CrypTool-Projekt

Der beste Weg, Kryptographie zu lernen und anzuwenden

Arkadius C. Litwinczuk

In diesem Artikel erhalten sie einen Überblick über das CrypTool-Projekt. Es ist das größte Lernprogramm für Kryptographie weltweit. Wir möchten Ihnen CrypTool 1 (CT1) und seine zwei Nachfolger CrypTool 2 (CT2) und JCrypTool (JCT) vorstellen, wobei wir nur auf einen kleinen Bereich der Möglichkeiten eingehen können. Alle Projekte sind Open-Source und online umsonst erhältlich.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Einsatz moderner Kryptographie
- Entwicklung des CrypTool-Projekts
- Verfügbare CrypTool-Versionen

WAS SIE VORHER WISSEN SOLLTEN...

- Grundlagen der Mathematik
- Grundlagen Kryptographie

Die Geschichte der Kryptographie geht über 2000 Jahre zurück. Geheime Kommunikation war schon immer wichtig – hauptsächlich für Politik und Militär. Der Durchbruch der Kryptographie erfolgte zeitgleich mit dem des Internets. Heute hat sich Kryptographie zu einer mathematischen Wissenschaft entwickelt, die von den meisten Menschen jeden Tag genutzt wird, ohne dass sie es wissen. Kryptographie kommt unter anderem in Mobiltelefonen, EC-Karten, Pay-TV, sicherer E-Mail oder beim Online-Shopping zum Einsatz. Die vier Ziele der modernen Kryptographie sind Authentizität, Integrität, V ertraulichkeit und Verbindlichkeit von digitalen Daten. Anwendungen, die diese Voraussetzungen erfüllen, erleichtern unser Alltagsleben enorm, zum Beispiel durch sicheres Online-Banking oder nicht reproduzierbare digitale Signaturen, die wichtige Dokumente schützen und verifizieren. Dies spart Zeit und erlaubt uns, den Einsatz von Papier zu verringern. Obwohl die Kryptologie eine essentiell wichtige Technologie in der modernen Kommunikation ist, ist sie den meisten Menschen kaum bekannt.

In der Gegenwart ist die Kryptographie nicht nur von militärischem oder geschäftlichem Nutzen. Jüngste Entwicklungen, wie die Inspektion von Laptops oder anderen elektronischen Geräten bei Grenzkontrollen, machen sie interessant für jeden von uns, der das Recht auf seine Privatsphäre schätzt. Die Technologie zum Schutz der Privatsphäre existiert bereits – sie ist umsonst. Es ist auf Grund der Komplexität von IT-Systemen und der immer schnelleren Entwicklung von Technologien fast unmöglich, ein zu hundert Prozent sicheres Computersystem zu erstellen. Mit der Kryptographie kann man aber, wenn sie korrekt angewendet wird, wertvolle Daten so sichern, dass sie unmöglich von Dritten eingesehen werden können (z.B. mit TrueCrypt). Dies schließt allerdings Sie selbst ein: W enn Sie Ihr Passwort vergessen, können Sie Ihre wert vollen Daten verlieren. Kryptographie gibt uns die Mittel zur Hand, um sichere E-Mails zu schreiben (z.B. mit Thunderbird und EnigMail), sie kann Gespräche über Instant-Messenger oder in sozialen Netzwerken sichern. Dennoch wird sie bisher von Privatpersonen kaum genutzt.

Die Vergangenheit hat gezeigt, dass sich proprietäre Verschlüsselungsalgorithmen im Nachhinein oft als unsicher erweisen. Viele Kryptographie-Forscher sind der Meinung, dass man nur solche Kryptoverfahren einsetzen sollte, die offengelegt sind: Dann können sie analysiert und ihre Sicherheit nachgewiesen werden. Das Gegenbeispiel sind die Millionen von unsicheren Mifare-Chips, die im Transportwesen weitverbreitet sind und deren Schwäche zu spät aufgedeckt wurde, was hohe Kosten verursachte, die hätten vermieden werden können. Ein anderes Beispiel ist die Verschlüsselung, die in schnurlosen DECT-Telefonen benutzt wird – nun kann Ihr Nachbar mit dem richtigen Werkzeug herausfinden, was sie am Telefon sagen.

Da viele starke kryptographische Algorithmen offen sind, hat jeder Zugang zu kryptographischen Technologien, die auf dem neuesten Stand der Technik sind. Wir alle haben die Möglichkeit, sie kennenzulernen und sie frei zu nutzen.

Das Ziel des CrypTool-Projektes ist es, Menschen dazu zu ermutigen und ihnen dabei zu helfen, die Kryptographie und die ihr zugrunde liegenden Techniken zu verstehen. Es veranschaulicht die aktuellen Verfahren, auch die der Kryptoanalyse und bekannte Attacken gegen kryptographische Systeme. CrypTool ist weltweit das verbreitetste Lernprogramm dieser Art.

Das CrypTool-Projekt versucht außerdem, Forschung von Unternehmen und Universitäten zu vereinen, sodass andere davon lernen können. Es gibt (vor allem) Studenten die Möglichkeit, dass ihre in der Bachelor-, Diplom- oder Masterarbeit entwickelte Software nicht einfach in der Schublade „verschwindet“, sondern erhalten bleibt, weiter gepflegt wird und von anderen Interessierten auf der ganzen Welt genutzt werden kann.

Das ursprüngliche CrypTool-Projekt wurde 1998 in einer großen Finanzinstitution gestartet. Das Ziel damals war internes Training, um das Bewusstsein für Kryptographie zu schärfen und Entwickler zu ermutigen, standardisierte Bibliotheken für Kryptographie zu nutzen (statt selbst geschriebene und nur nach einer Beurteilung sichere Software). Es wurde außerdem als Referenz benutzt, um neue Implementationen zu verifizieren.

Nachdem das innerbetriebliche Projekt endete, wurde es dank der Bemühungen von Prof. Bernhard Esslinger und der Unterstützung von Vorstandsmitglied

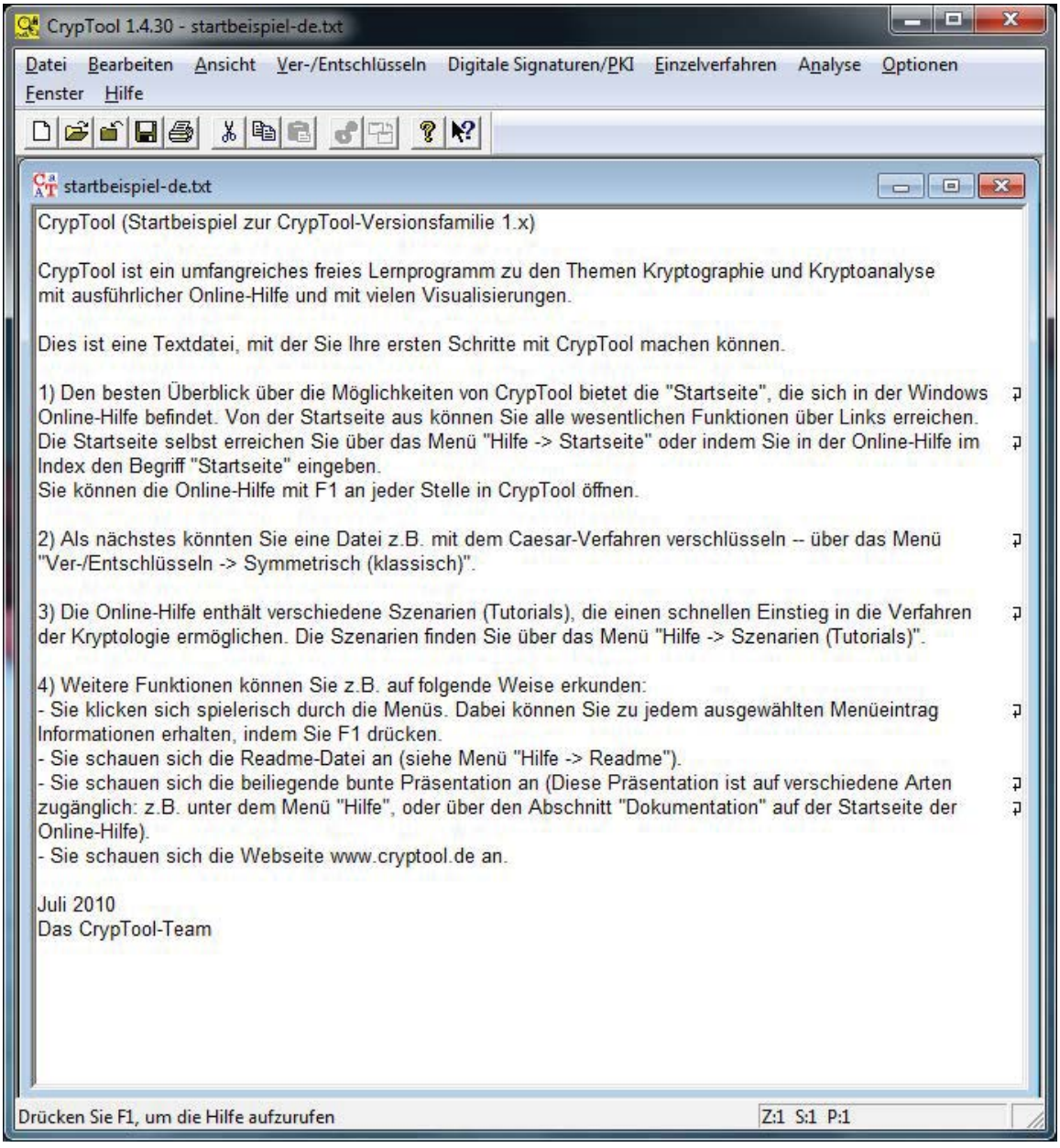

Abbildung 1. *CrypTool 1 – Hauptfenster*

Hermann-Josef Lamberti, der Internet-Community zur Verfügung gestellt und als Freeware im Jahr 2000 veröffentlicht. Seitdem hat sich das CrypTool-Projekt zu einer der vollständigsten Lernplattformen für Krypto -

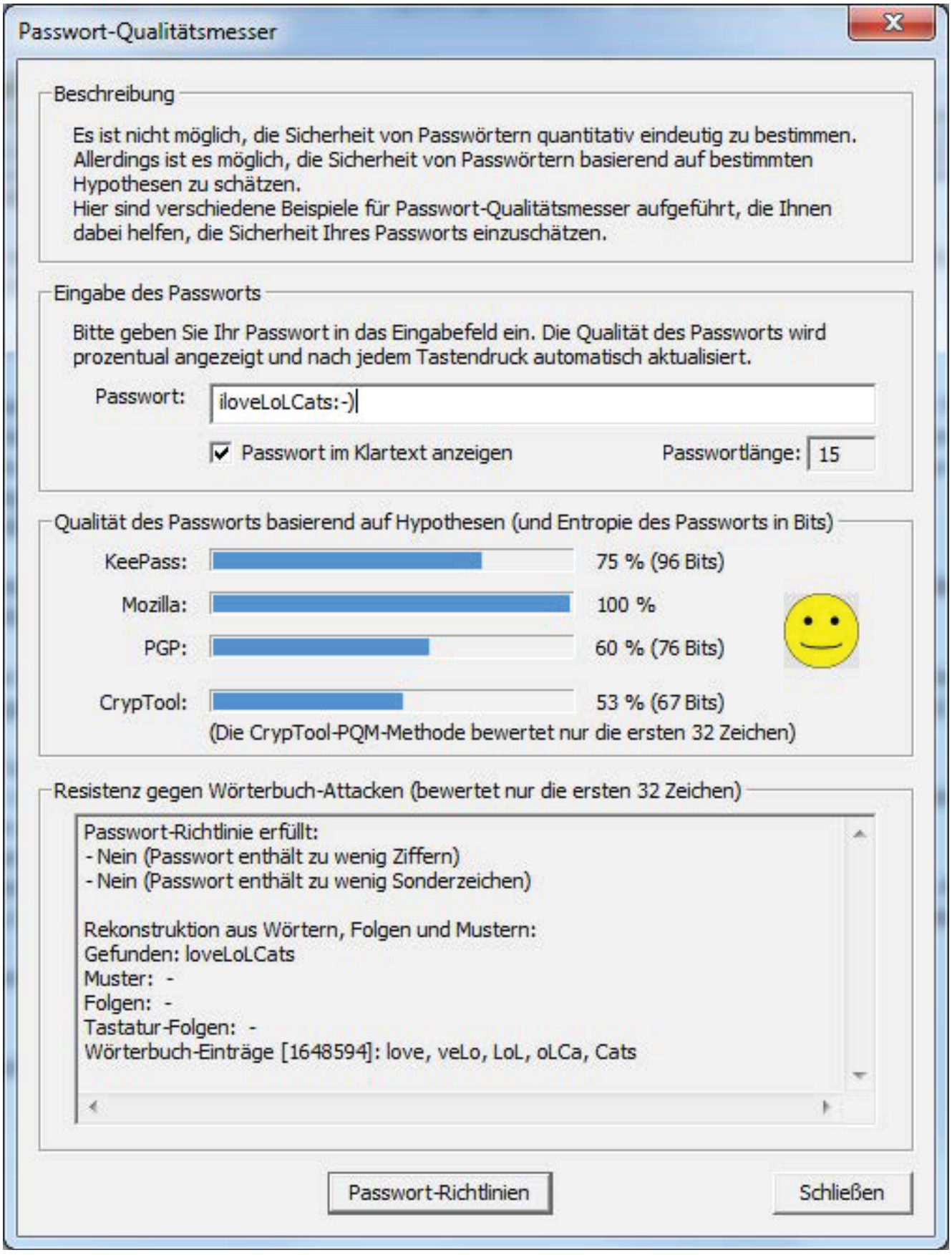

Abbildung 2. *CrypTool 1 – Password-Qualitätsmesser*

CT1	
Month	Downloads
Jan 2010	5.496
Feb 2010	5.628
Mar 2010	6.978
Apr 2010	6.128
May 2010	6.070
Jun 2010	4.550
Jul 2010	4.440
Aug 2010	4.962
Sep 2010	5.122
Oct 2010	6.300
Nov 2010	5.978
Dec 2010	5.297
Sum 2010	66.949

Abbildung 3. *CrypTool 1 wurde 2010 ca. 67 000 mal heruntergeladen.*

graphie entwickelt, die heute verfügbar ist. Im Jahr 2003 wurde CrypTool 1 zu einem von der Universität Darmstadt betreuten Open-Source-Projekt. Aktuell gibt es drei unterschiedliche Software-Implementationen, von denen jede eigene Fähigkeiten, Ziele und Technologien bietet.

CrypTool 1

Anforderungen: Windows XP oder neuer.

CT1 ist das gegenwärtig vollständigste und am weitesten entwickelte CrypTool, es implementiert fast alle wichtigen historischen und state-of-the-art Kryptographie-Funktionen. CT1 ist in C++ implementiert und nur für Win32 Betriebssysteme verfügbar.

Jede implementierte Funktion in CT1 benutzt ein einfach zu verwendendes graphisches Interface und bietet eine ausführliche Online-Hilfe, die auch ohne ein tiefere Kenntnis der Kryptographie verstanden werden kann. Sie enthält außerdem ein Lernprogramm zur Zahlentheorie, eine Visualisierung für sichere E-Mail und verschiedene Verschlüsselungsalgorithmen, um nur einige Beispiele zu nennen. CT1 ist in fünf verschiedenen Sprachen (Deutsch, Englisch, Polnisch, Serbisch und Spanisch) verfügbar. Eine Funktion von CT1, die für fast jeden nützlich sein kann, ist der Passwort-Qualitätsmesser (PQM). Es gibt unzählige ähnliche Programme online, aber die meisten verlangen, dass man das zu prüfende Passwort an einen Server sendet. Damit riskiert der Benutzer, dass jemand möglicherweise

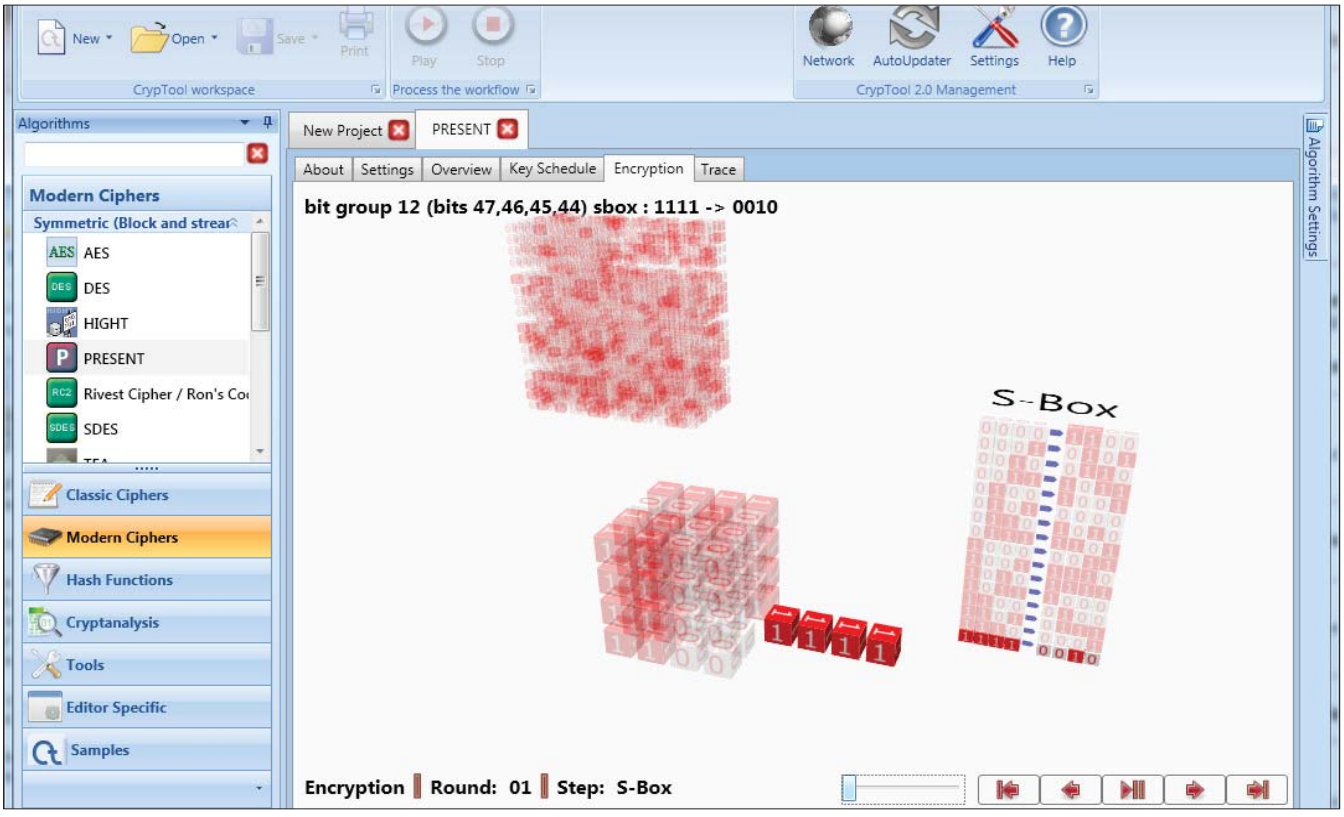

Abbildung 4. *CrypTool 2 – Visualisierung der PRESENT-Chiffre (z.B. für RFIDs)*

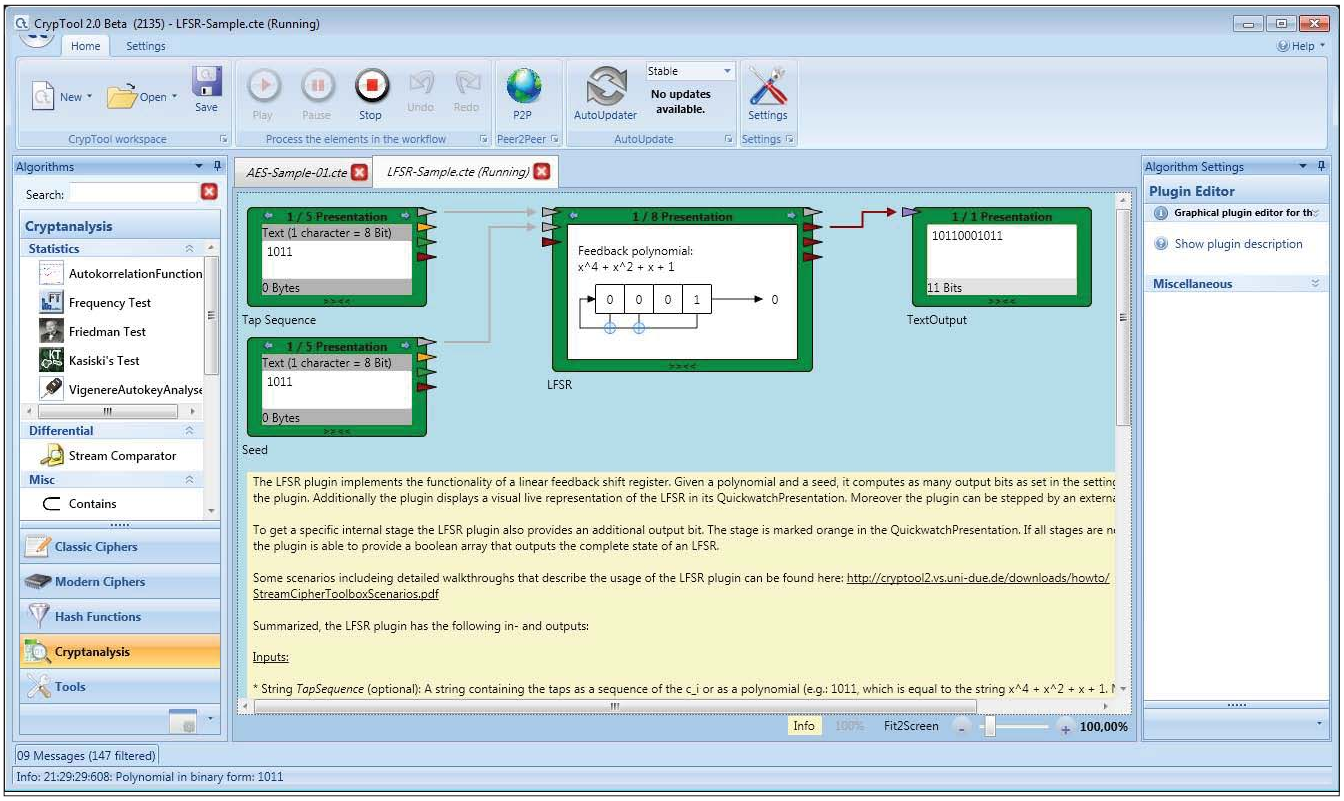

Abbildung 5. *CrypTool 2 – „Arbeitsplatz" mit einem LFSR (linear rückgekoppeltes Schieberegister)*

CT2	
Month	Downloads
Dec 2010	5.496
Nov 2010	5.161
Oct 2010	4.377
Sep 2010	3.681
Aug 2010	2.664
Jul 2010	2.480
Jun 2010	2.427
May 2010	3.231
Apr 2010	4.612
Mar 2010	3.863
Feb 2010	3.492
Jan 2010	2.233
Sum 2010	43.717

Abbildung 6. *CrypTool 2 wurde 2010 ca. 44 000 mal heruntergeladen.*

das Passwort für eine spätere Verwendung aufzeichnet. Das PQM, das in CT1 eingebaut wurde, läuft nur lokal auf Ihrem Computer, speichert nichts ab, und bietet mehr, als nur Buchstaben zu zählen und daraus Statistiken zu berechnen: Es vergleicht das Passwort auch mit einem Lexikon, das ebenfalls konfiguriert werden kann. Sie werden sich wahrscheinlich fragen, was ein Passwortcheck mit Kryptographie zu tun hat. Selbst wenn Sie einen der besten Verschlüsselungsalgorithmen verwenden, verlassen diese sich meist auf sichere Passwörter, die schwer herauszufinden oder zu erraten sind, oder auf große oder zufällige Zahlen, um ihr volles Sicherheitspotential zu erreichen.

Im Jahr 2007 wurden die Anforderungen der CT1-Nutzergemeinschaft in einer großen Umfrage zusammengetragen und die Präferenzen der potentiellen Benutzer betrachtet. Ein Ergebnis war, dass die beiden Nachfolger von CT1 beide auf einer reinen Plugin-Architektur beruhen – eines verwendet .NET und C#, und das andere Eclipse, Java und RCP.

CrypTool 2

Anforderung: Windows XP oder neuer, .NET 4.0.

CT2 ist der erste moderne Nachfolger, der aktuelle Entwicklungstechniken und einen komplett neuen didaktischen Ansatz verwendet. CT2 folgt dem Model der visuellen Programmierung und die Benutzeroberfläche orientiert sich am Microsoft Office 2007 User Interface Design. Das Modell der visuellen Program-

mierung ermöglicht es dem Benutzer, ein ausgedehntes Set von Funktionen mit der Maus zu kombinieren, anstatt auf fertige Funktionen beschränkt zu sein. Die grafische Benutzeroberfläche (GUI) basiert auf der Windows Presentation Foundation (WPF) und gibt Benutzern die Möglichkeit, das Bild nach Belieben zu skalieren. Das CT2-Projekt wird von der Universität Duisburg entwickelt und betreut. Die Leitung hat Dr. Wacker.

Eine sehr interessante Funktion, die vor kurzem implementiert wurde, ist die Möglichkeit zum verteilten Rechnen. CT2 kann ein ad-hoc Peer-to-peer-Netzwerk aufbauen, um rechenaufwändige Aufgaben zu beschleunigen.

Eine Besonderheit, die wir hier vorstellen möchten, ist das modulare Design. Es bietet einen Werkzeugkasten mit logischen Arbeitsabläufen auf der linken Seite. Sie können diese Werkzeuge verwenden, um kryptographische Funktionen zu implementieren, Arbeitsabläufe aufzubauen und sie gegen andere Analyse-Werkzeuge zu testen. CT2 bietet sogenannte Arbeitsplätze (work spaces) und eine Schritt-für-Schritt-Ausführung der Tests. Lehrer können dies benutzen, um Aufgaben für ihre Schüler vorzubereiten, um so die knappe Zeit in Übungen besser zu nutzen.

CT2 ist gegenwärtig als Beta 3 in Deutsch und Englisch verfügbar.

CT2 enthält mehr als hundert vordefinierte „Arbeitsplätze“, um darzustellen, wie die Plugins verwendet werden können. Der folgende Screenshot zeigt die Benutzung eines linear rückgekoppelten Schieberegisters (LFSR), das Schritt für Schritt analysiert werden kann.

JCrypTool

Anforderungen: Alle Plattformen mit Java run-time environment 1.6

JCT ist der Zwilling von CT2: Der zweite Nachfolger von CT1, allerdings mit anderen Zielen als CT2. Die Hauptanforderung, die es erfüllt, ist die Plattform-Unabhängigkeit. JCT wird ebenfalls als Open-Source-Projekt entwickelt. Es basiert auf der Eclipse Rich Client Platform (RCP) und ermöglicht es Studenten, Lehrern, Entwicklern und allen an Kryptographie Interessierten, kryptographische Algorithmen in einem modernen und einfach zu verwendenden Programm anzuwenden und zu analysieren. Es verwendet sowohl BouncyCastle als auch FlexiProvider als Krypto-Service-Provider. Dank FlexiProvider bietet es nicht nur Algorithmen, die bereits die Standardisie-

Abbildung 7. *JCrypTool – Startbildschirm*

rung durchlaufen haben, sondern auch Algorithmen aus der gegenwärtigen Forschung, vor allem solche aus dem Post-Quantum-Umfeld. JCT Release Candidate 4 (RC4) ist gegenwärtig in Deutsch und Eng - lisch verfügbar. Es wird auf SourceForge gehostet. Das JCT-projekt wird von Dominik Schadow geleitet. Das durchschnittliche Ranking von JCT auf Source-Forge liegt in den Top 300-3000 (von 180.000 registrierten Projekten).

Ein anschauliches Feature von JCT ist die eingebaute Visualisierung der Elliptic curve cryptography (ECC). ECC ist eine sehr interessante Technologie, die bei Nutzung weitaus kleinerer Schlüssel gleiche Sicherheit wie RSA bietet (ein 512 bit Schlüssel mit ECC entspricht der Sicherheit eines 15.260 bit RSA-Schlüssels). Dies ist vor allem für Geräte interessant, die keinen Platz für große Schlüssel haben, wie zum Beispiel eine Smartcard. Das Konzept hinter ECC wird im nachfolgenden Screenshot über reelen Zahlen gezeigt, es kann aber auch über einem diskreten Feld über p oder 2^m visualisiert werden.

Ein Aufruf an alle Interessierten

Das CrypTool-Projekt ist seit über 10 Jahren erfolgreich und ein Beispiel dafür, was Open Source errei - chen kann. Zum CT-Projekt gehören weitere verwandte Projekte wie CrypT ool-Online, das alle Codes und Funktionen ohne Installation direkt im Browser anbie - tet. *CrypTool-Mobile* bietet die Funktionen für moderne Smartphones an.

Ein anderes verwandtes Projekt, das vor kurzem mit drei deutschen Universitäten und Aufgaben-Autoren aus der ganzen W elt gestartet wurde, ist der in - ternationale Kryptographie-Wettbewerb *MysteryTwister C3*, bei dem Sie Ihre Kryptographie-Fähigkeiten testen können. Mit richtigen Lösungen können Sie in die Hall-of-Fame gelangen, oder Sie können in den moderierten Forem ihre Lösungsansätze und Fragen diskutieren.

Kryptographie umgibt uns überall und ich hoffe, dass wir mehr Menschen dazu ermutigen können, mehr über diese faszinierende Wissenschaft zu erfahren. Auf der CrypTool-Website finden Sie auch die offiziel-

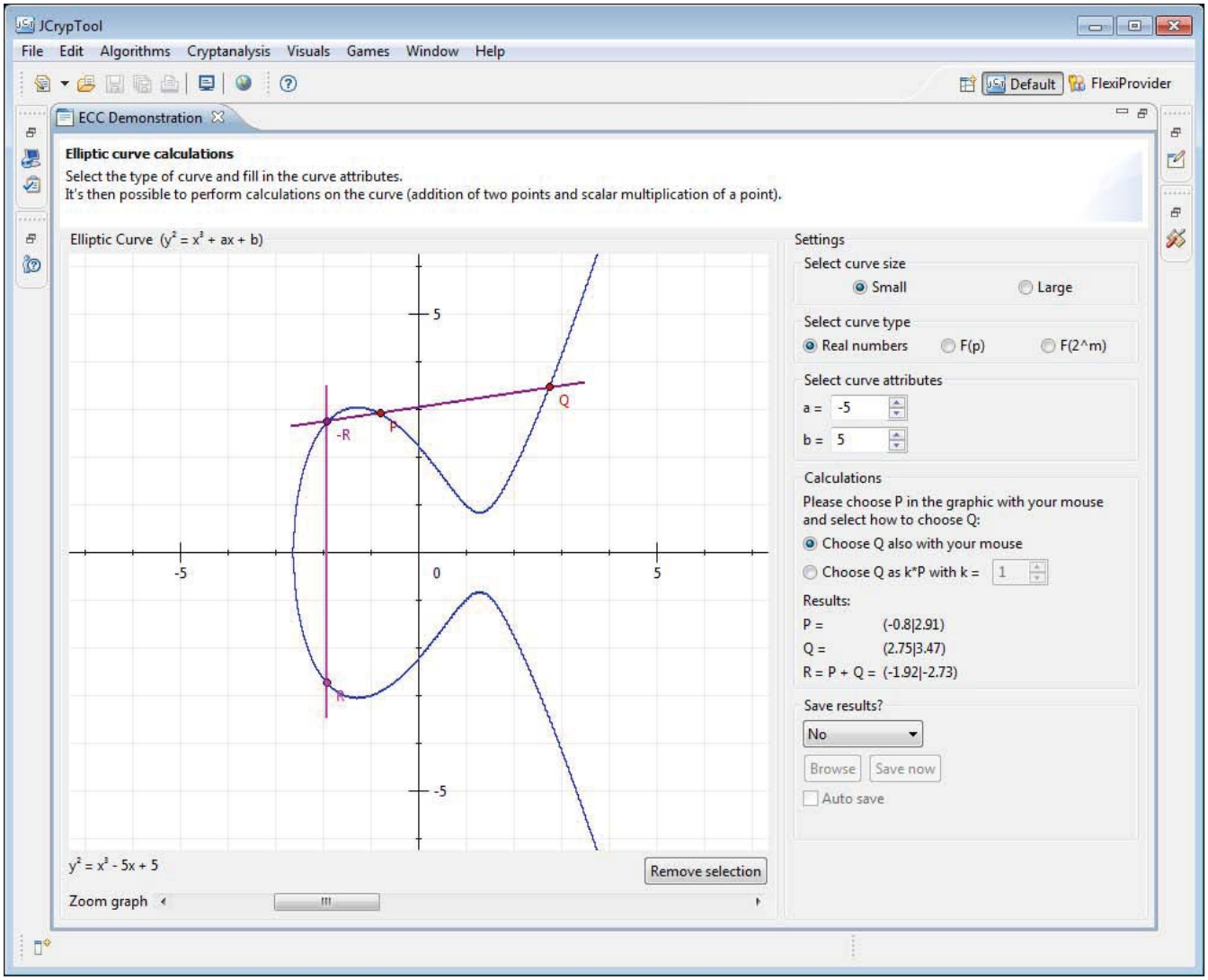

Abbildung 8. *JCrypTool – Elliptic curve cryptography-Visualisierung*

Links:

- *http://www.cryptool.org/* – Homepage des CrypTool-Projektes;
- *http://jcryptool.sourceforge.net/JCrypTool* – Entwickler-Homepage von JCT;
- *http://www.cryptool2.vs.uni-due.de* – Entwickler-Homepage von CT2;
- *http://www.cryptool.org/download/CrypToolPresentation-de.pdf* – Projektpräsentation;
- *http://www.cryptool-online.org/* – Homepage der Browser-Variante;
- *http://m.cryptool-online.org/ oder http://m.cryptool.org* – Homepage der Smartphone-Variante;
- *http://www.mysterytwisterc3.org/* – Internationaler Krypto-Verschlüsselungs-Wettbewerb MTC3.

JCT				
Month	Rank	Total Pages	Downloads	Proj. WebHits
Dec 10	1.479	7.519	835	24.774
Nov 10	1.512	16.424	922	26.884
Oct 10	810	25.495	905	29.268
Sep 10	719	9.267	745	23.518
Aug 10	477	5.032	558	21.103
Jul 10	829	2.523	689	22.960
Jun 10	652	3.561	784	21.673
May 10	1.019	7.552	867	26.155
Apr 10	1.674	8.751	870	26.514
Mar 10	1.664	6.960	1.002	30.185
Feb 10	1.032	5.196	838	26.377
Jan 10	376	8.485	845	26.673
Sum/Avg	1.020	106.765	9.860	306.084

Abbildung 9. *JCrypTool wurde 2010 ca. 10 000 mal heruntergeladen (Statistik aus SourceForge)*

le Projekt-Präsentation, in der Sie die Möglichkeiten von CrypTool in Bildern gezeigt bekommen. Ihre Vorschläge, konstruktive Kritik und Feedback sind dem Projekt jederzeit willkommen. Gegenwärtig unterstützen mehr als 50 Menschen weltweit in ihrer Freizeit das Projekt. Einige Unterstützer haben zugestimmt, ihre Informationen zu veröffentlichen – diese können online abgerufen werden unter http://www .cryptool.org/index.php/en/contributors-aboutmenu-36.html.

MysteryTwister C3 - Level I - Zahlenfolge-Aufgabe
Was ist die nächste Zahl in dieser Sequenz?
1 - 2 - 4 - 6 - 10 - 12 - 16 - 18 - 22 - 28 - 30 - 36 - 40 - ?
Wie haben Sie die Lösung gefunden?
– Besuchen Sie die MTC3-Homepage, um mehr Aufgaben zu diskutieren.

Das Projekt wird in seinen weiteren V ersionen hoffentlich noch mehr Menschen unterstützen, Krypto - graphie zu verstehen und sinnvoll einzusetzen.

ARKADIUS C. LITWINCZUK
Der Autor arbeitet als IT-Security-Berater und Entwickler rund um das Gebiet der Kryptographie.
Kontakt: Arkadius.Litwinczuk@gmail.com

Hakin9

HARD CORE IT SECURITY MAGAZINE .PDF

Hakin9 Monats- Online-Magazin; Ausgabe 2/2011 Februar

DIE WIKILEAKS STORY
DIE WAHRHEIT RUND UM DAS THEMA DATENSCHUTZ

PHP Trojaner
Gefahren für Opensource

CrypTool-Projekt
Der beste Weg, Kryptographie zu lernen und anzuwenden

DNSSEC: Wirksamer Schutz für das Domain Name System

PLUS

DAS PROJEKT „DATENSCHUTZ GEHT ZUR SCHULE“
DAMIT PRIVATES PRIVAT BLEIBT