DuD
Datenschutz und Datensicherheit

CrypTool – spielerischer Einstieg in klassische und moderne Kryptographie

Neue Version – fundierte Awareness in Deutsch und Englisch

Bernhard Esslinger

CrypTool ist ein Freeware-Programm, das einen spielerischen Einstieg in die Kryptographie bietet. Sowohl die Funktionalität als auch die Online-Dokumentation sind beträchtlich. Das in über vierjähriger Arbeit entwickelte Programm wird in Firmen zur Sensibilisierung für IT-Sicherheit und an Schulen und Hochschulen in Ausbildung und Lehre eingesetzt.

Bernhard Esslinger

Leiter IT-Sicherheit Deutsche Bank AG, Lehrbeauftragter IT-Sicherheit Universität Siegen, Schwerpunkte Strategische Konzepte im Konzern, Public-Private-Partnership, Aufbau interoperabler PKI-Strukturen.
E-Mail: bernhard.esslinger@db.com

Einleitung

Kryptographie ist ein hochaktuelles Thema, zu dem es inzwischen viele Bücher und eine aktive wissenschaftliche Forschung gibt: Firmen schützen ihre Daten damit, der Gesetzgeber ermöglicht damit digitale Unterschriften und in vielen Bereichen ist Kryptographie inzwischen Teil unseres Alltags geworden (Auto-Wegfahrsperren, sichere E-Mail, SSL-Browser-Verbindungen, verschlüsselte Fernsehkanäle, ...).

Vor über vier Jahren stellten wir bei internen Reviews fest, dass viele Entwickler unseres Hauses dann Krypto-Standards einhielten, wenn sie regulatorisch oder aus Interoperabilitätsgründen vorgeschrieben waren, dass sie an vielen Stellen aber auch „geniale“ eigene Kryptofunktionen erstellt hatten. Anweisungen und Richtlinien, solche Funktionen nur aus Standardbibliotheken zu nutzen, sind daher nur die halbe Miete. Viel wichtiger ist es, ein Grundverständnis zu schaffen. Die Toolsammlungen aus dem Internet, die vielen Büchern auf CD beiliegen, erfüllten diesen Anspruch bisher jedoch nicht.

1 CrypTool – wozu?

IT-Security-Management beinhaltet neben Risikoanalyse, optimaler Business-bezogener Organisation, Aufbau und Leben einer Policy sowie der entsprechenden Nutzung von Technologien wie Firewalls, Virenschutz und Authentisierungs- und Autorisierungsmechanismen noch ein weiteres wichtiges Gebiet: Aufklärung, Sensibilisierung, Awareness – all die psychologischen Aspekte, ohne die die anderen Maßnahmen nicht erfolgreich sein können.

Aber auch weil das Internet immer mehr privat genutzt wird, ist es wichtig, dass man ein Grundverständnis für Kryptographie gewinnt, um seine Daten angemessen gegen Lauschangriffe, Mithören, Diebstahl und Zerstörung zu schützen.

CrypTool ist ein modernes Instrument, das es den Mitarbeitern und Interessierten ermöglicht,

- spielerisch mit den Verfahren der Kryptologie vertraut zu werden und
- die nötige Awareness für IT-Sicherheit zu erwerben.

1.1 „Geniale“ klassische Verfahren

Ursprünglich standen die klassischen Verfahren im Vordergrund: Wenn Entwickler ohne tiefere Kryptographie-Kenntnisse ein Vigenere-ähnliches Verfahren neu erfinden, ist das eine beeindruckende, aus Sicht des 16. Jahrhunderts sogar geniale Leistung (das im 16. Jahrhundert erfundene polyalphabetische Vigenere-Verfahren galt 300 Jahre lang als unknackbar, bis Kasiski und Friedman es geistig durchdrangen).
Als Security-Verantwortlicher nur zu behaupten, das sei gegen die Vorschriften und dass ein Hacker das Verfahren leicht knacken kann, führt daher psychologisch nicht dazu, dass dieser Appell gerne angenommen und umgesetzt wird. Wenn man eine Attacke aber vorführen kann und dem interessierten Entwickler ein Instrument an die Hand gibt, mit dem er auch verstehen kann, was z. B. die statistische Größe Autokorrelation bedeutet und wie mit ihrer Hilfe solche Verfahren sogar systematisch gebrochen werden können, dann ändert sich das Verhalten und unsere Ansprechpartner haben mehr Verständnis für unsere Anliegen.

Daher wurde vor vier Jahren in der Deutschen Bank mit der Entwicklung von CrypTool begonnen.

Ziel war es, zwei Dinge miteinander zu verbinden, von denen normalerweise angenommen wird, sie gehören in verschiedene Welten: a) das Tool sollte „spielerisches Lernen“ unterstützen, es sollte b) aber auch „seriös“ in dem Sinne sein, dass es mathematisch und kryptographisch korrekt ist und dem Stand der Technik entspricht.

1.2 Offene Entwicklung

Im Laufe der Zeit wurden neben den reinen klassischen Verfahren weitere Bereiche der Kryptographie hinzugefügt wie moderne Verschlüsselungsverfahren, Zufallszahlentests oder Faktorisierungsalgorithmen.

Die Entwicklung geschah von vornherein zusammen mit Hochschulen, um die wissenschaftliche Korrektheit zu gewährleisten.

Das Programm war zunächst nur für den innerbetrieblichen Einsatz vorgesehen. Es wurde z. B. auch für die Ausbildung der Auszubildenden und Fachinformatiker eingesetzt. Schon bald konnte das Programm aber als Freeware der Internet-Gemeinde zur Verfügung gestellt werden, da der zuständige Vorstand der Deutschen Bank unsere Ansicht teilte, dass sich alle um IT-Sicherheit kümmern müssen und ihre Erfahrungen dabei austauschen sollten. Außerdem kommen das Feedback und alle Weiterentwicklungen an dem Freeware-Programm natürlich auch wieder der Deutschen Bank zugute.

Dieses Feedback führte z. B. zu der Entwicklung verschiedener Szenarien und Visualisierungen. In den Szenarien werden bestimmte Verfahren und ihre Umsetzung in CrypTool von Anfang bis Ende detailliert erläutert. Bei den Visualisierungen (Demonstrationen) sind aktuelle Verfahren wie die Hybridverschlüsselung oder die Digitale Signatur grafisch aufbereitet.

An der offenen Entwicklung nehmen verschiedene Firmen bzw. Mitarbeiter verschiedener Firmen und Hochschulen teil: Von der Firma Secude stammen die in CrypTool eingebundene Krypto-Bibliothek und Teile der Elliptischen Kurven-Implementation. Das Forschungszentrum Informatik in Karlsruhe trug wesentliche Teile bei. Weitere Teile kamen z. B. von den Universitäten Karlsruhe, Siegen und Gießen. Ebenso waren Studenten der Universitäten Frankfurt und Zagreb beteiligt. Reviews kamen z. B. von Mitarbeitern der Telekom, aber auch von Privatpersonen. Die Deutsche Bank stellte bis zur Version 1.3.03 die Projektleitung und die Maintenance für jedes neue Tool. Mitarbeiter wie Jörg-Cornelius Schneider oder Henrik Koy [Koy, Schneider] setzten etliche Tage ihrer Freizeit für CrypTool ein – ebenso wie viele ungenannte weitere Personen.

Seit Anfang 2002 liegt die monatliche Downloadrate bei 600 CrypTool-Paketen – mit steigender Tendenz.

2 Inhalt der Distribution

Zu einem downladbaren CrypTool-Paket gehören folgende vier Hauptbestandteile:

- Das Programm CrypTool
- Online- und Offline-Dokumentation
- Das Programm AES-Tool
- Die Geschichte „Der Dialog der Schwestern“

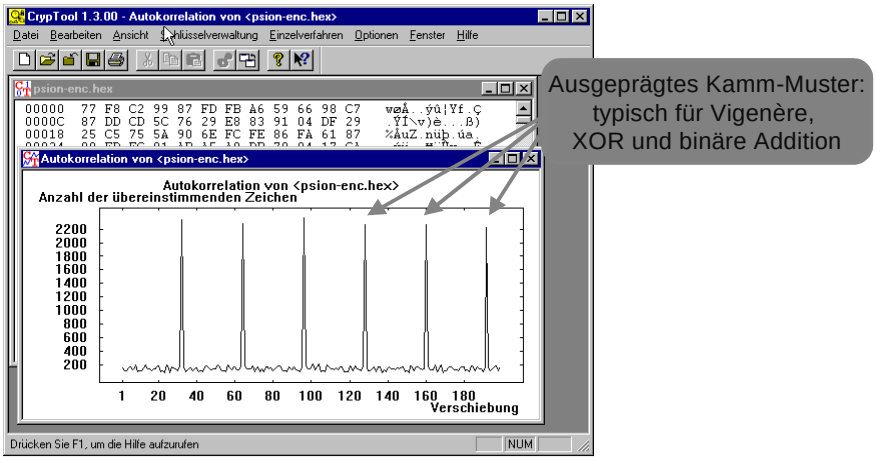

Abb. 1: Autokorrelationsanalyse einer klassisch polyalphabetisch verschlüsselten Nachricht

2.1 Programm CrypTool

Hauptbestandteil des CrypTool-Paketes ist das Programm CrypTool selbst. CrypTool ist keine Applikation, mittels derer im Wirkbetrieb Daten verschlüsselt oder anderweitig gesichert werden sollten.

- In CrypTool ist eine umfangreiche Sammlung kryptographischer Algorithmen implementiert, die hervorragend dokumentiert ist.
- Die meisten der kryptographischen Basisalgorithmen stammen:
  - von der Industrie-bewährten Secude-Bibliothek [Secude] und
  - von der Miracl-Bibliothek [Miracl].

  Somit ist CrypTool auch eine hervorragende Referenzimplementierung.
- Für die meisten klassischen und modernen Verfahren bietet CrypTool spezialisierte Analysealgorithmen. Z. B. kann ein Vigenère-verschlüsselter Text automatisiert entschlüsselt werden. Die Analyse der modernen Verfahren ist eingeschränkt, so dass CrypTool **nicht als Hackertool** eingesetzt werden kann.

2.2 Dokumentation

Zum Programm gehört eine umfangreiche, in deutsch und englisch vorhandene Dokumentation, die aus vier Teilen besteht:

- Readme-Datei: Darin finden sich viele Details zum CrypTool-Projekt und zu weiteren Tools mit ähnlicher Intention.
- Programm-Online-Hilfe, die aus über 200 Seiten besteht. Man kann sie an jedem Punkt des Programms per F1 aufrufen:
  - sie ist kontextbezogen zur Bedienung des Programms und mit weiterreichenden Erläuterungen;
  - sie enthält Tutorials bzw. Beispiel-Szenarien.
- Skript: Ein über 100 Seiten umfassendes Dokument zu Themen der Kryptographie, beigelegt als PDF-Datei. Darin geht es um die mathematischen Hintergründe (didaktisch aufbereitet), aber auch um die aktuellen Forschungsergebnisse zur Sicherheit des RSA-Verfahrens.
- Präsentation, die auf Folien die Möglichkeiten von CrypTool kurz aufzeigt (beigelegt als PDF-Datei).

2.3 Programm AES-Tool

AES-Tool ver- und entschlüsselt Dateien mit dem symmetrischen AES-Verfahren. Es

kann aus CrypTool heraus sowie als eigenständiges Programm aufgerufen werden und besitzt neben der grafischen Oberfläche auch eine Kommandozeilen-Schnittstelle (für den Batch-Betrieb). Optional kann AES-Tool selbstentpackende Executables erstellen, zu deren Entschlüsselung kein weiteres Programm erforderlich ist.

2.4 Kurzgeschichte

Ebenfalls im Paket enthalten ist die Geschichte „Der Dialog der Schwestern“ von Dr. Carsten Elsner. Darin wird von den Titelheldinnen eine Variante des RSA-Verfahren benutzt, um verschlüsselt zu kommunizieren. Diese spannende Geschichte wurde im Computermagazin c't 25/1999 in einer etwas gekürzten Fassung veröffentlicht. CrypTool liegt die ungekürzte Originalfassung bei.

3 Arbeiten mit CrypTool

Mit CrypTool kann man kryptographische Funktionen leicht demonstrieren, aber auch bekannte und unbekannte Verfahren analysieren – beides unter einer einheitlichen grafischen Benutzeroberfläche.

3.1 Der Einstieg

Wenn Sie nach dem Start von CrypTool die F1-Taste drücken, erscheint die Startseite der Online-Hilfe in WinHelp. Diese **Startseite** führt Sie über Links zu allen wesentlichen Komponenten und Funktionen von CrypTool.

Einen schnellen Einstieg in CrypTool finden Sie, wenn Sie einige Szenarien (Tutorials) der Online-Hilfe durchspielen (die Szenarien findet man auch über das Inhaltsverzeichnis der Windows-Hilfe unter „Beginn der Arbeit mit CrypTool“).

> Die Startseite der CrypTool Online-Hilfe ist der ideale Einstiegspunkt in CrypTool. Auch „Dokumentationsverächter“ sollten hierauf einen Blick riskieren.

3.2 AES-Verschlüsselung

Im folgenden wollen wir anhand zweier Beispiele zeigen, was Sie mit CrypTool anfangen können.

Das NIST (National Institute of Standards and Technology) rief 1997 einen Wettbewerb mit den Ziel aus, für die USA ein neues symmetrisches Verschlüsselungsverfahren zu entwickeln. Das öffentlich betriebene Auswahlverfahren hatte eine sehr hohe Transparenz. In CrypTool sind die fünf Kandidaten implementiert, die in die engere Auswahl kamen. Am 2.10.2000 endete das Verfahren: Damit trat der belgische Algorithmus Rijndael als „Advanced Encryption Standard“ (AES) die Nachfolge des inzwischen betagten Data Encryption Standard (DES) an.

Wir wollen im folgenden zeigen (Sensibilisierung), was passiert, wenn man eine zu kurze Schlüssellänge wählt: Dann ist auch der beste Algorithmus nicht gegen einfache Brute-Force-Attacken gefeit.

Wir nehmen an, Sie haben eine Datei (z. B. die mit ausgelieferte Datei deutsch.txt, die typische Muster der deutschen Sprache enthält) geöffnet. Diese verschlüsseln Sie mit dem AES-Algorithmus per **Menü**: Ver-/Entschlüsseln, Symmetrisch, Rijndael. Als Schlüssel geben Sie den (zu kurzen) hexadezimalen Key „16758“ ein. Dies sind nur 20 Bit. Maximal hätten Sie 64 Hexzeichen = 256 Bit eingeben können (intern wird der Rest mit Hex-Nullen aufgefüllt). Wenn ein Angreifer weiss, dass der Schlüssel nur 5 Hex-Zeichen lang ist, kann er mit CrypTool per Brute-Force die verschlüsselte Datei automatisch entschlüsseln lassen: **Menü** Analyse, Ciphertext only, Rijndael. Nach einigen Minuten findet die automatische Analyse den richtigen Klartext [siehe Abb. 2]. Dies klappt auch, wenn man den Klartext vor der AES-Verschlüsselung mit dem Vigenere-Verfahren verschlüsselt hat. Man kann hier also deutlich vermitteln, dass ein Schlüsselraum von einer Million Schlüsseln (2^{20}) selbst für einen Einzel-PC viel zu kurz ist. Andererseits ist CrypTool bewusst **kein Hackertool**: der durchsuchbare Schlüsselraum ist auf 20 Bit (5 Jokerzeichen bei der Analyse) beschränkt und die Implementierung bietet keinerlei Möglichkeit, die Analyse auf mehrere Rechner zu verteilen.

3.3 Visualisierung Digitale Signatur

Digitale Signaturen sind ein aktuelles politisches Thema. „Normale“ Bürger, denen man damit Wege zu Behörden oder Banken ersparen könnte oder Firmen, die über eine zukunftssichere Investition nachdenken, werden dabei aber immer wieder verunsichert, weil Experten über Details streiten (Signaturen mit unterschiedlichen rechtlichen Auswirkungen, nationales oder europäisches Recht) und wenig Pragmatismus und Kompromissbereitschaft zeigen, obwohl digitale Signaturen sowohl volkswirtschaftlich als auch sicherheitstechnisch sehr sinnvoll wären.

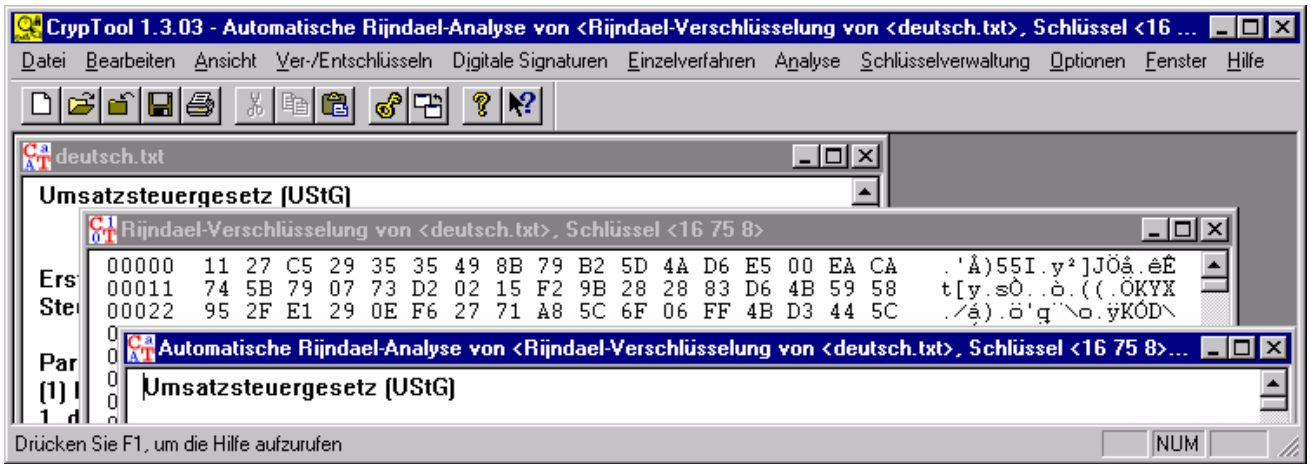

Abb. 2: Korrektes Ergebnis der automatischen Analyse

Mit CrypTool können Sie sehen, was man braucht, um eine digitale Signatur zu erzeugen, wie die Verfahren voneinander abhängen und welche Inhalte und konkreten Zahlen in „echten“ Signaturen, Zertifikaten, Hashwerten und PSEs (Personal Security Environment) enthalten sind. Mit „echt“ ist hier gemeint, dass die Formate und Größenordnungen genau denen von sicheren realen Prozessen mit und ohne Smartcard entsprechen.

Über die **Menü**-Einträge Einzelverfahren, RSA-Demo, Signaturerzeugung können Sie die Visualisierung der Signaturerzeugung aufrufen [siehe Abb. 3].

Dieser Dialog zeigt die Abläufe der Digitalen Signatur in Form eines Datenflussdiagramms. Die einzelnen Operationen (z. B.: Hashwert berechnen) können durch Anklicken ausgeführt werden, sofern die nötigen Eingabedaten vorliegen (erst dann werden die Symbole farblich hervorgehoben). Durch Anklicken der Datenelemente werden die Zwischenergebnisse im unteren Anzeigefeld sichtbar gemacht.

So sieht man z. B., dass die Software in der Lage sein muss, einen Hashwert eines Dokumentes zu berechnen, den geheimen Schlüssel aus der PSE zu lesen und verschiedene standardisierte Formate zu erzeugen. Außerdem sieht man, dass man dazu einen „elektronischen Ausweis“ (Zertifikat) braucht. Ohne vorab eine interoperable PKI für Zertifikate zu errichten, kann sich die Digitale Signatur nicht durchsetzen.

4 Wie geht es weiter?

Für CrypTool gibt es eine umfangreiche Liste an wünschenswerten Weiterentwicklungen (siehe in der Readme-Datei des Paketes, Kapitel 6). Dazu gehört z. B. eine Portierung auf Linux; heute läuft das Programm unter Linux nur in der WINE-Emulation.

Schon bisher wurde CrypTool gemeinsam von vielen Personen weiterentwickelt und die Resonanz aus vielen Ländern zeigt, dass dieses Paket gut ankommt. Die aktuelle Version 1.3.03 ist die letzte, die von der Deutschen Bank als Maintainer herausgebracht wurde. Ab September 2002 ist der Lehrstuhl „Sicherheit in der Informationstechnik“, Fachbereich Informatik unter Frau Prof. Dr. Claudia Eckert an der TU Darmstadt der neue Maintainer. Dort wird CrypTool dann nicht nur als Freeware, sondern sogar als Open-Source-Projekt der Internet-Gemeinde zur Verfügung gestellt und weiterentwickelt. Sie, liebe Leser, sind herzlich eingeladen, dabei mitzuwirken – durch Feedback, Wünsche, Kritik, Anregungen oder aktive Entwicklungsarbeit.

Fazit

Das CrypTool-Projekt lieferte in vierjähriger Arbeit ein Paket, das dem Benutzer einen spielerischen Einstieg in Kryptographie und Kryptoanalyse bietet. Neben der umfangreichen Hilfe bietet das Windows-Programm unter einer einheitlichen Oberfläche alle Möglichkeiten, durch Erfahrung Verständnis zu gewinnen. CrypTool wird sowohl zur Sensibilisierung von Mitarbeitern für IT-Sicherheit als auch in Ausbildung und Lehre eingesetzt und wurde inzwischen über eine Million Mal auf CD verteilt (z. B. auf der Bürger-CD des BSI oder auf einer Heft-CD der PC-Welt).

Die jeweils aktuellen Versionen finden Sie auf der CrypTool-Homepage zum Download:

- www.cryptool.de (deutsch)
- www.cryptool.org (englisch)

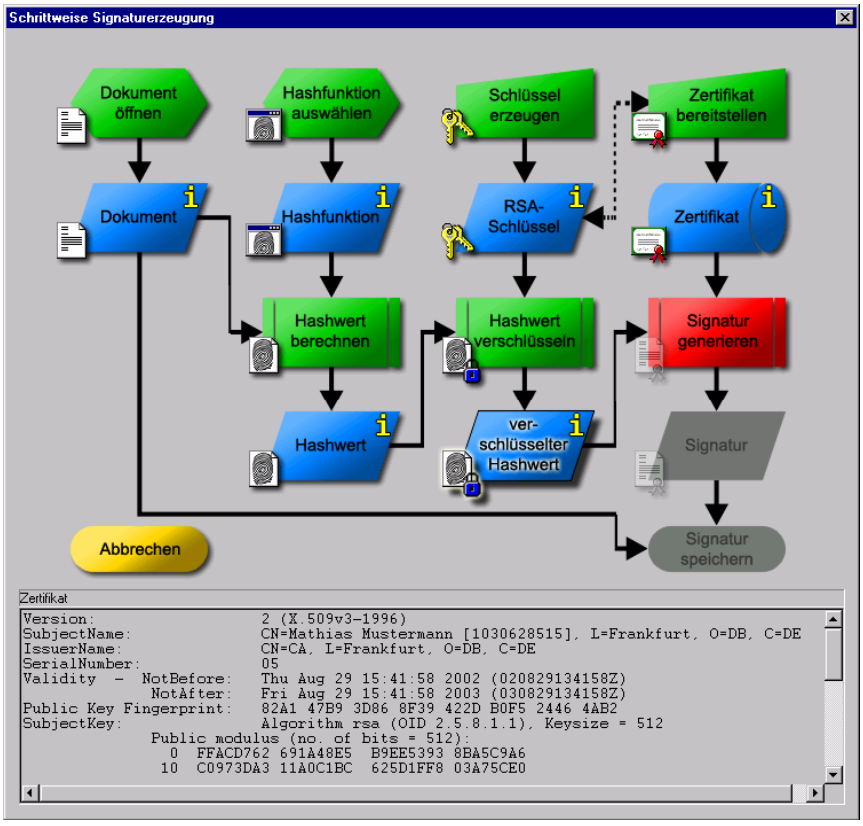

Abb. 3: Visualisierung der Erzeugung einer digitalen Signatur

Literatur

[Koy, Schneider] In dem Computermagazin c’t, Ausgabe 14/2001 wurde im Juli 2001 unter der Überschrift „Selbst geknackt“ ein fünfseitiger Artikel zu CrypTool von Henrik Koy und Jörg-Cornelius Schneider veröffentlicht.

[Miracl] Hersteller, dessen Langzahlarithmetik-Bibliothek kostenlos in CrypTool eingebunden werden durfte, http://indigo.ie/~mscott/

[Secude] Hersteller, dessen Industrie-bewährte Kryptobibliothek kostenlos in CrypTool eingebunden werden durfte, www.secude.com.

Weitere Literatur findet sich z. B. in der Online-Hilfe zu CrypTool.