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

[Einführung 1](#_Toc61863540)

[Literatur 2](#_Toc61863541)

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. 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 Rivest, Shamir und Adleman konzepiert und veröffentlicht.[[4]](#footnote-4)

# Literatur

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]

1. Vgl. Zitate aus IT-Sicherheit und Hacking, Absatz3 [↑](#footnote-ref-1)
2. Vgl. Einführung in die Kryptographie, Kapitel 3.3 [↑](#footnote-ref-2)
3. Vgl. Einführung in die Kryptographie, Kapitel 3.3 [↑](#footnote-ref-3)
4. Vgl. Asymmetrische Verschlüsselung, Absatz 4 [↑](#footnote-ref-4)