ASYMMETRISCHE VERSCHLÜSSELUNG

MARKUS BRUNSCH

Einführung in die asymmetrische Verschlüsselung

Januar 2021 – version 1.0

INHALTSVERZEICHNIS

Teil I

EINFÜHRUNG IN DIE KRYPTOGRAFIE

Verschlüsselung kann aus verschiedenen Gründen sinnvoll sein: Auf einem gemeinsam genutzten Computer kann sie Daten für die Mitbenutzer unlesbar machen. Gleiches gilt für Personen, die sich unberechtigt Zugang zu Ihrem Computer verschaffen. Informationen auf mobilen Geräten wie Notebooks und USB-Speichermedien geraten nicht in falsche Hände, wenn das Gerät gestohlen wird oder verloren geht und die Daten darauf verschlüsselt sind.[1]

1 https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Datenverschluesselung/datenverschluesselung_node.html

1 EINFÜHRUNG

1.1 GESCHICHTE DER KRYPTOGRAPHIE

ALTERTUM

Erste frühe Varianten waren Geheimnachrichten, die versteckt transportiert wurden.
So wurden beispielsweise in Ägypten Sklaven die Haare abrasiert, eine Nachricht eintätowiert und nachdem die Haare nachgewachsen waren, zum Empfänger geschickt. Eine weitere Variante waren kleine Löcher in Buchstabenform auf Papyrusrollen, die erst bei Gegenlicht dann sichtbar wurden.
Auch in Griechenland wurde bereits 500 v. Chr. ein Verschlüsselungsstab namens Skytale[1] entwickelt mit deren Hilfe Texte verschlüsselt werden konnten.

Julius Cäsar (etwa 100 v. Chr. bis 44 v. Chr.) soll die nach ihm benannte Cäsar-Chiffre [2] genutzt haben, die jeden Buchstaben im Alphabet um einen festgelegten Wert verschiebt.
Auszüge aus dem Paper von Hütter "Geschichte der Kryptographie''[4]

MITTELALTER

Al-KadiZwischen den Jahren 500 und 1400 gab es vor allem aus der arabischen Welt bedeutende Beiträge zur Kryptografie.[1]
In Europa soll Karl der Große als Verschlüsselungsmethode ein unbekanntes Alphabet in Verbindung mit einem Einsetzungsverfahren verwendet haben.

1 https://de.wikipedia.org/wiki/Skytale
2 https://de.wikipedia.org/wiki/Gaius_Iulius_Caesar

NEUZEIT

Zwischen dem 14. und 17. Jahrhundert hat die Kryptografie wie viele andere Wissenschaften einen großen Aufschwung. Die kaum veränderten Verfahren wurden in dieser Zeit weiterentwickelt.
Hier eine Auflistung der Innovationen dieser Zeit

- Chiffrierscheibe [3]
- Voynich-Manuskript [4]
- Beale-Chiffre [5]
- Dorabella-Chiffre [6]
- Weiterentwicklung durch Aufkommen der Telegrafie [7]

1.2 BEGRIFFLICHKEITEN

1.2.1 *Authentizität*

Beschreibt, dass eine Nachricht auch vom eigentlichen Absender verfasst und versendet wurde. Dies ist weniger ein Aspekt der Verschlüsselung, sondern eher vergleichbar mit einer Unterschrift oder einem Siegel. Authentizität dient dazu, seine Identität zu bestätigen. Richter's "*Verschlüsselung im Internet*" [6].

1.2.2 *Integrität*

Integrität ist der Nachweis darüber, dass die Nachricht auf dem Übertragungsweg nicht verändert oder manipuliert wurde. Die Integrität hängt von der Authentizität des Absenders ab, da nur mit der Grundlage des ëchtenÄbsenders die Sinnhaftigkeit einer Integritätsprüfung überhaupt aufkommt. Ist dies gegeben, kann anhand von digitalen Signaturen überprüft werden, ob die Nachricht in einer weise verändert worden ist. Dies geschieht dadurch, dass digitale Signaturen von der gesammten Nachricht abhängen. Richter's "*Verschlüsselung im Internet*" [6].

---

3 Chiffrierscheibe
https://de.wikipedia.org/wiki/Chiffrierscheibe
4 Voynich-Manuskript
https://de.wikipedia.org/wiki/Voynich-Manuskript
5 Beale-Chiffre
https://de.wikipedia.org/wiki/Beale-Chiffre
6 Dorabella-Chiffre
https://de.wikipedia.org/wiki/Dorabella-Chiffre
7 Kerckhoffs Prinzip
https://de.wikipedia.org/wiki/Kerckhoffs_Prinzip

1.2.3 *Vertraulichkeit*

Ziel ist es, eine Nachricht nur für berechtigte Personen zugänglich zu machen und zu verhindern, dass dritte sich unbefugt Zugriff zu der Nachricht verschaffen können.

1.2.4 *Verbindlichkeit*

Verbindlichkeit stelle eine eindeutige, nicht abstreitbare Zurückverfolgbarkeit der Nachricht zum Absender her. "*Motivation und Ziele der Informationssicherheit*" [5]

Teil II

ASYMMETRISCHE KRYPTOGRAFIE

In der asymmetrischen Kryptografie arbeitet man nicht mit einem einzigen Schlüssel, sondern mit einem Schlüsselpaar. Bestehend aus einem öffentlichen und einem privaten Schlüssel. Man bezeichnet diese Verfahren als asymmetrische Verfahren oder Public-Key-Verfahren.[8]

8 https://www.elektronik-kompendium.de/sites/net/1910111.htm

2 ASYMMETRISCHE VERSCHLÜSSELUNG

Ein großes Problem der Kryptografie ist der Schlüsselaustausch, hierfür bietet die asymmetrische Verschlüsselung eine Lösung.

2.1 PUBLIC KEY

Als Public Key wird der Teil des Schlüssel bezeichnet, der vom potenziellen Empfänger einer Nachricht frei zugänglich für jeden veröffentlich wird. Dieser Teil des Schlüssels wird vom Absender der Nachricht benötigt, denn mit diesem Schlüssel wird die Nachricht vor dem versenden verschlüsselt. Nach diesem Verschlüsselungsverfahren kann die Nachricht nur noch vom Empfänger mit dem Private Key gelesen (entschlüsselt) werden, nicht einmal der Empfänger kann jetzt noch auf die Daten zugreifen.

2.2 PRIVATE KEY

Als Private Key wird der Teil des Schlüssels bezeichnet, der nur dem Empfänger der Nachricht zur Verfügung steht und unter Verschluss gehalten wird. Dieser Schlüssel dient dazu, eingehende Nachrichten, die mit dem korrespondierenden Public Key verschlüsselt wurden, wieder zu entschlüsseln. Dies ist nur mit diesem Schlüssel möglich.

2.3 VOR UND NACHTEILE

Bei der asymmetrischen Verschlüsselung ergeben die folgenden Vorteile gegenüber einer symmetrischen Verschlüsselung:

- **Eliminierung des Schlüsselaustauschproblems**
  Bei der symmetrischen Verschlüsselung gibt es keinen sicheren Kanal zur Schlüsselübergabe, bei der asymmetrischen Verschlüsselung benötigt die Schlüsselübergabe keinen sicheren Übertragungskanal.[2]

- **Die Anzahl der benötigten Schlüssel ist geringer**
  Bei einer symmetrischen Verschlüsselung bräuchte jeder Benutzer von jedem Benutzer einen eigenen Schlüssel, bei dem asymmetrischen Verfahren reduziert sich die Schlüsselmenge auf je jeweilige Anzahl an Benutzern.[2]

- **Authentizität**
  Asymmetrische Verschlüsselung bietet zudem gegenüber der symmetrischen auch den Vorteil der Authentizität.

Nachteile, die sich durch die asymmetrische Verschlüsselung ergeben:

- **Ein erhöhter Rechenaufwand**
  im vergleich zur symmetrischen Kryptografie.

2.4 ABLAUF ASYMMETRISCHER VERSCHLÜSSELUNG

1. Erstellen eines Schlüsselpaares bestehend aus Public und Private Key.
2. Veröffentlichen des Public Keys.
3. Der Absender lädt sich den Public Key vom Empfänger.
4. Der Absender verschlüsselt die zu übertragenden Daten mit dem Public Key des Empfängers.
5. Der Empfänger ist nun in der Lage mithilfe seines passenden Private Keys die empfangene Nachricht zu entschlüsseln.

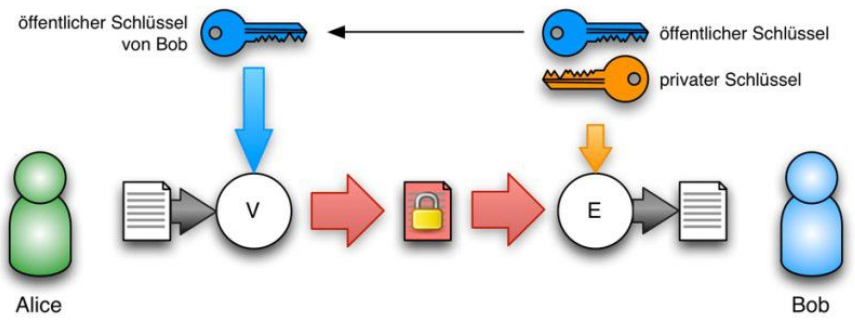

Abbildung 1: (V) Verschlüsseln
(E) Entschlüsseln

2.5 IMPLEMENTIERUNGEN ASYMMETRISCHER VERSCHLÜSSELUNG

- **S/MIME**
  steht für Secure Multipurpose Internet Mail Extension und ist ein Protokoll zum Verschlüsseln und Signieren von E-Mails.[3]

- **SSH**
  Secure Shell (SSH) ist eine Software, um Rechner remote zu steuern und zu verwalten. Dabei wird die Verbindung durch den Einsatz von Public Key Verfahren verschlüsselt, ganz im Gegensatz zu seinem Vorgänger Telnet dieser war unverschlüsselt.[3]

- **SSL**
  Secure Socket Layer (SSL) ist ein Protokoll, um TCP Verbindungen zwischen zwei Sockets zu verschlüsseln. Dabei kommt eine hybride Verschlüsselung zum Einsatz (mehr dazu später). SSL wurde später durch TLS (Transport Layer Security) abgelöst.[3]

- **VPN / IPsec**
  Virtual Private Networking und IP Security baut auf den Ideen und Grundlagen von SSL/TLS auf. Die Vorteile von IPsec beziehen sich auf die Verschlüsselung auf IP-Ebene (Layer 3) und nicht wie bei SSL/TLS auf Transport Ebene (Layer 4). Dadurch ist es IPsec möglich, den kompletten Datenverkehr eines Netzwerks zu verschlüsseln. Ebenfalls müssen bestehende Anwendungen nicht verändert werden da IPsec unter der Transport Schicht (Layer 4) arbeitet.[3]

3 HYBRIDE VERSCHLÜSSELUNG

Hier wird wie im Beispiel von TLS zuerst über eine asymmetrische Verschlüsselung ein sicherer Übertragungskanal aufgebaut im Anschluss werden temporäre symmetrische Schlüssel mit einer kurzen Lebenszeit generiert und über den sicheren Kanal verteilt. Im Anschluss wird dann mithilfe der symmetrischen Verschlüsselung weiter kommuniziert. Dadurch ergeben sich Performance Vorteile.

3.1 ABLAUF HYBRIDER VERSCHLÜSSELUNG

1. Erstellen eines Schlüsselpaares bestehend aus Public und Private Key.
2. Veröffentlichen des Public Keys.
3. Der Absender lädt sich den Public Key vom Empfänger.
4. Der Absender verschlüsselt die zu übertragenden Daten mit dem Public Key des Empfängers.
5. Der Empfänger ist nun in der Lage mithilfe seines passenden Private Keys die empfangene Nachricht zu entschlüsseln.
   Es besteht ein sicherer Übertragungskanal
6. Erstellung von Temporären Session Keys für eine symmetrische Verschlüsselung.
7. Übertragung des symmetrischen Keys über den sicheren Kanal.
8. Die Kommunikation wird nun über den symmetrischen Kanal geleitet.
9. Die asymmetrische Verbindung wird getrennt.

LITERATUR

[1] Ibrahim A Al-Kadi. *The origins of cryptology: The Arab contributions. In: Cryptologia*, 97–126. 1992.

[2] Jan Pelzl Christof Paar. *Kryptografie verständlich*. Springer Verlag, 2016.

[3] ekkehard LÖHMANN wolfgang ERTEL. *Angewandte Kryptographie*. Hanser, 2020.

[4] Arno Hütter. *Geschichte der Kryptographie*. 2000/2001. URL: https://www.oocities.org/siliconvalley/program/3996/pub/kryptographie.pdf.

[5] *Motivation und Ziele der Informationssicherheit*. 2020. URL: https://de.wikipedia.org/wiki/Informationssicherheit#Motivation_und_Ziele_der_Informationssicherheit.

[6] Helmut Richter. *Verschlüsselung im Internet*. 2002. URL: http://www.runway.ch/images/stories/dienstleistungen/m5%20verschluesselung%20im%20internet.pdf.

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both LaTeX and LyX:

https://bitbucket.org/amiede/classicthesis/

Dieses Paper ist unter der MIT Lizenz veröffentlicht der Quellcode ist auf GitHub abrufbar.

https://github.com/BackInBash/Technikerschule/tree/master/Jahr%201/WIA/Verschl%C3%BCsselung