Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info

12. Jahrgang, Heft 1, April 2012

Schwerpunkt:

Sensor-Actor-Netze

fokus: Lagebild für Kritische Infrastrukturen

fokus: Privatsphäre trotz intelligenter Zähler

report: Sicherheit im Cloud Computing

Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Sensor-Actor-Netze

Lagebild für Kritische Infrastrukturen

Für den Schutz Kritischer Infrastrukturen (SKI) ist der regelmässige Austausch von Informationen zwischen Behörden und Unternehmen unerlässlich. Dieser könnte in einem SKI-relevanten Lagebild gebündelt und aufbereitet werden. Darin können Behörden und Betreiber Informationen zum Schutz Kritischer Infrastrukturen bündeln und die Koordination im Hinblick auf Schutzmassnahmen verbessern.

Sicherheit im Energienetz der Zukunft

Durch den vermehrten Einsatz von ICT und der damit verbundenen erhöhten Anzahl von Schnittstellen im Energienetz entstehen neue Sicherheitsrisiken in Bezug auf Netzverfügbarkeit, Systemintegrität und Datenschutz. Ein Sicherheitskonzept für das intelligente Stromnetz der Zukunft sollte frühzeitig geplant werden.

PET – ein Konzept harrt der Umsetzung

Mit «Privacy Enhancing Technology» (PET) sollen neue Anwendungen «datenschutzverträglich» gemacht werden. Die inhärenten Zielkonflikte können nur aufgelöst werden, wenn neben der Technik auch das Datenschutzrecht in die Betrachtung einbezogen wird.

Privatsphäre trotz Intelligenter Zähler

Intelligente Zähler versprechen eine bessere Ausnutzung vorhandener Infrastruktur für Netzbetreiber und erhöhte Transparenz für Konsumenten. Kann die Privatsphäre im eigenen Heim bedingungslos geschützt werden, oder folgt auf den gläsernen Mobilfunkkunden nun der gläserne Stromkunde?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Sicherheit im Cloud Computing

Obwohl in den Medien intensiv über Cloud Computing und entsprechende ökonomische Vorteile berichtet wird, werden die latent vorhandenen Sicherheitsprobleme meist verschwiegen bzw. ignoriert. Muss man den Cloud-Anbietern einfach vertrauen?

E-Learning: Kryptografie und -analyse

Das Open-Source-Projekt CrypTool (CT) hat sich die Aufgabe gestellt, Kryptografie und Kryptoanalyse mit Beispielen und Visualisierungen so darzustellen, dass man ein gutes Verständnis und Awareness für IT-Sicherheit erreicht.

Familie und Arbeitsplatz: heikle Ortung

Location Based Services sind heikel oder unzulässig, wenn sie der Überwachung von Kindern und Arbeitnehmenden dienen. Die gesetzliche Vertretung ist bei älteren Kindern meist nicht befugt, an deren Stelle die Einwilligung zur Datenbearbeitung zu erteilen. Das Arbeitsrecht schränkt die Überwachung von Arbeitnehmenden erheblich ein.

EU: Zu neuen Ufern lockt ein neuer Tag?

Die EU-Kommission hat Entwürfe für eine «Regulation» und eine «Directive» zur Vereinheitlichung des Datenschutzrechts vorgelegt. Mit dem darin enthaltenen «right to be forgotten» und dem Strafenkatalog würde ein bedeutender Schritt in Richtung Harmonisierung des Datenschutzrechts getan. Es ist zu hoffen, dass der Gedanke der Entwürfe in der definitiven Fassung immer noch zu erkennen sein wird.

Aus den Datenschutzbehörden

Wer ist neu zur Datenschutzbeauftragten gewählt worden? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzszene.

report

forum

Lernen

E-Learning: Kryptografie und -analyse

Bernhard Esslinger, Prof., Leiter des CrypTool-Projektes, Universität Siegen, Siegen, Deutschland
esslinger@fb5.uni-siegen.de

Sibylle Hick, Dr., Mitarbeiterin im CrypTool-Projekt
sibylle.hick@cryptool.org

Die Buchung von Flügen, Reisen und Hotels im Internet, Online-Banking, Bestellungen bei Amazon oder eBay oder der Einsatz von Paketautomaten stellen neue Anforderungen an die Sicherheit. Hierbei sind vertrauliche Informationen (wie personenbezogene Daten, Identitäts- und Authentifizierungsdaten) sowie Bezahldaten zu schützen.

Dies geschieht in der Regel durch kryptografische Verfahren und Protokolle. Für den Kunden sollten diese Verfahren möglichst ohne sein Zutun oder einfach zu nutzen sein. Damit die Verfahren richtig angewendet werden, ist es zum einen wichtig, dass diese korrekt implementiert wurden, und zum anderen sollte der Benutzer verstehen, worauf zu achten ist, um den Dienst tatsächlich sicher und wunschgemäss zu nutzen.

Die oben genannten Anwendungen erfreuen sich grosser Beliebtheit, doch gleichzeitig werden die Menschen durch eine Vielzahl von Pressemitteilungen zu Risiken und Gefahren bei der Anwendung verunsichert.

CrypTool – ein E-Learning-Programm

Idee des Open-Source-Projektes CrypTool ist es, Menschen den Einsatz von Kryptografie und die damit zusammenhängenden Verfahren näher zu bringen. Dies schliesst die Kryptoanalyse mit ein, mit der bestimmte Verfahren, ohne den Besitz des normalerweise erforderlichen Geheimnisses (d.h. Schlüssels), angegriffen werden können. So kann man ein ganzheitliches Bild der Kryptologie gewinnen, die sowohl die Kryptografie als auch die Kryptoanalyse umfasst.

Überblick zu CrypTool

Mittlerweile kann das Projekt auf eine mehr als zehnjährige Geschichte zurückblicken[1]. Begonnen wurde die Entwicklung der Software 1998 im Rahmen einer Initiative der Deutschen Bank zu Awareness und IT-Sicherheit im Unternehmen. Hieraus entstand ein Open-Source-Projekt, das inzwischen nicht nur von Schulen und Universitäten sondern auch von zahlreichen Freiwilligen und Kryptografie-Interessierten genutzt und unterstützt wird. Projektteilnehmer kommen sowohl aus Nord- und Südamerika wie auch aus verschiedenen Staaten in Europa. Nähere Informationen sind über das CrypTool-Portal (<www.cryptool.org>) zu finden.

Die erste Version von CrypTool wurde als Windows-Applikation in C++ geschrieben und liegt mittlerweile in den Sprachen Englisch, Deutsch, Spanisch, Polnisch und Serbisch vor; Griechisch, Französisch und Russisch sollen in 2012 folgen. Während bei CrypTool 1 (CT1) nur noch kleinere Änderungen und vor allem Fehlerkorrekturen vorgenommen werden, haben sich inzwischen zwei Nachfolgeprojekte etabliert, die das Konzept von CrypTool auf aktuelle Software-Technologien übertragen.

CrypTool 2 (CT2) zeigt sich in einer modernen Lernoberfläche, die das Konzept der visuellen Programmierung umsetzt. Entwickelt wird die Software in C# unter Visual Studio 2010. CT2 kann in englischer Version heruntergeladen werden, an einer deutschen Version wird bereits gearbeitet.

JCrypTool (JCT) wird in der Programmiersprache Java mit der Entwicklungsumgebung Eclipse erstellt und liegt in deutscher und englischer Sprache vor. Die JCT-Anwendung kann nicht nur auf Windows, sondern auch auf Mac OS und Linux eingesetzt werden.

Diese drei CrypTool-Versionen bieten neben den kryptografischen Funktionen auch umfangreiche Erläuterungen in der Onlinehilfe an.

Mit CrypTool-Online (CTO) gibt es ferner eine Variante von CrypTool, die man im Browser auf dem Rechner oder auf dem Smartphone aufrufen kann (<www.cryptool-online.org>, <www.cryptool-mobil.org>).

Die Nutzung von CTO mit dem Smartphone erfreut sich bei der «modernen Schatzsuche» – dem sogenannten Geocaching – besonderer Beliebtheit, da sie zur Lösung kleiner kryptografischer Rätsel genutzt werden kann. Hierbei werden kryptografische Verfahren z.B. zur Verschlüsselung von Koordinaten eingesetzt, um den «Schatz» zu verstecken. CTO unterstützt den Anwender bei der Entschlüsselung.

Die kryptografischen Mechanismen, die man mit Cryp-

Tool kennengelernt hat, kann man in verschiedenen Herausforderungen (engl. Challenges) selber ausprobieren: Dazu unterstützt CrypTool den internationalen Krypto-Wettbewerb MysteryTwister C3 (MTC3) (<www.mysterytwisterc3.org>), der regelmässig neue Rätsel unterschiedlicher Schwierigkeitsgrade anbietet.

Zielgruppen

Das Projekt CrypTool mit seinen verschiedenen Versionen spricht mehrere Zielgruppen an, die sich für Kryptografie und IT-Sicherheit interessieren und diese spielerisch begreifen möchten.

Für den Unterricht mit Schülern wurde auf Anregung der INFOS[2] auf der Internetseite von CrypTool ein eigener Bereich für Lehrer eingerichtet: Das sogenannte Lehrerportal (<www.cryptoportal.org>) bietet Informationen für Schulen und fördert den Austausch zwischen Lehrern.

Besonders richtet sich das Open-Source-Projekt an Studenten, denn die Kryptologie hat sich inzwischen in Lehre und Forschung fest etabliert. Es bestehen zahlreiche Möglichkeiten, eigene Ideen zu kryptografischen Implementierungen auszuprobieren, um die Anwendung der Kryptografie sowie deren praktische Umsetzung besser zu verstehen.

Neben der wissenschaftlichen Lehre richtet sich das Projekt aber auch an Firmen, die das E-Learning-Tool zur Awareness-Bildung nutzen wollen. Mit CrypTool können moderne Verfahren auch mit «kleinen Zahlen» durchgeführt werden, um sie leichter zu verstehen.

Eine weitere Zielgruppe innerhalb von Unternehmen stellen Systemadministratoren dar, die häufig auch IT-Sicherheitsmechanismen umsetzen müssen.

Datenschützern und Juristen bietet CrypTool die Möglichkeit, einen verständlichen Einblick in die technischen Zusammenhänge z.B. bei digitalen Signaturen zu bekommen.

Anwendung in der Praxis

Kryptografische Mechanismen werden häufig als sehr komplex empfunden und manche sind es auf den ersten Blick auch. CrypTool erlaubt es dem Anwender, kryptografische Fragestellungen schrittweise zu verstehen und ggf. mit einer visuellen Darstellung zu beschreiben.

Passwörter

Ein Beispiel stellt die Verwendung von Passwörtern dar. Eine Vielzahl von Passwörtern bestimmt unser tägliches Leben. Bei der Beantragung eines neuen E-Mail-Postfaches beispielsweise oder bei der Authentifizierung für einen Online-Dienst muss ein neues Passwort angelegt werden. Dabei werden dem Kunden häufig bereits Anforderungen an die Länge des Passwortes und dessen Bestandteile vorgegeben, z.B. muss ein Passwort häufig Zahlen und Buchstaben enthalten oder es soll mindestens 8 Zeichen lang sein. Sofern dem Kunden nicht zusätzliche Hilfsmittel zur Verfügung gestellt werden, ist es für diesen schwierig zu erkennen, ob er ein «gutes» oder «schlechtes» Passwort gewählt hat, da er die Passwortgüte nicht bewerten kann.

CT1 bietet für diesen Anwendungsfall einen *Passwort-Qualitätsmesser* an. Damit hat der Anwender die Möglichkeit, verschiedene Passwörter einzugeben und anhand von Hypothesen eine Einschätzung zu erhalten, ob diese eine angemessene Sicherheit bieten. Wählt man z.B. ein Passwort, welches in einem Wörterbuch gefunden werden kann, so ist dies auch für einen Angreifer schnell auszuprobieren, wenn er automatisch nacheinander alle Wörter des Wörterbuches durchtestet. Einen solchen Angriff nennt man daher Wörterbuchangriff (engl. dictionary attack). Die Resistenz gegen Wörterbuch-Attacken wird im unteren Bereich des Passwort-Qualitätsmessers detailliert dargestellt. Auch Buchstaben, die auf dem Keyboard nebeneinander angeordnet sind oder aufeinanderfolgende Sequenzen bei Zahlen erleichtern die Angriffe.

Neben der Möglichkeit, ein beliebiges Passwort mit dem

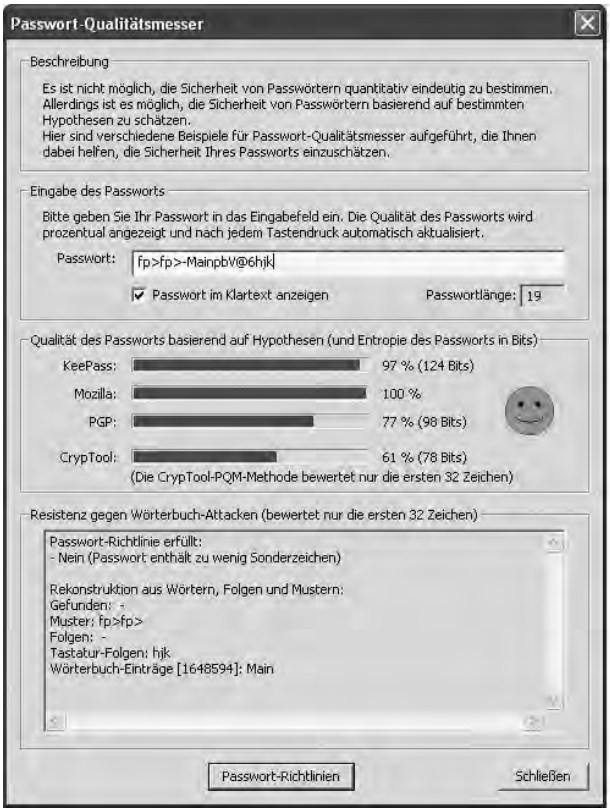

Abb. 1: Passwort-Qualitätsmesser in CT1

Kurz&bündig

Kryptografie ist in vielen Bereichen unseres Lebens zu finden, jedoch nicht immer sichtbar oder verständlich. Das Open-Source-Projekt CrypTool (CT) hat sich die Aufgabe gestellt, Kryptografie und Kryptoanalyse mit Beispielen und Visualisierungen so darzustellen, dass man ein gutes Verständnis und Awareness für IT-Sicherheit erreicht. Dabei richtet sich CT an unterschiedliche Zielgruppen. Dieser Beitrag beschreibt praktische Beispiele zur Kryptografie und deren Abbildung mit den unterschiedlichen Versionen der E-Learning-Software.

Qualitätsmesser auszuprobieren, kann man sich mit dem Tool *Passwort-Entropie* auch ein Passwort generieren lassen. Zwei entscheidende Faktoren bilden hierbei die Entropie und das verwendete Alphabet. Der Begriff der Entropie nach Claude E. Shannon[3] beschreibt den Informationsgehalt in einer Nachricht bzw. hier in einem Passwort (Bit pro Zeichen). Das Alphabet gibt an, welche Zeichen (Zahlen, Klein- und Grossbuchstaben sowie Sonderzeichen) für die Bildung eines Passwortes zur Verfügung stehen. So kann sich ein Anwender schrittweise einen Überblick über die verschiedenen Einflussfaktoren zur Passwortwahl verschaffen.

Auch in CTO werden dem Anwender im Bereich *Highlights* ein «Passwort-Check» und ein «Passwort-Generator» zur Verfügung gestellt, die eine Übersicht zur Bewertung und Komplexität geben. Jedes betrachtete Kriterium enthält dabei eine separate Bewertung und eine Punktzahl, die eine dedizierte Einschätzung erlauben.

Secure Sockets Layer

Kommunikationsverbindungen im Internet werden häufig mit dem Protokoll Secure Sockets Layer (SSL) bzw. der neueren Version, dem Transport Layer Security (TLS)[4] abgesichert, um zu übertragende Daten gegen unerlaubtes Abhören zu schützen. Eine mit TLS gesicherte Internetseite erkennt man daran, dass die Adresse mit «https://» anfängt. In manchen Browsern wird zusätzlich ein gelbes Schloss angezeigt, und man kann sich ein Zertifikat, welches im Rahmen des Protokolls Anwendung findet, im Detail anschauen. Im TLS-Protokoll kommen gleich mehrere kryptografische Mechanismen zum Einsatz. Die Vertraulichkeit der zu etablierenden Verbindung basiert auf einem symmetrischen Verschlüsselungsverfahren.

Für den Anwendungsfall, dass ein Systemadministrator eine Server-Verbindung mit TLS absichern möchte und nähere Informationen sucht, kann er sich einzelne Teile von TLS mit den verschiedenen CrypTool-Versionen visualisieren.

CrypTool bietet u.a. Demonstrationen zu DES[5] und AES an, die den Ablauf der Verschlüsselungsalgorithmen detailliert aufzeigen. Bei den symmetrischen Verschlüsselungsverfahren wie DES und AES handelt es sich um Blockchiffren, die eine Nachricht in Blöcke unterteilen und diese verschlüsseln. Die Blockverschlüsselung kann auf unterschiedliche Weise durch den sogenannten Betriebs- bzw. Verkettungsmodus vorgenommen werden. Für den ausgewählten Verkettungsmodus werden die verschiedenen Komponenten des Algorithmus aufgezeigt, und die zuvor schrittweise ausgewählten Funktionen und Parameter visualisiert. CT2 visualisiert die zuvor beschriebenen Algorithmen z.B. auch mit Unterstützung eines Wizards.

Neben der Vertraulichkeit spielt auch die Authentifizierung zwischen den Kommunikationspartnern bei TLS eine wichtige Rolle. So wird z.B. sichergestellt, dass ein bestimmter Kunde nach erfolgreicher Authentifizierung seine bereits zu einem früheren Zeitpunkt gespeicherten Benutzerdaten einsehen darf. Die Authentifizierung erfolgt auf Basis asymmetrischer Verschlüsselungsverfahren, die in unterschiedlichen Varianten bei TLS eingesetzt werden können. Hier sind insbesondere das RSA-Verfahren zum Signieren und das Diffie-Hellman-Verfahren (DH) zur Schlüsselaushandlung zu nennen.

Literatur

- Christof Paar/Jan Pelzl, Understanding Cryptography – A Textbook for Students and Practioners, Dezember 2009, Springer.
- Mark Stamp, Information Security: Principles and Practice, 2. Auflage, 2011, Wiley.
- Rolf Oppliger, Contemporary Cryptography, Second Edition, 2011, Artech House.
- Joachim Swoboda/Stephan Spitz/Michael Pramateftakis, Kryptografie und IT-Sicherheit: Grundlagen und Anwendungen, 2008, Vieweg+Teubner.
- Juraj Hromkovic/Karin Freiermuth/Lucia Keller/Björn Steffen, Einführung in die Kryptologie, 2010, Vieweg+Teubner.

Fussnoten

1 Bernhard Esslinger: CrypTool – Ein Open-Source-Projekt in der Praxis, in: Datenschutz und Datensicherheit 03/2009, 167–173.

2 Die INFOS ist eine zweijährig stattfindende Konferenz der GI (Gesellschaft für Informatik), auf der die Informatik-Lehrenden im deutschsprachigen Raum zusammenkommen. Nähere Informationen sind zu finden unter <http://www.fa-ibs.gi-ev.de/fachausschuss-informatische-bildung-in-schulen/infos.html>.

3 Claude Elwood Shannon, A Mathematical Theory of Communication, in: Bell System Technical Journal, Short Hills N.J. 27.1948, (Juli, Oktober), 379–423, 623–656. ISSN 0005-8580, <http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf>.

4 RFC 5246, IETF, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008. Abrufbar unter: <http://www.rfc-editor.org/rfc/rfc5246.txt>.

5 Im TLS-Protokoll wird nicht DES, sondern 3DES, als ein möglicher Verschlüsselungsalgorithmus (engl. cipher) angegeben. Bei 3DES, auch Triple DES genannt, wird der DES-Algorithmus dreimal hintereinander ausgeführt.

6 Vgl. <http://www.cryptool.org/de/ctp-dokumentation-de/ctp-functions-de>.

7 Zu den MINT-Fächern gehören Mathematik, Informatik, Naturwissenschaften und Technik (Ingenieurwissenschaften).

8 Nähere Informationen sind zu finden unter <http://www.cryptool.org/schuelerkrypto/>.

CrypTool bietet Demonstrationen zu RSA und DH und visualisiert RSA sowie DH in Verbindung mit elliptischen Kurven.

Sichere E-Mail mit S/MIME

In der realen Welt werden Nachrichten unterschrieben, um ihre Authentizität sicherzustellen. Auch in der elektronischen Welt bestehen Anforderungen an die Authentizität einer E-Mail. Dies kann mit einer elektronischen Signatur erreicht werden. Ein Standard, der dieses Verfahren umsetzt, ist S/MIME.

CT1 bietet eine animierte Demonstration dieses Verfahrens. Im sogenannten Control-Center-Fenster werden die verschiedenen Bestandteile und Parameter des S/MIME-Protokolls aufgelistet, die der Anwender beliebig verändern kann. Sind alle Einstellungen vorgenommen, kann man eine Flash-Animation aufrufen. In der Animation können alle Stationen einer S/MIME-gesicherten Kommunikation durchlaufen werden.

Funktionsübersicht

Eine Auflistung der bisher implementierten Verfahren[6] über alle vier Versionen von CrypTool findet sich auf dem CrypTool-Portal. Dort kann man nach verschiedenen Kategorien und Schlüsselwörtern suchen.

Erfahrungen mit CT und Schülern

Seit 2009 gibt es die Veranstaltung *Schülerkrypto mit CrypTool.* Darin wird Schülern das Thema Kryptologie spannend nähergebracht und versucht, sie für die MINT[7]-Fächer zu begeistern. Dies geschieht einerseits theoretisch durch Vorträge zur Kryptologie und ihrer Geschichte, andererseits können die Schülerinnen und Schüler die vorgestellte Theorie praktisch anhand von «Agentenaufträgen» mit CT1 und CT2 selber ausprobieren. Inzwischen wurde die Veranstaltung viermal durchgeführt[8]. Im Rahmen der letzten Schülerkrypto gaben 50% der teilnehmenden Schüler an, dass ihnen das E-Learning-Tool geholfen hat, Kryptografie und Kryptoanalyse besser zu verstehen, für 33% traf dies weitestgehend zu und für 17% traf dies immerhin noch teilweise zu. Dabei gaben 71% der Teilnehmer an, sich vor der Veranstaltung gar nicht oder sehr wenig mit Kryptografie beschäftigt zu haben, während 29% angaben, bereits Vorkenntnisse zu besitzen.

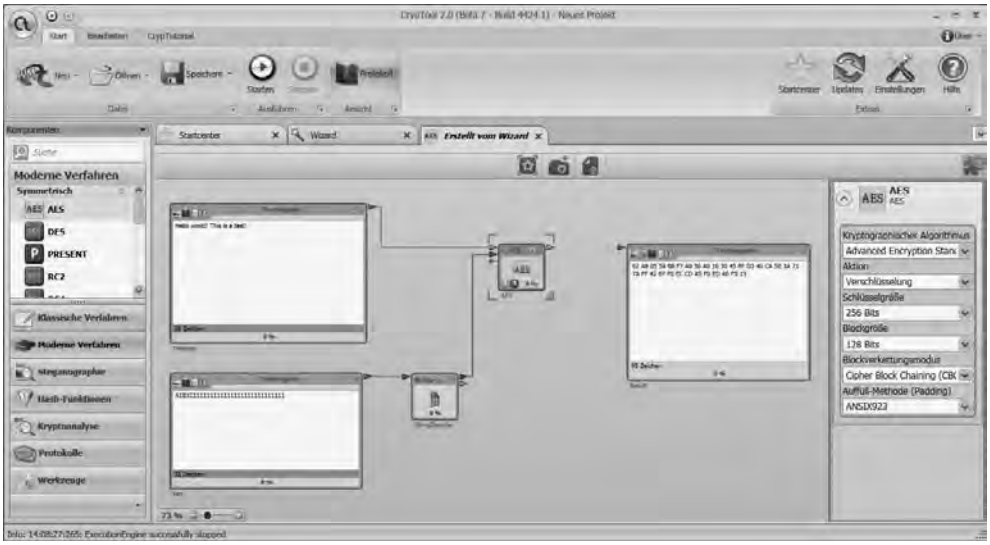

Abb. 2: Visualisierung der Algorithmen in CT2

Fazit

Das Open-Source-Projekt CrypTool richtet sich an verschiedene Zielgruppen und hat den Anspruch, geeignete Demonstrationen und Visualisierungen anzubieten, um dem jeweiligen Anwender ein besseres Verständnis von IT-Sicherheit und mehr Awareness für die damit zusammenhängende Kryptologie zu vermitteln. Dafür hat CrypTool mehrere Preise zur Didaktik erhalten.

Die Entwickler nutzen die jeweils modernsten Entwicklungsumgebungen und tauschen sich intensiv untereinander aus. Dabei wird das Projekt von ganz unterschiedlichen Mitwirkenden unterstützt, die entweder neue Implementierungen zu dem E-Learning-Tool hinzufügen, Fehler melden oder auch Feedback zur Anwendung geben. Das CrypTool-Projekt freut sich über alle Interessenten und bietet auf der Internetseite Informationen, wie man selbst zu einem Teil des Projektes werden kann (<www.cryptool.org>). ■

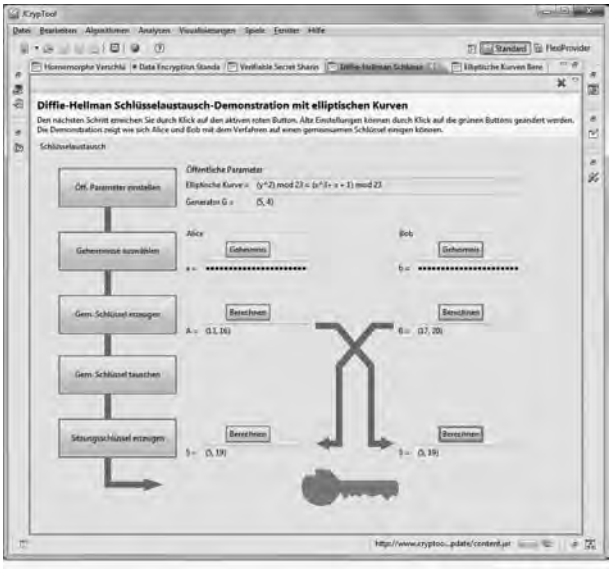

Abb. 3: Bei DH handeln zwei Kommunikationspartner ein Geheimnis aus, ggf. ohne sich vorher gekannt zu haben (hier in JCT).

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §