

Einführung in die Kryptologie mit CryptTool

Einführung / Motivation

**Workshop
INFOS 2009**



www.cryptool.com
www.cryptool.de
www.cryptool.org
www.cryptool.pl

Bedeutung der Kryptographie

Typischer Einsatz von Kryptographie im Alltag

Einsatzbeispiele für Kryptographie

- Telefonkarten, Handys, Fernbedienungen
- Geldautomaten, Geldverkehr zwischen Banken
- Electronic cash, Online-Banking, Sichere E-Mail
- Satellitenfernsehen, PayTV
- Wegfahrsperrung im Auto
- Digital Rights Management (DRM)



- Kryptographie ist schon lange nicht mehr nur auf Agenten, Diplomaten und Militärs begrenzt. Kryptographie ist eine moderne, mathematisch geprägte Wissenschaft.
- Der Durchbruch für den breiten Einsatz kam mit dem Internet.
- Für Firmen und Staaten ist es wichtig, dass sowohl die Anwendungen sicher sind, als auch, dass ...

... die Nutzer (Kunden, Mitarbeiter) ein Mindestverständnis und Bewusstsein (Awareness) für IT-Sicherheit besitzen !

Das CrypTool-Projekt

Ursprung im Awareness-Programm einer Großbank (betriebliche Ausbildung)

→ **Sensibilisierung der Mitarbeiter**

Entwickelt in Kooperation mit Hochschulen (Verbesserung der Lehre)

→ **Mediendidaktischer Anspruch**

1998 – **Projektstart** – Aufwand bisher mehr als 30 Mannjahre

2000 – CrypTool als **Freeware** verfügbar für Windows

2002 – CrypTool auf der **Bürger-CD des BSI** „Ins Internet – mit Sicherheit“

2003 – CrypTool wird **Open-Source** – Hosting durch die Uni Darmstadt (Fr. Prof. Eckert)

2007 – CrypTool in deutsch, englisch, polnisch und spanisch

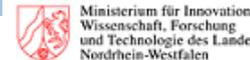
2008 – .NET-Version und Java-Version – Hosting durch die Uni Duisburg (Hr. Prof. Weis)

Auszeichnungen

2004 TeleTrusT (TTT Förderpreis)



2004 NRW (IT-Sicherheitspreis NRW)



2004 RSA Europe (Finalist beim European Information Security Award)



2008 "Ausgewählter Ort" bei der Standortinitiative "Deutschland – Land der Ideen"



Entwickler

– Entwickelt von Mitarbeitern verschiedener Firmen und Universitäten, Schülern + Studenten

→ Weitere Projekt-Mitarbeiter oder verwertbare vorhandene Sourcen sind immer herzlich willkommen (z.Zt. arbeiten ca. 45 Leute weltweit mit).

Einführung in die Kryptologie mit CryptTool

Von klassischen zu modernen Verfahren

**Workshop
INFOS 2009**



www.cryptool.com
www.cryptool.de
www.cryptool.org
www.cryptool.pl

Paradigmenwechsel (1)

Klassische Verfahren

- **Operieren auf Buchstaben, Buchstabengruppen oder auf Worten**
- **Verschlüsselungsprinzipien:**
 - Transposition,
 - Substitution, und
 - Kombinationen daraus.
- **Geheimhaltung der Verfahren**
- **Verwendung fast nur im Bereich der Diplomaten, Militärs und Agenten**

Paradigmenwechsel (2)

Moderne Verfahren

- **Prinzip von Kerckhoffs**
- **Forschungen zu Statistik, Komplexität, Falltürfunktionen**
- **Im Kriegsfall war die Menge an verschlüsselten Informationen VIEL größer als in Zeiten nicht-mechanischer / nicht-elektronischer Kommunikation**
- **Verteilung der Information, Wirtschaftsspionage, Echelon**
- **Nutzerkreis im Internet viel größer → Jedermann**
- **Schutzziele:**
 - **Vertraulichkeit/Geheimhaltung**
 - Es ist zu verhindern, dass Unbefugte den Inhalt einer Nachricht erfahren (mitlesen)
 - **Authentizität**
 - Die Identität des Absenders einer Nachricht muss für den Empfänger nachprüfbar sein (Fälschungssicherheit).
 - **Integrität**
 - Für den Empfänger muss es nachprüfbar sein, dass die erhaltene Nachricht bei der Übermittlung nicht manipuliert wurde (Übertragungssicherheit).

Nutzen der Kryptologie

Gefahren und Gegenmaßnahmen bei der Nutzung von Computern

➤ Gegenmaßnahmen erfordern Wissen:

- Kenntnis der Möglichkeiten der Angreifer
 - Empfinden Sie, dass Ihre Privatsphäre bedroht ist? Sensibilisierung der Schüler.
- Kenntnis der eigenen Gegenmaßnahmen

➤ Maßnahmen sind z.B. Updates, Firewalls, Virenschutz, Kryptographie (siehe: <http://www.bsi-fuer-buerger.de>)

➤ Um die oben genannten Schutzziele mit Mitteln der Kryptographie zu erreichen, gibt es viele moderne Konzepte, Algorithmen und Protokolle.

- Z.B. Erstellen einer eigenen kryptographischen Identität,
 - mit der man beweisen kann, wer man ist,
 - mit der man verschlüsseln und entschlüsseln kann,
 - mit der man signieren und validieren kann.
- Erfordert Infrastruktur, Vertrauensanker, Zusammenarbeit.

Weitere Infos

- esslinger@fb5.uni-siegen.de
- www.cryptool.de // www.cryptoportal.de
- **CrypTool-Präsentation**
 - <http://www.cryptool.com/download/CrypToolPresentation-de.pdf>
- **Kryptofibel „Kryptologie für Jedermann“
Pocketseminar im Zuge der Initiative „Deutschland – Sicher im Netz“**
 - <https://www.sicher-im-netz.de/content/sicherheit/hilfreiches/downloads/Kryptologie-fuer-Jedermann.pdf>
 - <https://www.sicher-im-netz.de/Default.aspx?sicherheit/hilfreiches/downloads/poketseminare>
- <http://www.hydrargyrum.de/kryptographie/>
 - Unterrichtsprojekt "Zahlentheorie in der Schule": Von Primzahlen zur Verschlüsselung mit RSA von Carsten Münchenbach
- <http://bscw.schule.de/pub/bscw.cgi/159132>
 - Helmut Witten, Ralph-Hardo Schulz: RSA & Co. in der Schule (Moderne Kryptologie, alte Mathematik, raffinierte Protokolle), in LOG IN
- ...