



ICH BIN BOB, AGENT BOB.
HILF MIR MEIN GEHEIMNIS
ZU WAHREN!

SCHÜLERKRYPTO

BY CRYPTOOL



SCHÜLERKRYPTO 2014

KASSEL

29.04.2014, 8:30-16:30
Wilhelmshöher Allee 71-73

U N I K A S S E L
V E R S I T Ä T



"Mqoogp Ukg bwt Uejwngtmtarvq!"
würde Caesar schreiben, wenn er nicht
wollte, dass Pompeius es versteht. Was
Caesar allerdings nicht ahnt, ist, dass
Pompeius die Nachricht mit einfachen Tricks
trotzdem lesen kann...

BESCHREIBUNG

In der eintägigen Veranstaltung der Schülerkrypto 2014 werden die Hintergründe dieser „Tricks“ beleuchtet und die darunterliegenden Prinzipien einfach erklärt. Nachdem die Schülerkrypto bereits in den letzten Jahren erfolgreich in verschiedenen Städten durchgeführt wurde, kommt sie nun auch nach Kassel. Die Veranstaltung richtet sich an naturwissenschaftlich interessierte Schülerinnen und Schüler der Oberstufe und soll das allgemeine Interesse an den MINT-Fächern und an einem späteren Studium wecken. Die Idee hinter dem Konzept der Schülerkrypto ist es, Kryptologie, d.h. die Wissenschaft der geheimen Botschaften, spielerisch und spannend zu erlernen. Die Teilnehmer erleben im Rahmen der Schülerkrypto angewandte Mathematik ohne komplizierte Formeln und zum Mitmachen. Dabei dürfen sie das Gelernte auch direkt an den PCs der Universität ausprobieren. Die schnellsten Lösungen werden mit kleinen Sachpreisen prämiert.

Der Dozent der Schülerkrypto 2014 in Kassel, Professor Wacker, ist der Entwicklungsleiter der eingesetzten Lernsoftware Cryptool 2.0. Sein Lehrauftrag beinhaltet unter anderem Vorlesungen an der Universität Kassel im Bereich der Angewandten Informationssicherheit.

PROGRAMM

08:30 - 10:15 Uhr Einführung in die Kryptologie I

- Einleitung
- Einfache Verschlüsselung
- Verbesserte Verschlüsselung



10:15 - 10:30 Uhr Frühstückspause

10:30 - 11:30 Uhr Agenteneinsatz I

- Grundausbildung zum Geheimagent
- Aufträge 1 und 2

11:45 - 13:00 Uhr Einführung in die Kryptologie II

- Maschinelle Verschlüsselung
- Moderne Verschlüsselung (Teil 1)

13:00 - 13:30 Uhr Mittagessen

13:30 - 14:30 Uhr Einführung in die Kryptologie III

- Moderne Verschlüsselung (Teil 2)

14:45 - 16:15 Uhr Agenteneinsatz II

- Agentenfortbildung
- Aufträge 3 und 4



16:15 - 16:30 Uhr Abschluss

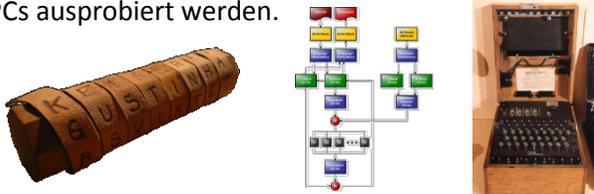
INHALTE

Im Rahmen der Schülerkrypto wird anhand von vielen praktischen Beispielen erklärt, wie man solche "Buchstabenhaufen", wie oben angegeben, erzeugt (Verschlüsselung) und sie auch wieder lesbar macht (Entschlüsselung und Kryptoanalyse).

Dabei werden folgende Themen an Beispielen erklärt und praktisch vorgeführt:

- Grundlagen der Kryptographie (Verschicken von geheimen Botschaften) und Kryptoanalyse (Lesen der Botschaft ohne Kenntnis des Geheimnisses)
- Geschichtliche Hintergründe der Verschlüsselung (z.B. "Hut 6" aus Bletchley Park, Room 40 und die schwarzen Kammern)
- Skytale, Caesar, Freimaurer, Enigma, DES, AES und RSA sind nur einige der vorgestellten Verschlüsselungsalgorithmen
- Zahlengruppen und Falltürfunktionen spielerisch erlernen und verstehen
- Verschicken von geheimen Botschaften, obwohl man weiß, dass die Botschaften auf dem Weg gelesen werden
- Alle Beispiele werden mit Hilfe des freien Lernprogramms CrypTool durchgeführt

Alle vorgestellten Verfahren können von den Teilnehmern selbst mit Stift und Papier oder mittels PCs ausprobiert werden.



ORGANISATORISCHES

Datum: 29.04.2014
Uhrzeit: 8:30 – 16:30 Uhr
Adresse:

Universität Kassel
Fachbereich 16 Elektrotechnik/Informatik
Wilhelmshöher Allee 71-73
34121 Kassel
Raum 0315 (Eingang C)

Die Teilnehmer erhalten ein kostenloses Mittagessen in der Universitätsmensa.

Materialien und weitere Informationen zu dieser und zu früheren Schülerkrypto Veranstaltungen finden Sie auf der Schülerkrypto Webseite:

<http://www.cryptool.org/schuelerkrypto>

ANMELDUNG

Die Teilnahme an der Schülerkrypto 2014 in Kassel ist kostenlos. Es wird allerdings eine verbindliche Anmeldung benötigt, da die maximale Teilnehmerzahl begrenzt ist.

Für eine Anmeldung zu der Schülerkrypto 2014 kontaktieren Sie das Schülerforschungszentrum (SFN) in Kassel bis zum 20.04.2014 unter:

E-Mail: kphaupt@sfn-kassel.de
Tel: +49 (561) 311116 oder
+49 (561) 76644971

Auch eine persönliche Anmeldung im SFN ist möglich.

VERANSTALTER

Die Schülerkrypto 2014 in Kassel ist ein Kooperationsprojekt zwischen dem Fachbereich 16 Elektrotechnik/Informatik der Universität Kassel und dem Schülerforschungszentrum Nordhessen der Universität Kassel in Kooperation mit Science-for-People und der Robert-Bosch-Stiftung.

KONTAKTDATEN

Prof. Dr. Arno Wacker (Dozent)

Universität Kassel
Fachbereich 16 Elektrotechnik/Informatik
Fachgebiet Angewandte Informationssicherheit
Pfnankuchstr. 1
34121 Kassel

Tel: +49 (561) 804 6644
Fax: +49 (561) 804 6643
E-Mail: arno.wacker@uni-kassel.de
Web: <http://www.ais.uni-kassel.de>

Klaus-Peter Haupt (Studiendirektor)

Studienseminar für Gymnasien Kassel
Leiter des Schülerforschungszentrums
Nordhessen der Universität Kassel

Parkstr.16
34131 Kassel

Tel: +49 (561) 76644971
E-Mail: kphaupt@sfn-kassel.de
Web: <http://www.sfn-kassel.de>
<http://www.science-for-people.de>