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 von 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 Vorhinein ein gegenseitiger Austausch des öffentlichen Schlüssels erfolgt sein, denn die zu schickende Nachricht ist vom Sender mit dem öffentlichen Schlüssel des Empfängers in einen Kryptotext um zu wandeln. 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 öffentlichen 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 Zwei Parteien aussieht. Dieses wird in folgender Grafik (nach [Eck13]) veranschaulicht:

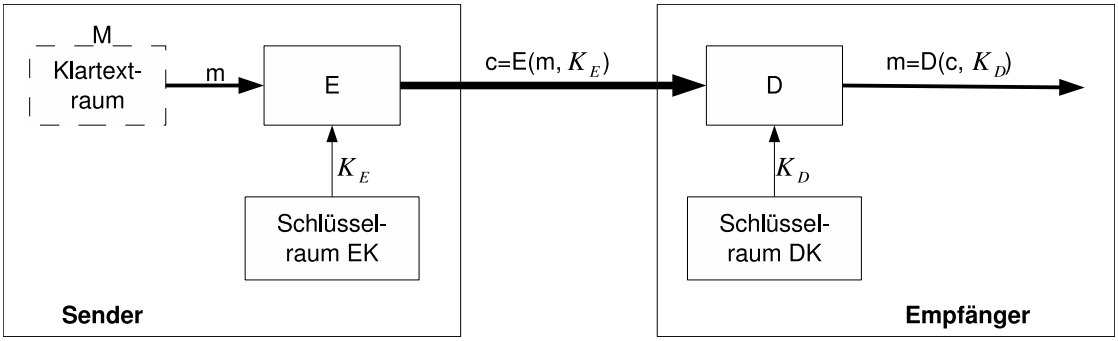

Abbildung 1: Komponenten eines Kryptosystems

1. Tupel
   (M, C, EK, DK, E, D)
2. 2 endliche Alphabete
   (A_1, A_2)
3. Menge von Klartexten
   $(M \subseteq A_1^* \backslash \emptyset)$
4. Klartext
   $(m \in M)$
5. Menge von Kryptotexten
   $(C \subseteq A_2^* \backslash \emptyset)$
6. Kryptotext
   $(c \in C)$
7. Verschlüsselungsschlüsselraum
   $(EK \backslash \emptyset)$
8. Entschlüsselungsschlüsselraum
   $(DK/\emptyset$
   $mit\ f : EK \to DK$
   $und\ f(K_E) = K_D)$
9. Verschlüsselungsverfahren
   $(E :\ MxEK \to C)$
10. Entschlüsselungsverfahren
    $(D :\ CxDK \to M)$
11. Es gilt:
    $\forall m \in M : D(E(m, K_E), K_D) = m$

Die Eigenschaft (11.) der Obigen Legende zeigt uns das Zusammenspielt unserer einzelnen Komponenten. Wird ein Klartext m mit einem Schlüssel $K_E \in EK$ durch ein kryptographisches Verfahren E in einen Kryptotext umgewandelt. So ist gegeben das dieser Kryptotext unter Verwendung des zu K_E gehörigen Schlüssels $K_D \in DK$, und des kryptographischen Verfahrens D wieder in den ursprünglichen Klartext m umgewandelt werden kann. Damit dies gegeben ist muss unser asymmetrisches Kryptosystem einige wichtige Punkte erfüllen. Es muss:

- eine effiziente Möglichkeit zur Erzeugung von Schlüsselpaaren (K_E, K_D) geben.
- garantiert sein das der Private (K_D) nicht effizient aus dem öffentlichen Schlüssel (K_E) gebildet werden kann.
- möglich sein effizient zu Ver-. und Entschlüsseln.

Um dies zu erreichen nutzen wir Einwegfunktionen.

2.3.1 Einwegfunktionen

Einwegfunktionen sind besondere Funktionen $(f : X \to Y)$ bei denen das Urbild (X) nicht unter vertretbarem, zeitlichem Aufwand aus dem Bild (Y) zu berechnen ist. Mathematische Probleme welche derartige Funktionen bilden sind unter Anderem das Faktorisierungproblem und der Diskrete Algorithmus. Es ist nicht bewiesen das die Umkehrung nicht möglich ist, jedoch Übersteigt die Komplexität der Berechnung unser heutiges Vermögen diese in einer vertretbaren Zeitspanne zu lösen.

Bei der Verwendung von normalen Einwegfunktionen in einem Kryptosystem wäre zwar die Sicherheit der Daten garantiert, jedoch stellt die Umkehrung selbst für autorisierte Personen ein unüberwindbares Hindernis dar. Wir benötigen zum Entschlüsseln unserer Daten eine Hintertür. Die so genannte Falltür. Einwegfunktionen mit Falltür bieten eine Identische Sicherheit wie normale Einwegfunktionen, und zudem die Option verschlüsselte Daten unter Kenntnis eines Geheimnisses (bei und der private oder öffentliche Schlüssel) zu entschlüsseln. Mathematische Probleme mit Falltür sind zum Beispiel die h-te Potenz modulo(n) oder der Zusammengesetzte modulo(n) ([Eck13]).

2.3.2 RSA

2.3.3 Verschlüsselung und Endschlüsselung

2.3.4 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.