

## PROGRAMM

### **Workshop Einführung in die Kryptologie mit CrypTool**

=====

**INFOS 2009, 22.9.09 von 13:00 - 16:00 h**

Zielgruppe: Sekundarstufe I und II

1. Kurzüberblick, ca. 15 Min. (Esslinger)

- Was ist Kryptologie?
- Was kann man mit CrypTool machen?

2. Monoalphabetische Verschlüsselung, ca. 45 Min.

[Goldkäfer, Caesar: Entschlüsselung durch Zeichenhäufigkeit bzw. durch vollständiges Austesten des Schlüsselraums],  
dabei Einsatz von CrypTool (Esslinger) und von kleinen  
Python-Programmen (Witten) mit praktischen Übungen  
per Hand und am Rechner.

3. Demonstrationen zu Vigenère und zu Vernam, ca. 30 Min.

- mit CrypTool (Esslinger),
- Hinweise zur unterrichtlichen Umsetzung,
- Nutzung von Arbeitsblättern zur Parallelstellensuche (Witten),
- Hinweis auf die ersten drei Folgen der RSA & Co. Serie aus LOG IN.

Anschließend kurze Pause mit der Möglichkeit, Fragen zu stellen und  
weiter selbstständig mit CrypTool zu experimentieren (15 Min).

4. Einführung asymmetrische Verschlüsselung (Witten).

Hierzu gibt es ein älteres Selbstlernprogramm der FhG als Flash-Animation.  
Neben der darin beschriebenen hierarchischen Schlüssel-Infrastruktur gibt  
es noch das von PGP her bekannte Web-of-Trust zur Schlüsselverteilung.  
Dauer: ca. 15 Min.

5. Grundprinzip der RSA-Verschlüsselung, RSA-Demo von CrypTool,  
Sicherheit von RSA, Anwendungen von RSA (Witten).

Dabei sollten die TeilnehmerInnen wieder konkrete Aufgaben mit  
CrypTool bearbeiten (Esslinger).

- Hinweis auf die bislang 3 Artikel zur "Neuen Folge" von RSA & Co.
  - Fragen, Infos zu CrypTool 2 und Java-CrypTool und zum  
Projektmanagement größerer Open-Source-Projekte.
  - Einsatz von Kryptographie in Firmen und Behörden.
  - Einsatz unter Windows: CT1 und CT2;  
unter Windows, Linux und Mac: JCT.
  - Python und Sage (im Browser) stehen auf allen Betriebssystem-Plattformen zur Verfügung.
- Dauer: ca. 60 Min.