CrypTool – sichere Kommunikation

Der Wunsch, zu übertragende Informationen geheim zu halten, ist eng mit dem Entstehen menschlicher Gesellschaften verbunden. Durch die breite kommerzielle Nutzung des Internets wird heutzutage praktisch jeder mit dieser Thematik konfrontiert.

Kryptologie – Gegenstand und Einordnung

Programmnamen werden oft – weil für den Laien unverständlich – als kryptisch bezeichnet. Die Information ist also versteckt. Unter Kryptologie wird die Lehre von sicherer (also geheimer) Kommunikation verstanden. Als sicher gilt eine Kommunikation dann, wenn bestimmte Grundanforderungen bezüglich der Vertraulichkeit, der Integrität, der Authentizität und der Verbindlichkeit von Informationen erfüllt sind. Der Begriff Kryptologie hat in den letzten Jahren den Begriff Kryptographie als Oberbegriff abgelöst. Gegenwärtig unterteilt man die Kryptologie in die Teilgebiete Kryptographie und Kryptoanalyse. Ersteres beschäftigt sich mit der Entwicklung von Prinzipien und Techniken, die unbefugte Dritte an der Kenntnisnahme des Inhaltes einer Nachricht hindern. Die Kryptoanalyse ist darauf gerichtet, aus einer Nachricht die Information ohne Kenntnis des geheimen Schlüssels zu gewinnen. Landläufig ausgedrückt beschäftigt sich diese mit dem „Knacken“ von Schlüsseln und Verfahren. Die Kryptologie ist heute ein wichtiger Aspekt der IT-Sicherheit und basiert auf anspruchsvollen Methoden der Mathematik und der Informatik (Bild ❶).

CrypTool-Projekt – Lernprogramm und mehr

Zur Verschlüsselung von Informationen gibt es diverse frei verfügbare Programme. Im Netz findet man eine Fülle von Informationen zu dieser Thematik, die ebenfalls frei zugänglich sind. Von diesen Angeboten unterscheidet sich CrypTool insbesondere durch Orientierung auf die Ausbildung sowie die Komplexität, mit der das Thema behandelt wird. CrypTool ist einerseits dazu geeignet, die Sensibilität für die Thematik zu fördern. Andererseits unterstützt es die Aneignung von Detailkenntnissen auf diesem Gebiet.

Entwickler und Sponsoren

CrypTool ist frei verfügbar. Die Nutzung unterliegt den Bedingungen der GPL-Lizenz, wobei allerdings einige Einschränkungen zu beachten sind. Die Lizenzbestimmungen sollten daher gründlich gelesen werden. Neben vielen freiwilligen Entwicklern sind an dem Projekt insbesondere Mitarbeiter der Universitäten Siegen und Darmstadt beteiligt. Interessant ist die Tatsache, dass das Projekt durch die Deutsche Bank gesponsert wird (Bild ❷).

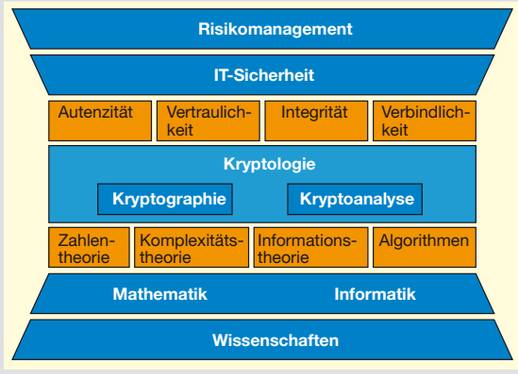
Das Interesse von Banken an sicherer Kommunikation (Stichwort Online-Banking) wird damit überaus deutlich.

Installation und erster Start

CrypTool kann direkt von der Homepage www.cryptool.de heruntergeladen werden. Da die Installationsdatei etwa 40 MByte umfasst, benötigt man einen schnellen Zugang für den Download. Die Installation ist unproblematisch, allerdings wird ein aktueller Rechner mit Windows XP oder Vista vorausgesetzt.
Mit der Installation wird ein Eintrag im Start-Menü angelegt, über den nicht nur das Programm an sich, sondern weitere Zusatzwerkzeuge und Dokumente aufgerufen werden können. Beim ersten Start wird eine Textdatei mit Hinweisen für die ersten Schritte angezeigt (Bild ❸). Unabhängig davon, wie umfangreich die vorhandenen Vorkenntnisse sind, ist es sinnvoll, diesen Hinweisen zu folgen.

Schrittweise Details erschließen

Die Funktionen der Software sind alle direkt über ein Hauptmenü erreichbar. Im Unterschied zu der ansonsten bei Lernprogrammen üblichen Vorgehensweise ist hier der fachliche Inhalt nicht in aufeinan-



❶ Kryptologie – ein Bestandteil der IT-Sicherheit

Quelle: CrypTool

❷ Entwickler und Sponsoren ▶

HAUPTZIELE ZUM SCHUTZ VON INFORMATIONEN

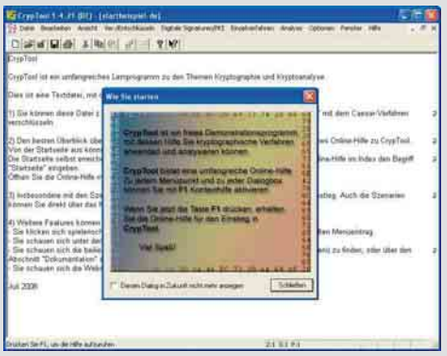
Vertraulichkeit – Zugriffsschutz
Nur dazu berechtigte Personen sollen in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.

Integrität – Änderungsschutz
Der Empfänger soll in der Lage sein festzustellen, ob die Daten oder die Nachricht nach ihrer Erzeugung verändert wurden.

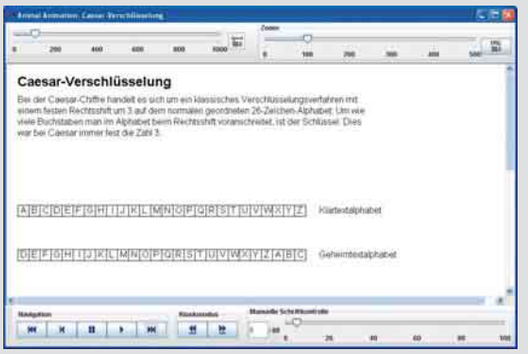
Authentizität – Fälschungsschutz
Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein, und seine Urheberschaft sollte nachprüfbar sein.

Verbindlichkeit – Nichtabstreitbarkeit
Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein, seine Urheberschaft zu bestreiten, d. h. sie sollte sich gegenüber Dritten nachweisen lassen.

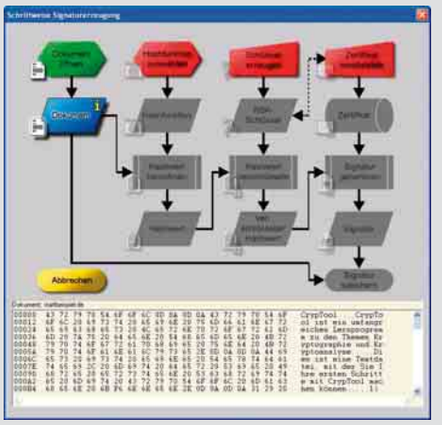
Quelle: Wikipedia



❸ Hauptmenü mit Textdatei und Hinweis-Fenster



❹ Vorgehensweisen werden anschaulich dargestellt



❺ Digitale Signaturen statt handschriftlicher Unterschriften ▶

der aufbauende Kapitel aufgeteilt. Der Nutzer wählt selbst, womit er sich in welcher Reihenfolge beschäftigen möchte. Wer kaum mit der Thematik Verschlüsselung vertraut ist, sollte zur Orientierung die einschlägigen Einträge auf www.wikipedia.de studieren, um sich einen ersten Überblick zu verschaffen. Hierzu eignet sich auch die programminterne Hilfe. So vorbereitet, kann man sich dann Schritt für Schritt den Inhalt dieser Lernhilfe erschließen.

Methodik

Zu den großen Vorzügen dieses Werkzeuges gehört die anschauliche Darstellung der verschiedenen Vorgehensweisen. Hier werden die durch den Rechner gegebenen Möglichkeiten genutzt und anspruchsvolle Sachverhalte mittels Animationen leicht verständlich dargestellt (Bild ❹). Wer einen Lernschritt nicht verstanden hat, kann diesen beliebig oft wiederholen. Aufbauend auf den theoretischen Grundlagen der verschiedenen Verfahren, kann man diese anhand praktischer Beispiele erproben (Bild ❺) und die gewonnenen Erkenntnisse vertiefen. In allen Arbeitsschritten sind weitergehende Erläuterungen integriert.

Ver- und Entschlüsseln

Die zur Wahrung der Vertraulichkeit entwickelten Verschlüsselungen werden entsprechend der üblichen Systematik in symmetrische, asymmetrische und hybride Verfahren unterteilt. Bei den symmetrischen Verfahren erfolgt noch eine weitere Unterscheidung in klassische und moderne Verfahren. Auch wenn nicht jedes Verfahren von Interesse ist, so trägt die gewählte Systematik entscheidend zum Verständnis der Gesamtproblematik bei.

Digitale Signaturen

Vielfach werden Betrachtungen zur Kryptographie auf Verschlüsselungsverfahren reduziert. Durch Verschlüsselung wird aber lediglich das Ziel „Wahrung der Vertraulichkeit“ erreicht. Zur Erreichung der Ziele Authentizität, Integrität und Verbindlichkeit bedarf es weiterer, als digitale Signaturen bezeichneter Maßnahmen. Die digitale Signatur erfüllt eine der handschriftlichen Unterschrift vergleichbare Funktion. Auch hier werden die verfügbaren Verfahren anschaulich erläutert und können anhand von Demonstrationen erprobt werden.

Analyse

Die Kryptoanalyse ist eher für Spezialisten von Interesse. Aber wer sich für die Verfahren interessiert, mit denen verschlüsselte und/oder signierte Dokumente angegriffen werden können, findet hierzu umfangreiches Informationsmaterial und verschiedene Werkzeuge.

Zugaben

Mit dem CrypTool-Paket wird auch das Verschlüsselungsprogramm AES-Tool installiert. AES-Tool ist für den praktischen Einsatz geeignet und basiert auf dem symmetrischen und lizenzfreien Rijndael-Algorithmus. Eine interessante Zugabe ist auch das Spiel Zahlenhai. Damit kann der Umgang mit Teilern und Primzahlen spielerisch geübt werden. Beide Programme sind auch separat nutzbar.

Hilfen und Informationen

CrypTool wird mit einem ganzen Paket von Hilfen und Fachinformationen ausgeliefert. Die CrypTool-Readme liefert Informationen zum Projekt, zu aktuellen Distributionen und geplanten Weiterentwicklungen. Über die programminterne Hilfe erhält der Nutzer nicht nur Hinweise zur Programmbedienung, sondern auch gut aufbereitete Fachinformationen. Die integrierten Tutorials enthalten Anleitungen zur schrittweisen Einarbeitung in verschiedene Detailthemen. Ein rund 230 Seiten umfassendes Script zu „Kryptographie, Mathematik und mehr“ von Prof. *Esslinger* gibt dem interessierten Nutzer die Möglichkeit, sich mit den theoretischen Grundlagen der Kryptographie zu beschäftigen. Gleiches gilt auch für die etwa 100 Folien umfassende Präsentation, die wie das Script als PDF-Datei vorliegt.

Fazit

Mit CrypTool steht ein E-Learning-Programm zur Verfügung, das kaum Wünsche offen lässt und derzeit das mit Abstand umfangreichste Hilfsmittel zur Aneignung von Kenntnissen zur Kryptographie darstellt. Die Animationen und Demonstrationsprogramme sind eine empfehlenswerte Bereicherung des Informatikunterrichts.

H. Möbus

KRYPTOGRAPHIE UND STEGANOGRAPHIE

Wenn es um die Geheimhaltung von Nachrichten geht, wird zuweilen neben Kryptographie auch von Steganographie gesprochen.

Kryptographie. Bei der Kryptographie wird der Inhalt der Nachricht vor unbefugten Dritten durch Verschlüsseln verborgen. Der Vorgang der Nachrichtenübermittlung an sich wird aber nicht verborgen oder kann eben aus technischen Gründen nicht verborgen werden.

Steganographie. An dieser Stelle setzt die Steganographie an, indem verborgen wird, dass überhaupt eine Nachricht übermittelt wird. Hierfür gibt es verschiedene Vorgehensweisen, wobei das Verbergen von Nachrichten in scheinbar belanglosen Bildern die derzeit bekannteste technische Variante ist. Natürlich kann eine Information vor dem „Einbetten“ in ein Bild verschlüsselt und mit einer digitalen Signatur versehen werden.