.

Zur Realisierung eines solchen Systems, veröffentlicht Bob einen öffentlichen Schlüssel zur Verschlüsselung, welcher jedem bekannt ist. Weiterhin besitzt Bob noch einen passenden privaten und somit geheimen Schlüssel, der für die Dechiffrierung verwendet wird.

Die asymmetrische Kryptographie basiert auf der Grundlage, dass jeder Anwender die Möglichkeit besitzt Daten zu verschlüsseln. Jedoch kann lediglich die Person, welche den

[19] Vgl. Paar & Pelzl, 2016, Seite 4 f.
[20] Vgl. Paar & Pelzl, 2016, Seite 173 ff.

dazugehörigen privaten und geheimen Schlüssel besitzt, die Daten wieder entschlüsseln und lesen[21].

Das in der folgenden Abbildung 4 gezeigte Basisprotokoll erlaubt es, Nachrichten zu verschlüsseln, ohne zuvor einen geheimen Schlüssel über einen sicheren Kanal ausgetauscht zu haben.

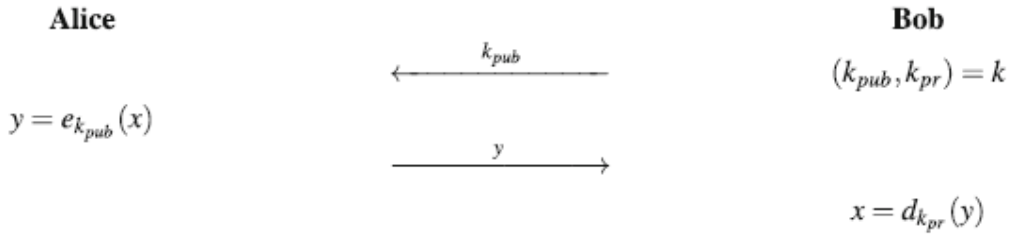

Abbildung 4:Basisprotokoll zur sicheren Datenübertragung mit asymmetrischer Kryptographie[22]

Das Protokoll kann jedoch ebenfalls dafür verwendet werden, um Schlüssel für symmetrische Chiffren wie AES oder 3DES auszutauschen. Voraussetzung hierfür ist lediglich, dass der symmetrische Schlüssel unter Verwendung des asymmetrischen Algorithmus verschlüsselt wird, z. B. durch einen AES-Schlüssel.

Sobald der symmetrische Schlüssel von Bob entschlüsselt wurde, können beide Parteien diesen zur symmetrischen Ver- und Entschlüsselung von Nachrichten verwenden. In der folgenden Abbildung 5 wird das Protokoll für den Schlüsseltransport dargestellt.

Der Hauptvorteil des Protokolls in Abbildung 5 gegenüber dem Protokoll in Abbildung 4 ist, dass die Daten mit einer symmetrischen Chiffre verschlüsselt werden, was wesentlich schneller als mit einer asymmetrischen Chiffre ist[23].

[21] Vgl. Paar & Pelzl, 2016, Seite 173 ff.
[22] Vgl. Paar & Pelzl, 2016, Seite 176
[23] Vgl. Paar & Pelzl, 2016, Seite 173 ff.

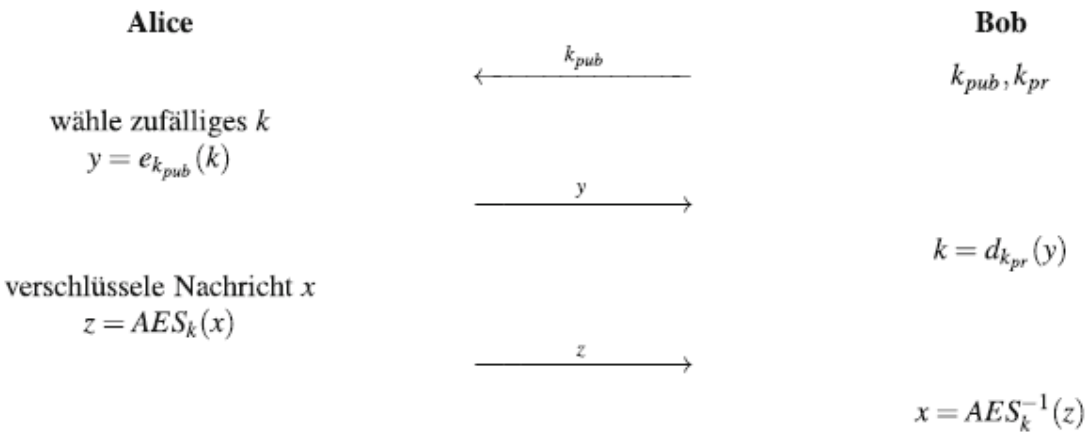

Abbildung 5: Basisprotokoll für den Schlüsseltransport mit asymmetrischer Kryptographie[24]

5. Kryptographische Hash-Funktionen und digitale Signaturen

Im folgenden Kapitel erfolgt ein Einblick in kryptographische Hashfunktionen und die digitalen Signaturen.

5.1 Hashfunktionen

Kryptografische Hash-Funktionen sind ein wichtiges kryptografisches Instrument und bilden einen eigenen Bereich in der Kryptographie. Kryptographische Hash-Funktionen generieren aus beliebig langen Datensätzen eine Zeichenkette mit einer festen Bit-Länge. Ein Datensatz kann ein Wort, ein längerer Text oder auch eine ganze Datei sein. Der erzeugte Hash-Wert der Zeichenkette wird als digitaler Fingerabdruck der Nachricht bezeichnet. Hash-Funktionen haben viele Anwendungen in der Kryptografie, sie sind ein wichtiger Teil von Signaturverfahren und kryptografischen Prüfsummen. Hash-Funktionen haben darüber hinaus noch viele andere Einsatzmöglichkeiten, wie zum Beispiel das Speichern von Passwörtern oder Schlüsselableitungen[25].

[24] Vgl. Paar & Pelzl, 2016, Seite 177
[25] Vgl. Paar & Pelzl, 2016, Seite 340 ff.

Eigenschaften von Hash-Funktionen:

- Eine Hash-Funktion kann eine Nachricht in beliebiger Länge verarbeiten.
- Eine Hash-Funktion erzeugt Hash-Werte in einer festen Länge.
- Hash-Funktionen sind effizient. Die Berechnung kann einfach realisiert werden.
- Hash-Funktionen sind Einwegfunktionen. Es ist rechnerisch unmöglich, für einen gegebenen Ausgangswert z einen Eingangswert x zu finden (Urbildresistenz).
- Kollisionsresistenz[26].

5.2 Digitale Signaturen

Das Ziel einer digitalen Signatur oder elektronischen Unterschrift ist es, einige wesentliche Eigenschaften der handschriftlichen Unterschrift in elektronischer Form zu realisieren. Dabei sollen die grundsätzlichen handschriftlichen Eigenschaften, wie die Echtheitseigenschaft, Identitätseigenschaft, Abschlusseigenschaft, Warneigenschaft und Verifikationseigenschaft übernommen werden.

Die Echtheitseigenschaft stellt sicher, dass das Dokument wirklich von demjenigen stammt, der die Unterschrift getätigt hat. Wobei ein enger Zusammenhang zwischen dem Dokument und der Unterschrift vorausgesetzt wird. Die Identitätseigenschaft stellt sicher, dass jede digitale Signatur persönlich ist und lediglich von einem einzigen Menschen ausgestellt werden kann. Die Abschlusseigenschaft signalisiert die Vollendung der Erklärung. Dies wird dadurch ausgedrückt, dass die Unterschrift am Ende der Erklärung steht. Durch die Verifikationseigenschaft kann ein Empfänger die Unterschrift verifizieren, etwa durch einen Unterschriftenvergleich. Die Warneigenschaft soll denjenigen, welcher die Unterschrift tätigt, vor einem voreiligen Unterzeichnen bewahren.

Mit Hilfe kryptographischer Mechanismen, wie zum Beispiel Hash-Funktionen, lassen sich die Eigenschaften auf die digitalen Signaturen übertragen. Somit ist eine Unterschrift in elektronischer Form sichergestellt. Ausgenommen hiervon ist lediglich die Warneigenschaft[27].

[26] Vgl. Paar & Pelzl, 2016, Seite 340 ff.
[27] Vgl. Beutelspacher, Schwenk, & Wolfenstetter, 2015, Seite 20 f.

6. Fazit

Die Wissenschaft der Kryptologie befindet sich in einem fortlaufenden Entwicklungsprozess. Die Anforderungen sind weiterhin steigend und aufgrund des Wandels der Gesellschaft hin zu einer Informationsgesellschaft, werden abermals Veränderungen gefordert.

Brandaktuelle Themen, wie zum Beispiel die Cyberkriminalität, untermauern die Notwendigkeit der Kryptologie. Diese negativen Schlagzeilen sollten die Menschen, aber auch die Industrien, sensibilisieren und den Fokus auf den Schutz und die Verschlüsselung der eigenen Daten richten[28].

Der mittels der Kryptographie unternommene Versuch, Daten über verschiedenste Verschlüsselungsmethoden geheim zu halten, dient der Absicherung des individuellen Rechts auf die Unantastbarkeit der Privatsphäre. Denn insbesondere diese gilt es im Datenrausch des Internets zu schützen, sei es bei Bestellungen, Bankgeschäften, beim normalen E-Mailverkehr oder beim generellen Surfen durch das Internet.

Die Industrie hat ebenfalls ein großes Interesse an der sicheren Kommunikation. Informationen und Daten legen den Grundstein für eine langfristige Existenz eines Unternehmens und diese gilt es zu schützen.

Ein Bericht des Axel Springer Verlags aus dem Magazin „Welt“ besagt, dass mittlerweile jedes zweite deutsche Unternehmen sabotiert und bestohlen wird. Dies geschieht im Rahmen der Cyberkriminalität auf unterschiedlichste Weisen. Jedoch ist hierbei die Wissenschaft der Kryptologie eine Möglichkeit, sich weiterzuentwickeln und sich in der Zukunft stärker zu schützen[29].

[28] Vgl. Bundesministerium des Innern, 2018
[29] Vgl. Heuzeroth, 2017

Literaturverzeichnis

Beutelspacher, A., Schwenk, J., & Wolfenstetter, K.-D. (2015). *Moderne Verfahren der Kryptographie* (Bd. 8.). Wiesbaden: Springer Spektrum Verlag.

Bundesministerium des Innern, f. B. (2018). *Bundesministerium des Innern, für Bau und Heimat*. Von https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html abgerufen

Heuzeroth, T. (21. Juli 2017). *Welt*. Von https://www.welt.de/wirtschaft/article166877297/Jedes-zweite-deutsche-Unternehmen-wird-sabotiert-und-bestohlen.html abgerufen

Paar, C., & Pelzl, J. (2016). *Kryptographie Verständlich.* Berlin, Heidelberg: Springer Vieweg Verlag.

Stobitzer, C. (Mai 2018). *Kryptowissen.* Von http://www.kryptowissen.de/kryptologie.html abgerufen

Stobitzer, C. (Mai 2018). *Kryptowissen*. Von http://www.kryptowissen.de/geschichte-der-kryptographie.html abgerufen

Swoboda, J., Spitz, S., & Pramateftakis, M. (2008). *Kryptographie und IT-Sicherheit.* Wiesbaden: Vieweg+Teubner Verlag.

Eidesstattliche Erklärung

„Ich erkläre an Eides Statt, dass ich die vorstehende Arbeit „Einführung in die Grundbegriffe der Kryptologie“ selbständig angefertigt und mich fremder Hilfe nicht bedient habe. Alle Stellen, die wörtlich oder sinngemäß veröffentlichtem oder nicht veröffentlichtem Schrifttum entnommen sind, habe ich als solche kenntlich gemacht.“

_____ _____

Ort, Datum Lukas Kirschnick