# VerSchlüsselerlebnisse NG

**Auf interessante Weise Wissen um Kryptografie und Kryptanalyse zu vermitteln ist nicht einfach. Cryptool ist ein kostenloses E-Learning-Tool, das dabei hilft, die Security- und Krypto-Awareness von Mitarbeitern zu verbessern. Zum zehnjährigen Jubiläum erscheint nun eine neue Generation der Software, die aktuelle Programmier-Trends und Möglichkeiten zur Partizipation aufgreift.**

*Von Philipp Südmeyer, London, und Bernhard Esslinger, Frankfurt*

Das Jahr 1998 war die Geburtsstunde des Cryptool-Projekts: Damals wurde in der Deutschen Bank AG mit der Entwicklung einer Software für die Security-Awareness begonnen. Im Laufe der vergangenen 10 Jahre ist diese Applikation zur weltweit beliebtesten E-Learning-Software im Bereich Kryptologie avanciert.

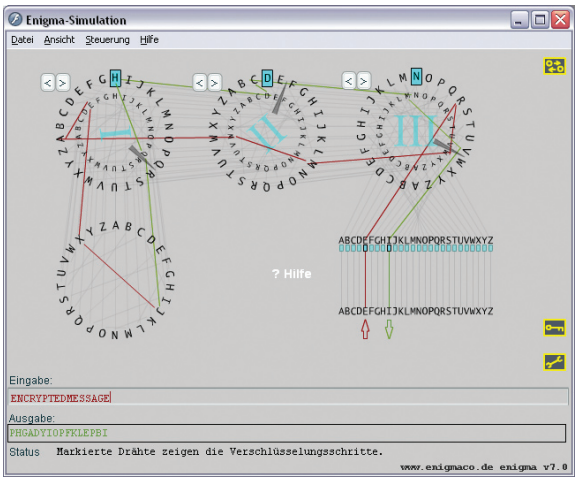
Ursprung des Awareness-Programms war damals wie heute die Einsicht, dass der Mensch üblicherweise der kritische Faktor in einem Sicherheitskonzept ist. Entsprechende Trainings zum Sicherheitsbewusstsein sind daher essenziell für die Informationssicherheit im Unternehmen. Die Deutsche Bank wollte ihren Mitarbeitern die Signifikanz guter kryptografischer Verfahren softwareunterstützt näher bringen.

Aus dieser firmeninternen Initiative ist unter der Leitung von Bernhard Esslinger ein Projekt gewachsen, das nicht mehr nur Interne, sondern auch die interessierte Öffentlichkeit zur Zielgruppe hat: Cryptool wird seit vielen Jahren als Open-Source-Projekt weiterentwickelt, das weltweit Nutzer und Unterstützer findet. Ferner ist im April 2008 das Cryptoportal für Lehrer online gegangen (www.cryptoportal.org), das von Lehrern für Lehrer betrieben wird und eine Möglichkeit bietet, sich über die Krypto-Lehre an Schulen auszutauschen. Das Cryptool-Projekt ist hier vornehmlich der Träger und Betreiber der Plattform. Die Idee zum Portal entstand im Rahmen einer Tagung der Gesellschaft für Informatik (GI), auf der Lehrern die Nutzung von Cryptool als didaktisches Werkzeug vorgestellt wurde.

Vor allem durch die positiven Reaktionen aus dem akademischen Umfeld hat sich das zunächst rein deutsche Projekt immer internationaler ausgerichtet. Seit kurzem stehen sowohl die Projekt-Website als auch die Software in vier Sprachen zur Verfügung: Deutsch, Englisch, Polnisch und Spanisch.

Die E-Learning-Software Cryptool erschließt dem Nutzer eine breite Palette klassischer und moderner kryptologischer Methoden. Von Anfang an wurde darauf geachtet, sowohl kryptografische Verfahren als auch die dagegen anwendbaren Kryptanalysen so aufzubereiten, dass der Nutzer die jeweiligen Techniken spielerisch erfahren kann. Um gezielt auch den unerfahrenen Anwender erreichen zu können, wurde besonders auf eine ausführliche und klar verständliche kontextsensitive Onlinehilfe Wert gelegt, die sowohl Informationen zur Bedienung des jeweiligen Dialogs gibt als auch über das gerade genutzte kryptologische Verfahren informiert.

Ergänzend zur E-Learning-Software werden stets ein aktuelles Skript sowie eine Präsentation zum Thema Kryptologie bereitgestellt.




*Visualisierung der Funktionsweise der Enigma in Flash (Cryptool 1.x)*

## Cryptool 1.x

Die gesamte 1.x-Serie der Cryptool-Applikation ist primär in C++ programmiert. Im Laufe der Zeit wurde das Programm teilweise um Funktionen erweitert, die in anderen Sprachen entwickelt wurden. So sind beispielsweise sowohl der Advanced Encryption Standard (AES bzw. Rijndal) als auch die Chiffriermaschine Enigma in Flash visualisiert. Insgesamt wartet das aktuelle Cryptool-Release 1.4.20 mit weit über 60 Krypto-Funktionen auf.

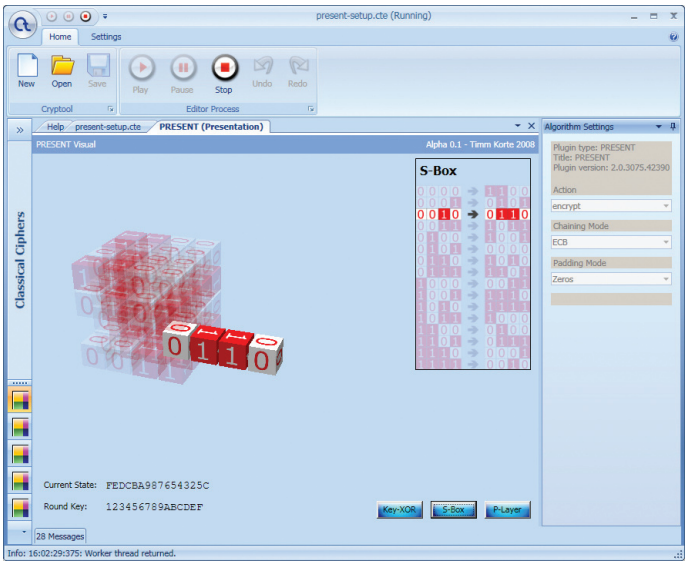
Cryptool 1.x basiert auf einer monolithischen Kern-Architektur; zum Zeitpunkt seiner Erst-Entwicklung

entsprach das Programm damit aktuellen Standards und Programmieransätzen. Die IT hat sich in den vergangenen zehn Jahren jedoch mit rasender Geschwindigkeit weiterentwickelt: Neue Programmiersprachen sind entstanden, die im Allgemeinen objektorientiert sind; programmiert wird heute in ausgereiften Entwicklungsumgebungen. Für viele grundlegende Bereiche stehen so genannte Frameworks zur Verfügung, sodass sich der Entwicklungsprozess im Software-Lebenszyklus weiter straffen lässt. Das Internet hat sich mittlerweile zu einem omnipräsenten Medium entwickelt, das in der Informationsgesellschaft als selbstverständlich angesehen wird – XML und Web-Services finden immer mehr Anklang und eines der zurzeit am meisten beachteten IT-Themen sind serviceorientierte Architekturen (SOA).

Nach vielen Jahren der Weitereinwicklung von Cryptool 1.x ist es daher Zeit für einen Generationswechsel: Um den Nutzern eine moderne Anwendung liefern zu können, erfährt Cryptool eine Generalüberholung. Mit ehrgeizigem Ziel wird seit rund einem Jahr an einem zeitgemäßen Nachfolger für Version 1.x gearbeitet. Beim Entwurf der Software-Architektur stand eine Prämisse im Vordergrund: Die Nachfolgeversion soll neuesten Standards der Software-Entwicklung folgen und damit besonders reizvoll für freiwillige Helfer sein. Des Weiteren sollten moderne Design-Ansätze der Benutzerschnittstelle (Graphical User Interface, GUI) implementiert werden. Diesen Grundgedanken folgend wurde das Projekt in zwei verschiedene Ansätze aufgeteilt: eine auf Java und dem Eclipse-Framework basierende und eine auf dem .NET-Framework aufsetzende Architektur.

## Cryptool 2.0

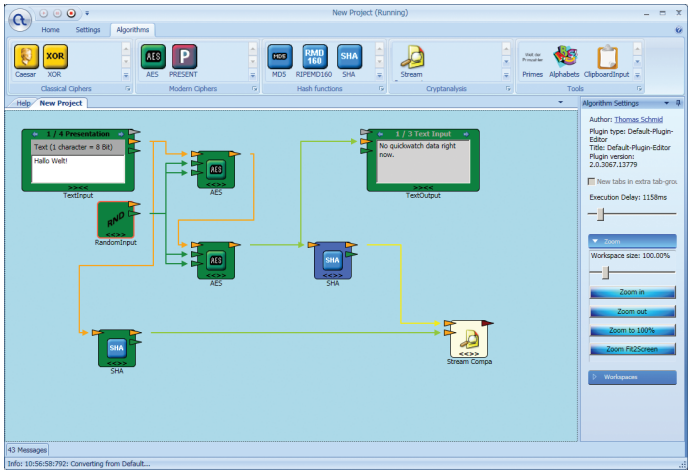
Die Architektur für Cryptool 2.0 haben allen voran Mitarbeiter des Fachgebiets „verteilte Systeme“ der Universität Duisburg-Essen entworfen; Grundlage ist Microsofts Framework .NET 3.5. Die grafische Oberfläche wird in der Windows Presentation Foundation (WPF) entwickelt: Dadurch lassen sich alle in Cryptool 2.0 dargestellten Grafiken frei skalieren, was beispielsweise bei der Visualisierung kryptologischer Verfahren sehr nützlich ist.




*Visualisierung der Blockchiffre PRESENT (Cryptool 2.0)*

Cryptool 2.0 stellt eine Pure-Plug-in-Architektur dar: Die Basisapplikation besteht primär aus einer Laufzeitumgebung zum Ausführen von Plug-ins. Den so genannten Kernel bildet das CrypCore-Modul, das vornehmlich das Auffinden und Laden von Plug-ins übernimmt. Die Benutzerschnittstelle steht derzeit in Form des CrypWin-Moduls als GUI bereit (s. u.). Über das Modul CrypConsole soll Cryptool 2.0 darüber hinaus eines Tages auch über die Eingabeaufforderung nutzbar werden: So ließen sich die Cryptool-Funktionen in Batch-Dateien verwenden. Die CrypPluginBase bildet die technische Infrastruktur für Plug-in-Entwickler, aber beispielsweise auch Funktionen zum Öffnen, Bearbeiten oder Vergleichen von Dateien.

In Form der CrypPlugins wird die eigentliche Funktionalität von Cryptool 2.0 abgebildet: Durch den völlig modularen Ansatz und die Eigenschaft, jede Einzelfunktion




*Visuelle Programming mit Cryptool 2.0*

## Einladung zum Tag der offenen Tür

Das Institut für Wirtschaftsinformatik in Siegen hatte sich mit dem Cryptool-Projekt bei dem bundesweiten Wettbewerb „365 Orte im Land der Ideen“ in der Kategorie Wissenschaft und Technik beworben. Unter den rund 1500 Bewerbern wurde Cryptool von einer prominenten Jury als einer der „365 plus 1“ ausgewählten Orte 2008 gekürt; prämiert werden Orte, die zukunftsorientierte Ideen entwickeln und aktiv umsetzen. Das Gesamtprojekt wird in einer öffentlichen Veranstaltung am 22. Juli 2008 im Rahmen eines Tags der offenen Tür an der Universität Siegen vorgestellt. Näheres unter www.land-der-ideen.de/CDA/ort_des_tages,1987,1,,de.html?action=detail&id=4477

durch ein separates Plug-in abzubilden, ist die Einstiegsschwelle für neue Entwickler im Software-Projekt auf ein Minimum reduziert worden. Um das Mitmachen weiter zu vereinfachen, stehen außerdem „How-to“-Hilfen bereit, die Schritt für Schritt die Entwicklung eines einfachen Plug-ins beschreiben.

Um ein hohes Maß an Sicherheit und Qualität zu gewährleisten, können im Standard-Modus von Cryptool 2.0 lediglich solche Plug-ins genutzt werden, die das Cryptool-Team digital signiert hat. Programmierer können ihre Plug-ins aber in einem speziellen Entwickler-Modus nutzen. Alle durch das Cryptool-Team signierten Plug-ins sind zukünftig mithilfe eines integrierten Web-Service-Clients abrufbar. So lässt sich Cryptool 2.0 in einer Basisversion herunterladen und zur Laufzeit um benötigte Funktionen erweitern.

### Visuelle Programmierung

Im Rahmen einer Diplomarbeit zum Thema visuelle Programmierung in moderner Component-Plug-in-Architektur hat Thomas Schmid an der Uni Siegen einen grafischen Editor als CrypWin-Modul entwickelt (http://cryptool2.vs.uni-due.de), der die visuelle Programmierung kryptografischer Protokolle per Drag-and-Drop unterstützt: Der Editor ermöglicht die Verkettung verschiedener Plug-ins zu einer Prozesskette. Solche Prozessketten werden auf einer grafischen Arbeitsfläche erstellt und arbeiten nach dem Datenflussprinzip: Die enthaltenen Komponenten sind die für Cryptool 2.0 bereitgestellten Plug-ins, die das Hauptmenü des GUI nach Themen sortiert auflistet.

Der Benutzer kann ein Plug-in per Drag-and-Drop auf die Arbeitsfläche ziehen, woraufhin es dort als Icon erscheint, dessen Ein- und Ausgänge entsprechend ihres Typs farblich markiert sind, sodass man leicht erkennen kann, welche Schnittstellen grundsätzlich miteinander zu verbinden sind. Durch Ziehen eines Plug-in-Ausgangs zum gewünschten Eingang des Folge-Plug-ins lassen sich zwei Module zusammenschalten. Der Editor verhindert die Erstellung syntaktisch fehlerhafter Programme, indem nur Verbindungen zwischen passenden Schnittstellentypen zugelassen werden: Wenn der Nutzer versucht zwei inkompatible Schnittstellen miteinander zu verbinden, leuchtet der Endpunkt der Verbindung rot auf.

Neben dieser intuitiven Steuerung wird der Benutzer durch zusätzliche Tooltips und einen einheitlichen Dialog zur Konfiguration der Plug-ins unterstützt. Dieser Konfigurationsdialog wird in einem zentralen Fenster der Cyptool-Oberfläche angezeigt, sodass immer klar ersichtlich ist, an welcher Stelle man Anpassungen vornehmen kann.

Zudem können Plug-ins ausführliche Beschreibungen und Präsentationen der Datenverarbeitung bereitstellen: Diese Elemente werden durch den Editor in eigenen „Karteikarten“ (Tabs) dargestellt, sobald der Nutzer einen Doppelklick auf das zugehörige Icon durchführt. Als erste Implementierung dieser Art ist im Rahmen einer Bachelor-Arbeit an der Ruhr-Universität Bochum die voll funktionsfähige Visualisierung des Algorithmus PRESENT entstanden, einer speziell für ressourcenschwache Hardware (z. B. RFIDs) entwickelten Blockchiffre (www:lightweightcrypto.org/present).

## JCrypTool

Das JCrypTool-Projekt hat das Ziel, einen plattformunabhängigen Nachfolger für Cryptool 1.x zu liefern. Als Programmiersprache wurde Java und als Basis für die Applikation die Eclipse Rich Client Platform (RCP) ausgewählt. Letztere erfreut sich aufgrund ihrer Flexibilität und Mächtigkeit vor allem bei Enterprise-Applikationen zunehmender Beliebtheit. Durch das robuste RCP-Framework und dessen Plug-in-Orientierung lässt sich auch JCrypTool leicht um zusätzliche Funktionen erweitern. Zusätzlich stellt das RCP-Framework Infrastrukturfunktionen für die Applikation bereit: Auf diese Funktionen können Programmierer von JCrypTool-Plug-ins bei der Entwicklung zurückgreifen und sich somit bei der Entwicklung auf die Integration ihres spezifischen Fachwissens konzentrieren.

Im August 2007 ist eine erste Entwicklerversion – „Milestone 1“ – veröffentlicht worden, um

## Literatur

[1] Cryptool, Projekt-Homepage, www.cryptool.org

[2] Bernhard Esslinger, VerSchlüsselerlebnisse, CrypTool unterstützt Verständnis für die Grundlagen der Internetsicherheit

Entwicklern eine stabile Basis für die Weiterentwicklung von JCrypTool zur Verfügung zu stellen. Diese erste Version verfügt über Plug-ins für klassische und moderne kryptografische Verfahren. Der für Ende Juni 2008 geplante „Milestone 2" wird über mehr Funktionen verfügen und sich auch schon an Endanwender richten. So wurde unter anderem die kryptografische Bibliothek FlexiProvider des Fachbereichs Kryptographie und Computer-Algebra an der Technischen Universität Darmstadt integriert: Diese Bibliothek bietet modernste kryptografische Verfahren an, die mit JCrypTool angewendet werden können. Ein weiterer Bestandteil von Milestone 2 wird eine neue Version des aus Cryptool 1.x bekannten „Zahlenhais" sein, einem Spiel zum Umgang mit Teilern und Primfaktoren. Zusätzlich bietet Milestone 2 mehr Beispiel-Plug-ins, die als Vorlage für Entwickler dienen werden. Die ersten offiziellen Release-Versionen von JCrypTool und Cryptool 2.0 werden im Jahre 2009 erscheinen.

## Neue Website

Zeitgleich mit der Veröffentlichung der Alpha-Version von Cryptool 2.0 ist auf www.cryptool.de auch ein neues Webdesign online gegangen – die neue Seite verdeutlicht, dass sich im Projekt große Veränderungen anbahnen. Interessierte Leser sind herzlich eingeladen, sich auf den neuen Cryptool-Webseiten umzusehen. Das Team freut sich über Feedback – und mehr noch über ambitionierte Menschen, die ihren Teil zu diesem gemeinnützigen Projekt beitragen wollen. ■

*Philipp Südmeyer (Philipp.Suedmeyer@db.com) ist Enterprise Security Strategist & Designer bei der Deutschen Bank AG. Bernhard Esslinger (bernhard.esslinger@db.com) ist Leiter des Kryptografie-Kompetenzzentrums bei der Deutschen Bank AG und Professor für IT-Security an der Uni Siegen.*

# *Verantwortlich für die IT-Sicherheit…*

**<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.**

**Jetzt Probeheft anfordern!**


<kes>

- liefert Ihnen strategisches Know-how, damit Sie eine solide Grundlage zur Entscheidungsfindung haben
- berichtet über Trends und Neuentwicklungen
- gibt Hilfen zum Risikomanagement
- erläutert einschlägige Gesetze im Umfeld der IT und TK
- informiert über die wichtigsten Messen und Kongresse
- ermöglicht es Ihnen durch Anwenderberichte von den Erfahrungen anderer zu profitieren
- gibt mit Marktübersichten einen Überblick über ausgewählte Produkte und Dienstleistungen

## *<kes>-online*

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung, das Thema der Woche und außerdem aktuelle Artikel zum Probelesen.

Abonnenten erhalten zusätzlich ein Passwort mit dem sie Zugriff auf alle aktuellen Artikel und auch auf das Online-Archiv erhalten.

## *ABONNEMENT-BESTELLUNG*

☐ **Ich abonniere die Zeitschrift <kes> ab Heft Nr.....**
**Als Dankeschön erhalte ich das erste Heft gratis.**

Das Abonnement enthält ein Passwort zur Nutzung des Abo-Bereichs auf www.kes.info mit allen aktuellen Beiträgen und dem <kes>-Archiv.
Ich kann das Abonnement bis 14 Tage nach Erhalt des ersten Exemplars formlos widerrufen.

Nach Ablauf der Widerrufsfrist wird das Abonnement zu den regulären Bedingungen gültig:

Jahresbezugspreis (6 Ausgaben) € 122,00 inkl. MwSt. und Versandkosten (Schweiz SFr 238,00 / restl. Ausland € 137,00).

Der Jahresbezugspreis wird jeweils für ein Jahr im Voraus berechnet. Eine Kündigung des Abos ist dennoch jederzeit zur nächsten nicht gelieferten Ausgabe möglich. Überbezahlte Abogebühren werden rückerstattet.

Ich bin einverstanden, dass die Deutsche Post AG eine eventuell geänderte Anschrift weitergibt.

## *PROBEHEFT-ANFORDERUNG*

☐ Bitte schicken Sie mir gratis und unverbindlich ein Exemplar der <kes> - Die Zeitschrift für Informations-Sicherheit zum Probelesen zu.

Datum | Zeichen | Unterschrift

Lieferung bitte an

Telefon Durchwahl

## FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Abonnenten-Service
Postfach 12 34
55205 Ingelheim