Asymmetrische Kryptographie in Java

Norman Vetter

Seminar „Sichere verteilte Anwendungen mit Java“

Universität Potsdam

Wintersemester 2012/13

Inhaltsverzeichnis

1 Einleitung

So sieht eine Section aus!

2 Theoretische Grundlagen

2.1 Ziele

Ein kryptographisches System dient zum verschlüsseln und entschlüsseln von Texten und anderen Daten, um deren Inhalt vor Dritten geheim zu halten. Genauer gibt ein Kryptosystem an wie ein Klartext in einen von Dritten nicht lesbaren Kryptotext umgewandelt werden kann. Und wie dieser Kryptotext später wieder in einen lesbaren Klartext transformiert wird. Anders als die Steganografie zielt die Kryptographie darauf ab lediglich den Inhalt einer Nachricht zu verschlüsseln, nicht aber deren Existenz zu verbergen. Die asymmetrische Kryptographie ist eines dieser kryptographischen Systeme.

2.2 Asymmetrische Kryptographie

Die asymmetrische Kryptographie wurde Mitte 1970 von Ralph Merkle sowie Diffie und Hellmann entwickelt. Sie beruht auf der Idee zur Kommunikation zwischen 2 Instanzen ein Schlüsselpaar zu verwenden. Dieses Schlüsselpaar besteht aus dem privaten und dem öffentlichen Schlüssel. Zur Kommunikation muss im vornherein ein gegenseitiger Austausch des öffentlichen Schlüssels erfolgt sein, denn die zu schickende Nachricht ist vom Sender mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln. Nach Empfang entschlüsselt der Empfänger nun die Nachricht mit seinem eigenen privaten Schüssel. Im Falle einer Antwort verschlüsselt der ehemalige Empfänger (nun Sender) seine Nachricht wieder mit dem öffentlichen Schlüssels seines Gegenüber. Welcher die Entschlüsselung erneut mit dem eigenen privaten Schlüssel durchführen muss. Somit ist während der Kommunikation kein erneuter Austausch eines sicheren Schlüssels notwendig, und auch erneute Kommunikationen können mit den bereits vorhandenen Schlüsseln durchgeführt werden. Wichtig ist hierbei jedoch, dass die Sicherheit des privaten Schlüssels und die Authentizität des öffentlich Schlüssels gewährleistet ist. Mehr dazu in den folgenden Kapiteln.

2.3 Grundlage asymmetrischer Systeme

Im obigen Szenario haben wir gesehen wie ein grober Kommunikationsablauf zwischen 2 Parteien aussieht. Folgende Grafik (nach [Eck13]) veranschaulicht dies in Bezug auf kryptographische Systeme im Allgeinen:

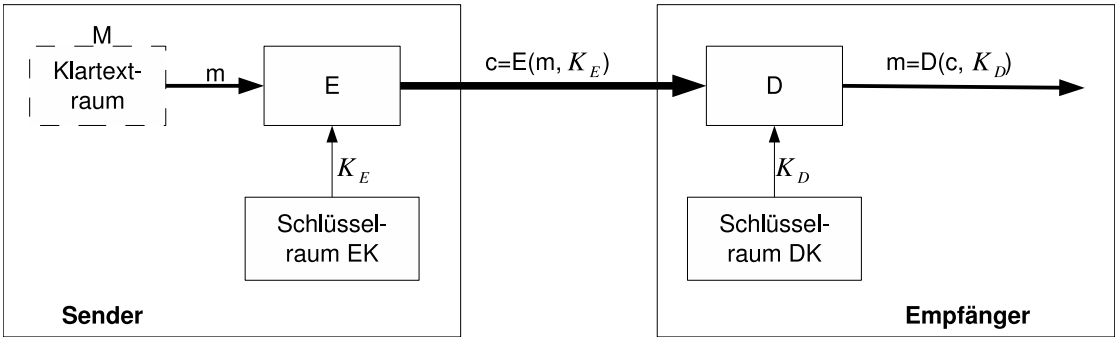

Abbildung 1: Komponenten eines Kryptosystems

- Tupel = (M, C, EK, DK, E, D)
- 2 endliche Alphabete (A_1, A_2)
- Menge von Klartexten $(M \subseteq A_1^* \backslash \emptyset)$
- Klartext $(m \in M)$
- Menge von Kryptotexten $(C \subseteq A_2^* \backslash \emptyset)$
- Kryptotext $(c \in C)$
- Verschlüsselungsschlüsselraum $(EK \backslash \emptyset)$
- Entschlüsselungsschlüsselraum $(DK/\emptyset$ $mit\ f : EK \rightarrow DK$ $und\ f(K_E) = K_D)$
- Verschlüsselungsverfahren $(E: \ MxEK \rightarrow C)$
- Entschlüsselungsverfahren $(D: \ CxDK \rightarrow M)$
- Es gilt: $\forall m \in M : D(E(m, K_E), K_D) = m$

2.3.1 Vetreter

2.3.2 Verschlüsselung und Endschlüsselung

2.3.3 Schlüsselmanagement

2.4 Hybride Kryptographie

3 Kryptographie mit Java

3.1 So wird zitiert

Ein spannender Artikel ist [**?**]. Lesenswert ist auch [**?**]

4 Eine section mit eingebundener Abbildung

In Abbildung 1 wird ... dargestellt. Es folgt eine ausführliche Beschreibung:

5 Zusammenfassung

Zum Schluss bitte eine Zusammenfassung!

Literatur

[Eck13] Claudia Eckert. *IT-Sicherheit : Konzepte - Verfahren - Protokolle*. Oldenburg, 2013.