Trennung von Ver- und Entschlüsseln mittels Einwegfunktion

Grundlegend für die asymmetrische Kryptographie sind Einwegfunktionen mit Falltür. Einwegfunktionen sind dadurch charakterisiert, dass sie leicht berechenbar sind, ihre Umkehrfunktion aber nur mit riesigem Rechenaufwand bestimmt werden kann. Ein klassisches Beispiel dafür ist ein Telefonbuch: Während die Telefonnummer leicht zu finden ist, wenn man den Namen kennt, ist das Auffinden des Namens sehr schwer, wenn nur die Telefonnummer bekannt ist. Auch das Zerreißen ein eines Blatts Papier lässt sich leicht durchführen, das Zusammenfügen der zerrissenen Teile ist dagegen für den Restaurator eine anspruchsvolle Aufgabe.

Bei einer Einwegfunktion mit Falltür (kurz: Falltürfunktion) gibt es sozusagen eine „Hintertür", mit deren Kenntnis die Umkehrfunktion wiederum leicht zu bestimmen ist. Ein Beispiel dafür ist ein Briefkasten: Während das Einwerfen eines Briefes leicht geschieht, ist es schwer, ihn danach wieder herauszufischen – es sei denn, man hat den Schlüssel zum Briefkasten. In dieser Stunde werden Vorhängeschlösser als ein Beispiel für eine Falltürfunktion eingesetzt. Auch hier ist es einfach, ein Schloss durch Zudrücken zu schließen, das Schloss ohne Schlüssel zu öffnen ist allerdings aufwändig.

Zur Einführung in die asymmetrische Kryptographie wird den Schülerinnen und Schülern der Arbeitsauftrag erteilt, ein Geheimnis mittels einer Kiste zu übertragen, wobei jeder Kommunikationspartner über ein Vorhängeschloss mit passendem Schlüssel verfügt. Damit können sie selbstständig erarbeiten, wie durch eine Trennung von Ver- und inverser Entschlüsselungsfunktion das übermitteln geheimer Schlüssel vermieden werden kann:

Die Schülerinnen und Schüler teilen sich sich in zwei Gruppen, um ein Rollenspiel durchzuführen. Jede Gruppe erhält ein Vorhängeschloss, eine der Gruppen zusätzlich einen Karton/Truhe. Die Gruppen erhalten die Aufgabe, eine Nachricht in dem Karton an die andere Gruppe zu versenden. Dabei muss der Karton den in der Mitte platzierten Lehrer passieren, ohne dass dieser die Möglichkeit hat, die Nachricht zu lesen.

Die Lösung dieses Problems kann mit verschiedenen Verfahren gelöst werden. Im Diffie-Helmann-Schlüsseltausch schließt die versendende Gruppe den Karton, in dem die Nachricht liegt, mit ihrem Schloss zu und schickt ihn zur anderen Gruppe. Diese Gruppe befestigt ihr Schloss ebenfalls am Karton und schickt ihn wieder zum ursprünglichen Sender zurück. Dieser entfernt nun sein Schloss und sendet den Karton zurück, der nun geöffnet werden kann. Bei dem Diffie-Hellman-Schlüsseltausch handelt es sich nicht um ein vollwertiges asymmetrisches Verschlüsselungsverfahren. Es ist nicht gegen „man-in-the-middle"-Angriffe geschützt, so kann eine übermittelnde Station die Antworten der Kommunikationspartners imitieren und seinen eigenen Schlüssel anstatt denen der Kommunikationspartner übermitteln um so Kenntnis von der übertragenen Botschaften zu erlangen. Der amerikanische Mathematiker ElGamal entwickelt 1985 aus dem Diffie-Hellman-Verfahren ein vollwertiges asymmetrisches Kryptosystem, das auch noch heute verwendet wird.

Um zu verdeutlichen, dass dieses Verfahren auch Angriffsmöglichkeiten bietet und die Lösung des Schlüsseltauschproblems nicht 100%ige Sicherheit bietet, kann das Szenario erneut durchgeführt werden. Diesmal befestigt der Lehrer/die Lehrerin jedoch ein eigenes Schloss an dem Karton und sendet ihn sofort an die sendende Gruppe zurück. Diese entfernt nun korrekterweise ihr Schloss und versendet den Karton erneut. Der Lehrer/die Lehrerin hat nun die Möglichkeit, die Nachricht zu lesen. Gleichzeitig nimmt der Lehrer/die Lehrerin einen baugleichen Karton, der eine eigene Nachricht enthält und sendet ihn – anstatt des Originals – weiter. Der falsche Karton wird durch die Schülerinnen und Schüler mit einem Schloss versehen und an den Lehrer / die Lehrerin zurück geschickt. Nun entfernt er/sie sein/ihr eigenes Schloss und sendet den Karton sogleich zurück (man-in-the-middle-Angriff).

Die Modellierung Diffie-Hellman-Verfahren auf der Ebene von Kisten und Schlössern trennt nicht zwischen privatem und öffentlichem Schlüssel und ist daher für die Anbahnung des RSA-Verfahrens ungeeignet. Entdecken die Schülerinnen und Schüler das Diffie-Hellman-Verfahren, so sollte durch die Demonstration des man-in-the-middle Angriffs eine weitergehende Überlegung

motiviert werden, wie sich ein Austausch der Schlösser verhindern lässt. Hier sollte der Lehrer/die Lehrerin das Szenario gezielt erweitern und ein Treffen der Kommunikationspartner zur Vorbereitung der späteren Kommunikation vorschlagen, wobei nach wie vor keine geheimen Informationen ausgetauscht werden sollen. Es bietet sich an, dass die Gruppen im Vorfeld der Kommunikation ihre Schlösser austauschen (die dann die öffentlichen Schlüssel symbolisieren) und dabei die zum Aufschließen notwendigen Schlüssel (die privaten Schlüssel im Sinne der asymmetrischen Kryptologie) behalten. Nun kann die Kiste direkt von der sendenden Gruppe mit dem Schloss der empfangenden Gruppe verschlossen und nur von der empfangenden Gruppe wieder geöffnet werden.

Abschließend sollten die Schülerinnen und Schüler aufgefordert werden, das zuletzt beschriebene Verfahren schriftlich festzuhalten und die Trennung von Ver- und Entschlüsslungsfunktion als zentrale Idee der Lösung zu benennen.

Material

- 2 Kisten, an denen sich je 2 Vorhängeschlösser anbringen lassen
- 3 Vorhängeschlösser mit Schlüssel (je für Gruppe 1, Gruppe 2, Lehrer)
- Folie mit Arbeitsauftrag Asymmetrisch verschlüsseln ohne Austausch geheimer Informationen am Beispiel Vorhängeschloss