Lorenz Faber

FTI1 | it.Schule Stuttgart

Exposee

Ein Paper über die symmetrische Kryptographie, welche eine kurze Einführung, die Geschichte, Erklärung der Verfahren und Vor- bzw. Nachteile beinhaltet.

Asymmetrische Verschlüsselung

Public-Key Verfahren

Inhaltsverzeichnis

[1 Einführung 1](#_Toc61878780)

[2 Geschichte 1](#_Toc61878781)

[3 Prinzip 2](#_Toc61878782)

[4 Das RSA-Verfahren 2](#_Toc61878783)

[4.1 Schlüsselerzeugung 3](#_Toc61878784)

[5 Anwendungsfälle 3](#_Toc61878785)

[5.1 3](#_Toc61878786)

[6 Literaturverzeichnis 3](#_Toc61878787)

# Einführung

“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.”  
– Edward Snowden

Dieses Zitat von Edward Snowden, einem der größten und meistgesuchten Whistleblower und ehemaliger CIA-Mitarbeiter beschreibt, wie wichtig es ist, dass Kryptographie stark genug ist und verlässlich sein muss. Viele Verschlüsselungstechniken standen in der Vergangenheit in der Kritik, jedoch nicht alle Verfahren der Kryptographie wurden als nicht mehr sicher eingestuft. Die verschiedenen asymmetrischen Kryptographie-Verfahren gelten noch bis heute als sehr sicher. [[1]](#footnote-1)

Ende der 1970iger Jahre wurden sie entwickelt, da es in großen Kommunikationsnetzwerken als sehr aufwendig oder gar unmöglich galt, einen Schlüssel, welcher zur Ver- und Entschlüsselung verwendet wurde, sicher auszutauschen (symmetrische Verschlüsselungsverfahren). [[2]](#footnote-2)

Die Frage, warum dennoch auch symmetrische Verschlüsselungsverfahren heutzutage noch verwendet werden ist berechtigt und kann wie folgt beantwortet werden: Weil die asymmetrischen Verschlüsselungsverfahren viel langsamer sind als die komplexesten symmetrischen Verschlüsselungsverfahren. Es gibt eine Mischform, die „hybride Verschlüsselung“, welche die Vorteile aus beiden Verfahren nutzt - Dazu aber später mehr.[[3]](#footnote-3)

# Geschichte

Das asymmetrische Verschlüsselungsverfahren gibt es noch nicht so lange und wurde erst 1975 veröffentlicht. Die symmetrische Verschlüsselung existiert hingegen schon seit über 2000 Jahren und kam erstmals zur Zeit des großen Cäsars auf.[[4]](#footnote-4) Diffie und Hellmann hatten die Idee zur asymmetrischen Verschlüsselung. Ein erstes fertiges Verfahren gab es aber erst 1977, also zwei Jahre später und wurde von **R**ivest, **S**hamir und **A**dleman konzipiert und veröffentlicht. Dieser Algorithmus, welcher nach den ersten Buchstaben der Erfinder benannt wurde (RSA) wird noch heute oft angewendet. [[5]](#footnote-5) Auch in den Jahren danach kamen immer mehr Verfahren hinzu.

# Prinzip

Im Vergleich zu dem symmetrischen Verschlüsselungsverfahren werden bei der asymmetrischen Verschlüsselung zwei Schlüssel, ein sogenanntes Schlüsselpaar, anstatt einem Schlüssel verwendet. Der Ablauf ist folgender:

Zuerst wird das Schlüsselpaar generiert, welches einen privaten und einen öffentlichen Schlüssel enthält. Hierbei ist zu erwähnen, dass der private Schlüssel sich nicht aus dem öffentlichen Schlüssel berechnen lassen darf.[[6]](#footnote-6) Der öffentliche Schlüssel wird, wie der Name schon sagt, veröffentlicht. Dies kann zum Beispiel per direkter Nachricht wie einer Mail oder auch einem Server erfolgen. Bei dieser Vorgehensweise fällt auf, im Vergleich zu der symmetrischen Verschlüsselung, dass dieser Schlüssel nicht über einen sicheren Weg übertragen werden muss und jeder diesen besitzen dürfte. Öfter hofft man auch auf eine Globale Verteilung des öffentlichen Schlüssels, damit kein zweiter, gefälschter Schlüssel verbreitet wird.

Wer nun also den öffentlichen Schlüssel hat, kann seine Nachricht an den Empfänger mit diesem verschlüsseln. Die Nachricht kann ausschließlich mit dem geheimen Schlüssel entschlüsselt und angeschaut werden. Der geheime Schlüssel hat nur der Ersteller des öffentlichen Schlüssels und somit der letztendliche Empfänger.

Es ist sehr wichtig, dass der geheime, private Schlüssel nur der Empfänger hat, denn jeder der diesen Schlüssel hat kann auch alle Nachrichten entschlüsseln, die von anderen mit dem öffentlichen Schlüssel verschlüsselt und versendet wurden. [[7]](#footnote-7)

Abb1.: Ablauf der Asymmetrischen Verschlüsselung, Lorenz Faber

# Das RSA-Verfahren

Wie in der Geschichte schon bereits erwähnt ist das RSA-Verfahren einer der ersten und bis heute bekanntesten Verfahren. Die Grundfunktionsweise besteht daraus, große Zahlen in ihre Primfaktoren zu zerlegen. Da dies eine komplexe Vorgehensweise ist, besteht auch darin die Schwierigkeit dieses Verfahren zu knacken bzw. zu umgehen.[[8]](#footnote-8)

## Schlüsselerzeugung

Der Schlüsselerzeugungsalgorithmus des RSA-Verfahrens generiert zwei Primzahlen mit einer fest definierten Bit-Länge.

# Anwendungsfälle

Das Asymmetrische Verschlüsselungsverfahren wird heutzutage sehr oft und vielseitig angewendet.[[9]](#footnote-9)

* Emailverkehr (OpenPGP oder S/MIME)
* Protokolle (SSH oder https)
* Digitale Signaturen (zur Authentizitätsprüfung und Verifizierung)

## 

# Literaturverzeichnis

1. ZITATE AUS IT-SICHERHEIT UND HACKING in itsicherheitonline.de, [online] <https://itsicherheitonline.de/zitate-aus-it-sicherheit-und-hacking/>, [18.01.2021]
2. Johannes Buchmann: Einführung in die Kryptographie, 6. Auflage Dezember 2015 ISBN 978-3-642-39774-5
3. Asymmetrische Kryptografie (Verschlüsselung) in elektronik-kompendium.de, [online] <https://www.elektronik-kompendium.de/sites/net/1910111.html> , [18.01.2021]
4. Asymmetrische Verschlüsselung in stufyflix.de, [online] <https://studyflix.de/informatik/asymmetrische-verschlusselung-1609> [18.01.2021]
5. Asymetrische Verschlüsselung in kryptowissen.de, [online] <https://www.kryptowissen.de/asymmetrische-verschluesselung.html> [18.01.2021]

1. [1], Absatz 3 [↑](#footnote-ref-1)
2. [2] Kapitel 3.3 [↑](#footnote-ref-2)
3. [2], Kapitel 3.3 [↑](#footnote-ref-3)
4. [5], Absatz 2 [↑](#footnote-ref-4)
5. [4], Absatz 4 [↑](#footnote-ref-5)
6. [2], Kapitel 8.1 [↑](#footnote-ref-6)
7. [5], Absatz 3 [↑](#footnote-ref-7)
8. [2], Kapitel 8.3 [↑](#footnote-ref-8)
9. [4], Absatz 10 [↑](#footnote-ref-9)