Ein Rollenspiel zum Verschlüsseln

von Michael Fothe

In diesem Beitrag wird ein Rollenspiel beschrieben, das im Rahmen eines Thüringer Projekts zur Schulentwicklung am Friedrichgymnasium Altenburg erprobt und in einem Workshop auf der INFOS 2005 der Fachöffentlichkeit vorgestellt wurde (vgl. Fothe u. a., 2005).

Ausgangssituation

Anna und Bert wollen sicher kommunizieren. Sie verwenden dazu ein symmetrisches Verschlüsselungsverfahren. In einer ersten Szene erzeugt Anna einen Sitzungsschlüssel und sendet diesen an Bert. Mit diesem Schlüssel werden die Nachrichten ver- und entschlüsselt. Weitere Szenen stellen mögliche Angriffe von dritter Seite und Abwehrmaßnahmen dagegen dar. Dabei wird ein asymmetrisches Verschlüsselungsverfahren eingesetzt. Die Szenen des Rollenspiels werden von Anna, Bert, Clara, Dirk und einer Schülerin bzw. einem Schüler, die bzw. der ein Trustcenter darstellt, aufgeführt. Dabei kommen die farbigen Karten der Größe DIN A4 zum Einsatz, die von der Lehrperson bereitgestellt und in der Tabelle 1 wiedergegeben werden.

Die Karten dienen der Visualisierung und stellen eine Kommunikationshilfe dar. Zu Beginn einer Szene wählen die Schülerinnen und Schüler die richtigen Karten aus und bringen diese in die richtige Reihenfolge (meist: Text, Vorgang, Schlüssel, Text). Beim Erläutern der Vorgänge halten die Schüler die Karten wie beim Kartenspiel – jedoch deutlich sichtbar für ihre Mitschüler. Benötigte Schlüssel und Texte werden von dem einem zu einem anderen Akteur „physisch“ übergeben.

Das Rollenspiel ist für den Informatikunterricht der gymnasialen Oberstufe vorgesehen. Die nachfolgend beschriebenen Szenen können beim Erarbeiten der verschiedenen Verfahren isoliert aufgeführt werden. Möglich ist auch die Aufführung aller Szenen nacheinander in einer Festigungsphase. Das Rollenspiel soll das Verstehen sowohl einfacher als auch komplexer Handlungsabläufe fördern, die beim Thema „Verschlüsseln“ auftreten. Die Mitschüler von Anna, Bert, Clara, Dirk und dem „Trustcenter“ stellen Fragen zum Ablauf. Sie hinterfragen Ungenauigkeiten und Fehler und schlagen Varianten für das Rollenspiel vor. Die Durchführung des Rollenspiels soll gruppendynamische Lernprozesse und kooperatives Lernen anregen und ermöglichen.

Die nachfolgenden Regeln für das Rollenspiel sind weniger strikt formuliert. Dies ermöglicht den Akteuren auch autonomes und nicht determiniertes Handeln. Das Thema „Verschlüsseln“ darf im Informatikunterricht nicht nur auf das Rollenspiel reduziert werden. Die Schülerinnen und Schüler sollen u. a. auch ein Computerprogramm für ein einfaches Verschlüsselungsverfahren entwerfen und implementieren.

Art	Farbe	Aufschrift	
Vorgänge	rot	Verschlüsseln	
		Entschlüsseln	
		Signieren	
		Überprüfen	
		Hash-Wert berechnen	
		Hash-Werte vergleichen	
Texte	gelb	K	Klartext
		K_V	verfälschter Klartext
		K_S	signierter Klartext
		H_K	Hash-Wert vom Klartext
		H_{KS}	signierter Hash-Wert vom Klartext
		G	Geheimtext
		G_V	verfälschter Geheimtext
Schlüssel	grün	S	Sitzungsschlüssel
		$S_{AÖ}$	öffentlicher Schlüssel von Anna
		$S_{AÖZ}$	öffentlicher Schlüssel von Anna – zertifiziert
		S_{AP}	privater Schlüssel von Anna
		$S_{BÖ}$	öffentlicher Schlüssel von Bert
		$S_{BÖZ}$	öffentlicher Schlüssel von Bert – zertifiziert
		S_{BP}	privater Schlüssel von Bert
		$S_{CÖ}$	öffentlicher Schlüssel von Clara
		$S_{CÖZ}$	öffentlicher Schlüssel von Clara – zertifiziert
		S_{CP}	privater Schlüssel von Clara
		$S_{DÖ}$	öffentlicher Schlüssel von Dirk
		$S_{DÖZ}$	öffentlicher Schlüssel von Dirk – zertifiziert
		S_{DP}	privater Schlüssel von Dirk
		$S_{TÖ}$	öffentlicher Schlüssel vom Trustcenter
		S_{TP}	privater Schlüssel vom Trustcenter

Tabelle 1: Die benötigten farbigen DIN-A4-Karten.

Die 1. bis 4. Szene

Für das Rollenspiel werden nachfolgend fünf Szenen näher beschrieben.

1. Szene
Anna und Bert wollen sicher kommunizieren. Sie verwenden dazu ein symmetrisches Verschlüsselungsverfahren. Anna sendet einen Sitzungsschlüssel S an Bert. Mit diesem Schlüssel werden die Nachrichten ver- und entschlüsselt.

Anna übergibt Bert die Karte mit dem Sitzungsschlüssel S. Dann erläutert sie das Verschlüsseln des Klartexts K mit dem Sitzungsschlüssel S zum Geheimtext G (siehe Bild 1).

Anna übergibt Bert die Karte mit dem Geheimtext G. Bert erläutert das Entschlüsseln anhand der in Bild 2 wiedergegebenen Karten.

2. Szene
Clara greift beim Senden des Sitzungsschlüssels S von Anna nach Bert an. Sie fängt den Schlüssel ab, liest ihn und leitet ihn an Bert weiter. Clara kann nun alle Nachrichten im Klartext mitlesen oder sogar verfälschen.

3. Szene
Für den sicheren Transport des Sitzungsschlüssels S wird ein asymmetrisches Verschlüsselungsverfahren verwendet. Anna bittet Bert um Zusendung seines öffentlichen Schlüssels $S_{BÖ}$, verschlüsselt den Klartext (also den Sitzungsschlüssel S) mit diesem Schlüssel und sendet den erhaltenen Geheimtext an Bert. Bert entschlüsselt den Geheimtext mit seinem privaten Schlüssel S_{BP} und kennt nun den Klartext (d. h. den Sitzungsschlüssel S).

4. Szene
Dirk greift beim Senden des Schlüssels $S_{BÖ}$ von Bert nach Anna an. Er fängt den Schlüssel ab und sendet Anna seinen eigenen öffentlichen Schlüssel $S_{DÖ}$. Anna erhält den Schlüssel und denkt, dass es der öffentliche Schlüssel von Bert ist. Sie verschlüsselt den Klartext mit dem Schlüssel $S_{DÖ}$ und sendet die Nachricht zu Bert. Dirk fängt die Nachricht ab und entschlüsselt sie mit dem Schlüssel S_{DP}. Er liest den Klartext und kann ihn sogar verändern. Dann verschlüsselt er den Klartext mit $S_{BÖ}$ und sendet den Geheimtext an Bert. Bert entschlüsselt mit dem Schlüssel S_{BP}. Anna und Bert merken von Dirks Machenschaften nichts.

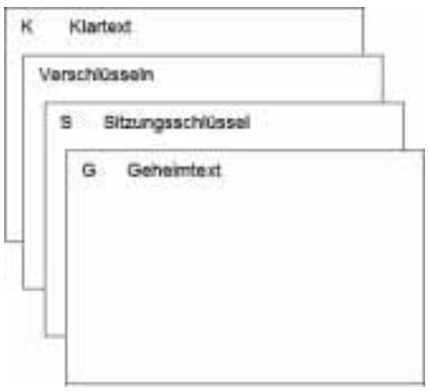

Bild 1: Benötigte Karten der ersten Szene (Veschlüsseln).

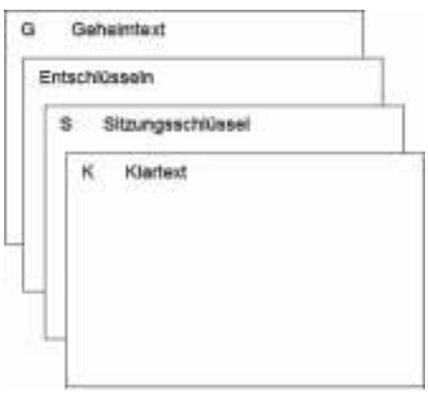

Bild 2: Das Entschlüsseln wird von Bert anhand dieser Karten erklärt.

Signieren und Überprüfen

Vor der 5. Szene wird die digitale Signatur thematisiert. Das Signieren eines Klartexts K durch Bert wird mit den in Bild 3 wiedergegebenen Karten beschrieben.

Bert sendet den signierten Klartext K_S nach Anna.

Anna überprüft nun, ob alles mit rechten Dingen zugegangen ist. Dabei werden die im Bild 4 (nächste Seite) wiedergegebenen Karten genutzt.

Wenn beim Überprüfen ein sinnvoller Klartext entsteht, so kann davon ausgegangen werden, dass kein erfolgreicher Angriff stattgefunden hat.

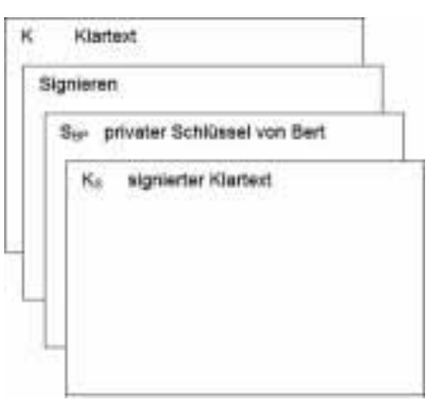

Bild 3: Die Karten für das Thema „Digitale Signatur“.

Bild 4: Der signierte Klartext wird von Anna überprüft.

Folgerichtig (vom Rechenaufwand her) ist nicht das Signieren des Klartexts, sondern das Signieren des Hash-Werts vom Klartext (siehe Bild 5). Der Hash-Wert wird mit einer Einweg-Hash-Funktion berechnet. Solche Funktionen bilden eine Zeichenfolge variabler Länge auf eine Zeichenfolge fester Länge ab. Die Funktion f ist eine Einweg-Hash-Funktion, wenn sich f(x) leicht und $f^{-1}(x)$ praktisch nicht berechnen lässt. Bei einer Einweg-Hash-Funktion ist es praktisch unmöglich, zwei Zeichenfolgen zu finden, die den gleichen Hash-Wert haben. Wird eine Zeichenfolge geringfügig verändert, so hat dies eine beträchtliche Änderung des Hash-Werts zur Folge (siehe auch Kasten „Hash-Wert“, nächste Seite).

Bert verschickt den Klartext K und den signierten Hash-Wert H_{KS} vom Klartext (das ist die digitale Signatur) an Anna. Anna überprüft die digitale Signatur und erhält dabei den Hash-Wert H_K vom Klartext. Sie berechnet den Hash-Wert des erhaltenen Klartexts K neu und vergleicht dann diesen mit dem übermittelten Hash-Wert (siehe Bild 6).

Eine Variante ist das zusätzliche Verschlüsseln des Klartexts zusammen mit der digitalen Signatur. Nur der dabei entstehende Geheimtext wird verschickt.

Die 5. Szene

5. Szene
Anna benötigt den öffentlichen Schlüssel $S_{BÖ}$ von Bert unverfälscht. Um dies zu garantieren, lässt ihn Bert von einem Trustcenter zertifizieren. Er sendet an Anna seinen zertifizierten Schlüssel $S_{BÖZ}$. Anna überprüft das Zertifikat und kann dann sehr sicher sein, dass sie wirklich den öffentlichen Schlüssel von Bert besitzt.

Diese Szenenbeschreibung wird in folgende Schritte umgesetzt:

Bert sendet seinen öffentlichen Schlüssel $S_{BÖ}$ zu einem Trustcenter. Das Trustcenter überprüft die Authentizität von Bert und zertifiziert dann seinen Schlüssel. Das Zertifizieren erfolgt durch Signieren mit dem privaten Schlüssel S_{TP} (siehe Bild 7).

Bild 5: Einführung eines Hash-Werts.

Bert erhält vom Trustcenter seinen zertifizierten öffentlicher Schlüssel $S_{BÖZ}$. Er sendet diesen nach Anna. Anna überprüft das Zertifikat (siehe Bild 8, nächste Seite).

Der öffentliche Schlüssel $S_{TÖ}$ vom Trustcenter ist jedermann, also auch Anna, sicher bekannt.

Erfahrungen

Die erste Version des Rollenspiels erprobte Annemarie List im Informatikunterricht der 11. Klasse. Die Erfahrungen, die sie gemacht hat, wurden beim Erarbeiten der jetzt vorliegenden zweiten Version berücksichtigt.

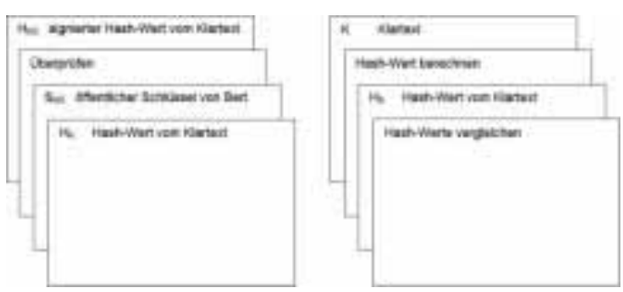

Bild 6 (oben): Die Hash-Werte werden verglichen.

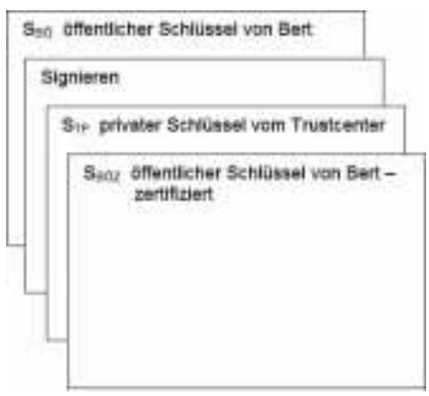

Bild 7 (links): Das Trustcenter wird einbezogen.

Bild 8: Das Zertifikat wird von Anna überprüft.

In mehreren Diskussionen zur vorliegenden Fassung wurden Kritiken und Anregungen formuliert:

- ▷ Bei der Vielzahl von Karten ist es schwer, den Überblick zu behalten.
- ▷ Die Karten, die für Unterschiedliches stehen (Vorgänge, Texte, Schlüssel), unterscheiden sich zu wenig voneinander (nur in der Farbe).
- ▷ Manche Karten sollten zweifarbig gestaltet werden (so z. B. die Geheimtexte, die sich auf einen Klartext und einen Schlüssel beziehen).
- ▷ An den Karten können mechanische Veränderungen so vorgenommen werden, dass nur bestimmte Karten in der richtigen Reihenfolge zusammenpassen.
- ▷ Mithilfe von Briefumschlägen können bestimmte Vorgänge deutlicher gemacht werden.
- ▷ Die Gestaltung der Karten ist textorientiert und damit zu abstrakt. Grafiken, wie z. B. ein Schlüsselsymbol, können die Anschaulichkeit erhöhen.
- ▷ Statt nur mit Worten wie „Verschlüsseln“ und „Klartext“ sollte mit einem konkreten Verschlüsselungsverfahren und mit einem konkreten Klartext operiert werden.
- ▷ Der Übergang vom Sitzungsschlüssel S zum Klartext ist verwirrend (siehe Beschreibung der 3. Szene).
- ▷ Anstatt die Karten durch die Lehrperson bereitzustellen, sollten diese von den Schülerinnen und Schülern im Unterricht selbst hergestellt werden.
- ▷ Auch die Rückseiten der Karten sollten beschriftet sein, und zwar speziell für Linkshänder.

Diese Hinweise wurden jedoch noch nicht umgesetzt. Das Rollenspiel kann also auch von Ihnen, den Leserinnen und Lesern der Fachzeitschrift LOG IN, weiterentwickelt werden!

Prof. Dr. Michael Fothe
Casio-Stiftungsprofessur
Friedrich-Schiller-Universität Jena
Fakultät für Mathematik und Informatik
Ernst-Abbe-Platz 2
07743 Jena

E-Mail: fothe@minet.uni-jena.de

Hash-Wert

Ein *Hash-Wert* (auch *Streuwert* genannt) ist ein skalarer Wert, der aus einer komplexeren Datenstruktur (Zeichenketten u. a.) mittels einer Hash-Funktion berechnet wird. Ein Hash-Wert wird auch als *Fingerprint* bezeichnet. Denn wie ein *Fingerabdruck* einen Menschen nahezu eindeutig identifiziert, ist ein Hash-Wert eine nahezu eindeutige Kennzeichnung einer übergeordneten Menge.

Bei einer *Hash-Funktion* geht es darum, eine lange Eingabe (zum Beispiel einen Text) in eine kurze Ausgabe (den *Hash-Wert* des Textes) zu verwandeln. Das Anwenden einer solchen Funktion ist beispielsweise dann sinnvoll, wenn zwei *große ähnliche* Dateien verglichen werden sollen: Anstatt die einzelnen Zeichen eines Textes daraufhin durchzusehen, ob auch wirklich jeder Buchstabe gleich ist, reicht der Vergleich der *Hash-Werte* der beiden Dokumente, und es ist sofort ersichtlich, ob diese beiden gleich oder verschieden sind.

Im hier vorliegenden Zusammenhang ist die *Hash-Funktion* von Bedeutung, weil Daten zusammen mit Schlüsseln gespeichert werden und die Wertemenge der Schlüssel viel größer ist als die Menge der Textobjekte. In der Praxis wird dann eine *Hash-Funktion* dazu benutzt, um aus einer n-stelligen Zahl eine kleinere zu erzeugen. Wird beispielsweise eine E-Mail übertragen, kann der Autor den *Hash-Wert* generieren lassen: Um zu prüfen, ob es Übertragungsfehler (oder Verfälschungen) gegeben hat, muss die E-Mail nicht etwa ein zweites Mal komplett versandt und mit der ersten verglichen werden, sondern es wird nur der Hash-Wert gebildet und dieser mit dem Wert der E-Mail des Autors verglichen.

Eine *Hash-Funktion* ist also eine Funktion, die zu einer Eingabe aus einer (üblicherweise) großen Quellmenge eine Ausgabe aus einer (im Allgemeinen) kleineren Zielmenge (die *Hash-Werte*, meist eine Teilmenge der natürlichen Zahlen) erzeugt. *Hash-Funktionen* unterscheiden sich in der Definitionsmenge ihrer Eingaben, der Zielmenge der möglichen Ausgaben und im Einfluss von Mustern und Ähnlichkeiten verschiedener Eingaben auf die Ausgabe (vgl. auch Baumann, 1999).

Die Bezeichnung „Hash“ leitet sich vom englischen Verb „to hash“ ab, das soviel wie „zerhacken“ bedeutet.

Literatur

Baumann, R.: Digitale Unterschrift – Sichere Rechtsgeschäfte im Internet (Teil 2). In: LOG IN, 19. Jg. (1999), H. 3/4, S. 82–88.

Becker, K-Cl.; Beutelspacher, A.: Datenverschlüsselung – Anwendungen der Kryptologie. In: LOG IN, 16. Jg. (1996), H. 5/6, S. 16–21.

Fothe, M.; Hohmann, K.; List, A.; Moldenhauer, W.; Stoll, Th.; Straßburg, G.; Zideck, M.: Rollenspiele im Informatikunterricht – Arbeitsergebnis eines Projektes zur Schulentwicklung in Thüringen. In: Rohland, H. (Hrsg.): Informatik & Schule 2005 „Unterrichtskonzepte für informatische Bildung – Praxisband. Praxisberichte, Workshops und Poster der INFOS ’05. Reihe „Technische Berichte“. Dresden: Fakultät Informatik der Technischen Universität Dresden, 2005, S. 67–68.

Portz, M.: Sicherheit in Netzen. In: LOG IN, 16. Jg. (1996), H. 5/6, S. 27–32.

Schubert, S.: Basismechanismen der Informationssicherheit. In: LOG IN, 16. Jg. (1996), H. 5/6, S. 10–15.