

Evaluation der Lernsoftware CrypTool 2

Fragebogen zu Vorkenntnissen der Probanden

Im Rahmen meiner schriftlichen Hausarbeit für das Erste Staatsexamen im Fach Mathematik möchte ich die Lernsoftware CrypTool 2 evaluieren. Das Lernprogramm für Verschlüsselungsverfahren wurde ursprünglich zu internen Schulungszwecken von einer deutschen Großbank entwickelt, später als freie Software veröffentlicht und auch im Rahmen von Kryptographie-Vorlesungen an Universitäten (oder Schulen) verwendet. Die Version 2 des Programms befindet sich gerade in der Entwicklung und richtet sich auch an Interessierte, die keinen begleitenden Kurs besuchen.

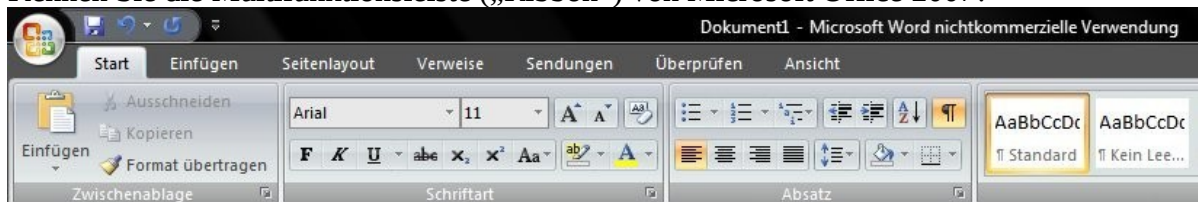
Von großem Nutzen sind mir natürlich Erfahrungen, die Nutzer mit der Anwendung des Programmes gemacht haben. Ihre Bereitschaft, CrypTool 2 zu testen, würde mich in meiner Arbeit sehr unterstützen.

Zunächst möchte ich Sie um einige Angaben bezüglich Ihrer Vorkenntnisse bitten.

A1 Wie würden Sie Ihre eigenen Vorkenntnisse im Fach Mathematik beschreiben?
(Schul- oder Studienabschluss in Mathematik, Anwendung mathematischer Kenntnisse im Beruf/ im Alltag, Interesse, Einschätzung der eigenen Fähigkeiten)

A2 Wie oft und zu welchen Zwecken nutzen Sie Computer (beruflich wie auch privat)?
(Beginnen Sie bitte mit der Tätigkeit, die Sie am häufigsten am PC ausüben.)

A3 Kennen Sie die Multifunktionsleiste („Ribbon“) von Microsoft Office 2007?



Kommen Sie gut damit zurecht? Wenn nicht, können Sie dies begründen?

A4 Nutzen Sie Erklärungen aus Wikipedia, um Sachverhalte zu verstehen?
Wie sind Ihre Erfahrungen damit?

A5 Haben Sie Erfahrungen in der Nutzung von Lernsoftware? Arbeiten Sie gerne mit Lernprogrammen? Wenn nicht, was empfinden Sie als störend?

A6 Unter Kryptographie versteht man die Verschlüsselung von Daten.
Wissen Sie, wo wir im alltäglichen Leben mit Verfahren der Kryptographie in Berührung kommen?

A7 Kennen Sie Verfahren der Datenverschlüsselung? Welche?

A8 Finden Sie das Gebiet der Kryptographie interessant?
Wenn ja, worüber würden Sie gerne im Einzelnen mehr erfahren bzw. wissen?

Um CrypTool 2 installieren zu können, benötigen Sie Windows XP, Vista oder neuer sowie das Microsoft .NET Framework 3.5 mit Service Pack 1.

Das Programm CrypTool 2 (sowie das .NET Framework und Service Pack 1, falls noch nicht vorhanden) kann kostenlos aus dem Internet heruntergeladen werden unter:

<http://cryptool2.vs.uni-due.de/index.php?page=14&lm=1&ql=4>

Falls Sie nur über eine langsame Internetverbindung verfügen, lasse ich Ihnen auch gerne eine CD mit allen nötigen Dateien zukommen, E-mail an chmeyer@uni-koblenz.de oder Anruf genügt.





CrypTool 2 verfügt über eine neuartige Oberfläche mit einer ebenfalls neuartigen Bedienung, genannt „visuelle Programmierung“. Eine kurze (englischsprachige) Einführung finden Sie unter der Karteikarte „Help“.



Für diese Evaluation habe ich ein paar „Arbeitsblätter“ vorbereitet, die wahlweise per Doppelklick auf die Datei oder aber mit dem Befehl „Open“ in der Multifunktionsleiste (im oberen Teil des Fensters, unter Menü-Tab "Home") geöffnet werden können. Die gespeicherten Arbeitsblätter laden Sie bitte herunter unter:






<http://userpages.uni-koblenz.de/~chmeyer/aufgaben.zip>

Aufgaben zur Bearbeitung mit CrypTool 2

1. Zuerst sollen Sie ein wenig mit dem Programm vertraut werden.
 - Öffnen Sie die Datei 1_Caesar.cte.
 - Drücken Sie die Taste F11, dadurch wird der Anzeigebereich vergrößert.
 - Drücken Sie oben links in der Titelleiste den Start-Knopf. 
 - Im linken Kasten steht der Klartext, im unteren erscheint nun der verschlüsselte Geheimtext.
 - Schieben Sie bei den Feldern, die die Buchstabenhäufigkeit anzeigen, die Schieberegler so, dass Sie die Auswertung komplett sehen. 
 - Vergleichen Sie beide Auswertungsdiagramme. Sie bemerken, dass die Verteilung der Buchstaben ungleichmäßig bleibt, alle Buchstaben sind nur im Alphabet verschoben.
 - Ändern Sie nun den Kennbuchstaben der Verschlüsselung.
 - Drücken Sie dazu zunächst oben links in der Titelleiste den Stop-Knopf. 
 - Klicken Sie auf Caesar-Symbol in der Mitte des Anzeigenbereichs (es wird orange hinterlegt) und öffnen sie am rechten Seitenrand das Menü „Algorithm Settings“.
 - Geben Sie im Feld „Key as single letter“ einen beliebigen Buchstaben ein.
 - Das Menü verschwindet wieder, wenn man erneut auf „Algorithm Settings“ klickt.
 - Um den Text zu verschlüsseln, drücken Sie erneut den Start-Knopf. 

Entschlüsseln Sie einen mit Caesar verschlüsselten Geheimtext.

- Öffnen Sie die Textdatei Caesar_geheim.txt durch Doppelklick mit einem Texteditor.
- Kopieren sie den Geheimtext in das linke Textfeld („Text Input“).
- Klicken Sie auf das Caesar-Symbol in der Mitte des Anzeigenbereichs und öffnen Sie wieder die Einstellungen mit „Algorithm Settings“. Hier wählen Sie bei „Action“ die Funktion „Decrypt“ - „Entschlüsseln“.
- Versuchen Sie, den Geheimtext zu entschlüsseln. Nutzen Sie die Buchstabenhäufigkeit.

2. Das zweite Verfahren ist die Vigenere-Verschlüsselung.
 - Bei Vigenere wird der Klartext nicht mit einem einzelnen Buchstaben verschlüsselt, sondern mit einem Kennwort. So wird beispielsweise aus „eeee“ mit dem Kennwort „abcd“ der Geheimtext „efgh“.
 - Öffnen Sie die Datei 2_Vigenere.cte (und klicken auf Start: ).
 - Vergleichen Sie die Verteilung der Buchstabenhäufigkeit von Klartext und Geheimtext.
 - Probieren Sie nun verschiedene Kennwörter aus. (Unterbrechen Sie dazu den Ablauf mit Stop , klicken auf das Vigenere-Symbol, rufen rechts die „Algorithm Settings“ auf und ändern Sie den Eintrag im Feld „Shift key (multiple letters)“. Jetzt drücken Sie bitte wieder auf Start .
 - Warum ist „pssst“ ein schlechteres Kennwort als „strenggeheim“ oder „eiffelturm“? (Hinweis: Buchstabenwiederholungen, Kennwortlänge)
3. Entschlüsseln Sie eine mit Vigenere verschlüsselte Nachricht
 - Öffnen Sie nun die Datei 3_Vigenere.cte (und klicken auf Start: .
 - Hier erscheinen nun zwei Analysewerkzeuge, mit denen man die Kennwortlänge abschätzen kann.
 - Der Friedman-Test berechnet anhand einer mathematischen Formel (gestützt auf die statistische Buchstabenverteilung im Text) eine ungefähre Kennwortlänge. Dieser Test kann aber auch durchaus um einige Buchstaben falsch liegen.
 - Der Kasiski-Test zeigt die Abstände zweier gleicher Buchstabenpaare im Text an. Bitte bewegen Sie den Schieberegler so, dass Sie die komplette Verteilung sehen. Die Kennwortlänge ist vermutlich ein Maximum der Verteilungskurve. (Oder ein Vielfaches oder ein Teiler davon). Auch hier gibt es nur Hinweise auf die Kennwortlänge, es ist etwas „Fingerspitzengefühl“ gefragt.
 - Der gespeicherte Klartext ergibt daher bei beiden Tests eine Kennwortlänge von 1 (nach Kasiski möglicherweise auch 8).
 - Öffnen Sie die Textdatei Vigenere_geheim.txt durch Doppelklick mit einem Texteditor.
 - Kopieren Sie den Geheimtext in das linke Textfeld („Text Input“).
 - Bevor Sie weiterlesen: Versuchen Sie die Länge des Kennworts zu bestimmen, das Kennwort hat etwas mit mir zu tun.
 - Versuchen Sie den Text zu dechiffrieren. (Stop, Vigenere anklicken, „Algorithm settings“, Action: Decrypt, „Shift key (multiple letters)“ erraten).
 - Das Kennwort hat 9 Buchstaben. Der Friedman-Test liegt zwar mit 10,5 daneben, beim Kasiski-Test erkennt man jedoch ein Maximum bei 9 (und eines bei 18). Möglicherweise könnte das Kennwort auch 3 Buchstaben haben, doch dafür ist das „Maximum“ bei 3 zu gering. Haben Sie das Kennwort erraten? Es beginnt mit ch.
4. AES
 - Öffnen Sie nun die Datei 4_AES.cte (und klicken auf Start: .
 - Das Schaubild soll die Funktionsweise von AES sowie die Bedeutung der Pseudo-Zufallszahlen zeigen. Im „wirklichen Leben“ wird der geheime Schlüssel zuvor über eine asymmetrische (und rechenintensivere) Verschlüsselung ausgehandelt.
 - Falls Sie mehr über AES erfahren möchten, kann ich Ihnen empfehlen:
 - die beiden Rijndael-Programme (später: AES) aus dem Programmumfang des „alten“ CrypTool unter: <http://userpages.uni-koblenz.de/~chmeyer/cryptool>
 - http://www.realtec.de/privat/aes_algo.html
 - http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

5. Enigma (schwierigere Zusatzaufgabe)
- Versuchen Sie den Geheimtext aus der Datei Enigma_geheim.txt zu entschlüsseln.
 - Dazu sollen Sie selbst ein solches Arbeitsblatt erstellen. Klicken Sie auf „Home“ (oben links) und dann auf „New“. Die nötigen Bausteine finden Sie links im angedockten Fenster unter „Classic Ciphers“ und „Tools“.
 - Hinweis: Es wird Ihnen helfen, wenn Sie unter den „Algorithm Settings“ des „TextOutput“ Feldes in der unteren Hälfte bei „Type“ den Eintrag „string“ auswählen. Denn ansonsten werden Sie es nicht mit dem Enigma-Ausgang verbinden können.
 - Verwendete Daten: Enigma I / M3; Key: CBM; Rotoren: III, I, II; Reflektor: UKW A
 - Falls Sie mehr über Enigma erfahren möchten kann ich Ihnen empfehlen:
 - das Enigma_de Programm aus dem Programmumfang des „alten“ CrypTool unter: <http://userpages.uni-koblenz.de/~chmeyer/cryptool>
 - [http://de.wikipedia.org/wiki/Enigma_\(Maschine\)](http://de.wikipedia.org/wiki/Enigma_(Maschine))

Abschließende Fragen zur Beurteilung von CrypTool 2

- E1 Wie gut konnten Sie die gestellten Aufgaben bewältigen? Welche Probleme gab es?
- E2 Wie gefällt Ihnen das Programm CrypTool 2 (positive und negative Aspekte)?
- E3 Bewerten Sie bitte die graphische Aufbereitung des Arbeitsplatzes („visuelle Programmierung“).
- E4 Was hat Sie überfordert, war ungewohnt, hinderlich oder irritierend?
- E5 Trauen Sie es sich zu, mit dem Programm selbständig weiter zu arbeiten? (Wenn „Nein“, warum nicht?)
- E6 Haben Sie Verbesserungsvorschläge für das Programm? (Bitte auch Anmerkungen und Kommentare)

Bitte senden Sie mir Ihre Antworten zu den Fragen per E-mail (möglichst bis Ende August 2009). Die Antworten bieten mir wichtige Anhaltspunkte, wie ein neuer Benutzer das Programm sieht und wo es möglicherweise Probleme gab.

Vielen Dank für Ihre Unterstützung und Mühe.

Christian Meyer
chmeyer@uni-koblenz.de

