

Wissenschaftliche Prüfungsarbeit

gemäß § 12 der Landesverordnung über die Erste Staatsprüfung für das Lehramt an
Realschulen vom 31.03.1982 in der derzeit gültigen Fassung.

des Kandidaten Christian Meyer

der Universität Koblenz-Landau in Koblenz

Fach Mathematik

Thema **Evaluation der Software „CrypTool 2“ unter
didaktischen Aspekten**

Erstgutachter Univ.-Prof. Dr. Peter Ullrich

Zweitgutachter Prof. Dr. Rüdiger Grimm

Abgabedatum 06.11.2009

Inhaltsverzeichnis

1. Einleitung.....	5
1.1. Motivation und Zielsetzung der Arbeit.....	7
2. Programmbeschreibung: CrypTool 2.....	9
2.1. Ziele des Programms.....	10
2.2. Leistungsumfang.....	11
2.3. Vergleich von CrypTool 2 mit CrypTool 1.4.30 - Beta 04.....	13
2.3.1. Programmoberfläche.....	13
2.3.2. Bedienung.....	14
2.3.3. Zugaben.....	15
2.4. Bisherige Arbeiten zu CrypTool 2.....	16
2.4.1. Diplomarbeit zum Editor für CrypTool 2.....	16
2.4.2. Diplomarbeit zu Primes – Die Welt der Primzahlen.....	17
3. Didaktische Analyse.....	18
3.1. Lerngruppenanalyse.....	18
3.2. Sachanalyse.....	20
3.3. Didaktisch-methodische Überlegungen.....	24
3.3.1. Gegenwartsbedeutung.....	25
3.3.2. Zukunftsbedeutung.....	25
3.3.3. Sachstruktur.....	26
3.3.4. Exemplarische Bedeutung.....	27
3.3.5. Zugänglichkeit.....	28
3.4. Befragung von Probanden zur Arbeit mit CrypTool 2.....	29
3.5. Lernziele.....	32

4. Betrachtung von CrypTool 2.....	34
4.1. Installation und Programmstart.....	34
4.1.1. Installationsvoraussetzungen.....	34
4.1.2. Programmstart.....	35
4.2. Graphische Oberfläche von CrypTool 2.....	36
4.2.1. Die Multifunktionsleiste Ribbon.....	37
4.2.2. Das Navigationsfenster Algorithms.....	42
4.2.3. Das Fenster Algorithm Settings.....	43
4.2.4. Das Logbuch (Messages).....	44
4.2.5. Der Workspace zur visuellen Programmierung.....	46
4.2.6. Die Darstellung der Algorithmen.....	50
4.3. Das Programm Die Welt der Primzahlen.....	58
5. Fazit und Erweiterungsvorschläge.....	64
5.1. Startcenter.....	65
5.2. Guided Tour.....	67
5.3. Lernebenen.....	68
5.4. Sub-Workspaces.....	72
5.5. Beispiel: RSA.....	73
5.6. Schlusswort.....	77
6. Abbildungs- und Literaturverzeichnis.....	79
7. Anhang.....	85
7.1. Danksagung.....	85
7.2. Befragung von Probanden (Fragebogen).....	86
7.3. Aufgaben zur Bearbeitung durch die Probanden (Bildschirmfotos).....	90
7.4. Antworten der Probanden.....	97

7.5. Graphiken zur „Krypto-Entwicklung“ von H. Witten.....	125
7.6. Entwurf zu Startcenter und visueller Programmierung.....	126
7.7. Teilnahmebestätigung HRPI-Fortbildung.....	129
7.8. Versicherung.....	130

1. Einleitung

Kryptologie, die Lehre der Verschlüsselung, ist eine sehr alte Kunst, die schon in der Antike - bei Ägyptern, Griechen und Römern - angewendet wurde. Geschichtlich betrachtet war sie bis vor wenigen Jahrzehnten eine Domäne von Mächtigen, Verschwörern und Geheimdiensten. Das Gebiet der Kryptologie umfasst die drei Aspekte Kryptographie, Kryptoanalyse und Steganographie. Zur Kryptographie gehört das Schreiben und Lesen von verschlüsselten Nachrichten, Kryptoanalyse befasst sich mit dem Entziffern unbekannter Geheimtexte und Steganographie ist die Kunst der Verschleierung einer Kommunikation¹. Der Begriff Kryptographie wird allerdings auch häufig ungenau als Synonym für Kryptologie verwendet.

Die moderne, mathematische Kryptographie begann 1949 mit Claude Shannon (vgl. [WP:Kr_graphie]). Doch erst durch die Erfindung und Verbreitung des Computers und die damit verbundene schnellere, offenere und vielseitigere Kommunikation bzw. Datenverarbeitung entwickelte sich zunehmend ein Bedürfnis, persönliche Daten in großem Umfang zu schützen. Dabei sind allem drei Hauptziele² zu nennen, die durch kryptographische Verfahren erreicht werden sollen (vgl. [Esslinger 1], S.7 und [WP:Kr_graphie]):

- **Vertraulichkeit:** Es soll kein Unbefugter in der Lage sein, die Daten zu lesen oder auszuwerten.
- **Integrität:** Die Daten sollen vor Manipulation sicher sein. Zumindest aber soll feststellbar sein, ob die Daten vollständig sind und ob Veränderungen stattgefunden haben.
- **Authentizität:** Der Urheber der Nachricht soll fälschungssicher erkennbar sein. Dadurch ergibt sich eine Vertrauenswürdigkeit in die Nachricht bzw. in die Daten, zum anderen kann eine Verbindlichkeit aus dem Inhalt der Nachricht hergestellt werden (z.B. bei Geschäftsabschlüssen).

¹ Hier werden Nachrichten versteckt übermittelt, beispielsweise durch modifizierte und unauffällig in einem Bild platzierte Morsezeichen.

² Anders als in beiden Quellen angegeben, behandle ich „Verbindlichkeit / Nichtabstreitbarkeit“ nicht als viertes Hauptziel, da dies aus den Punkten Authentizität und Integrität folgt. Außerdem lässt sich so den Hauptzielen jeweils ein Algorithmotyp zuordnen (vgl. 3.2 Sachanalyse).

Auch wenn es den wenigsten Menschen bewusst sein dürfte, sind wir im Alltag von einer Vielzahl kryptographischer Anwendungen umgeben, ja mehr noch: Wir verlassen uns ganz selbstverständlich darauf, dass unsere Daten „sicher“ sind.

Die Anwendungen der modernen, mathematischen Kryptographie reichen von elektronischen Zugangssystemen, Pay-TV und gesicherten Internetverbindungen über Funkverbindungen (Netzwerk: WLAN oder Mobilfunk: GSM) bis hin zu bargeldlosen Zahlungen, elektronischen Ausweisdokumenten oder der neuen elektronischen Krankenakte. Kryptographische Verfahren bieten Schutz vor dem Verlust vertraulicher Informationen. In den letzten Jahren sind einige Vorfälle bekannt geworden, deren möglichen negativen Auswirkungen durch die sachgerechte Verwendung kryptographischer Verfahren hätten verhindert werden können:

- 1994 wurde die deutsche Enercon GmbH, ein Hersteller von Windkraftanlagen, vermutlich Opfer von Industriespionage. Es wird angenommen, dass der US-amerikanische Geheimdienst NSA mit Hilfe des Spionagesystems Echelon wichtige interne Daten abgefangen und an die US-amerikanische Konkurrenz weitergeleitet hat (vgl. [Schröm]).
- In den Jahren 2007 und 2008 gab es in Großbritannien eine Serie von Verlust und Diebstahl persönlicher Daten. So gingen laut Tagesschau vertrauliche Kontodaten von mehr als einer Million Briten, ein Speicherstick mit den Daten aller 84.000 Häftlinge und den Informationen zu 33.000 Wiederholungstätern, Daten von über 600.000 Rekruten sowie die Daten von allen 25 Millionen Kindergeldempfängern verloren (vgl. [Tagesschau]).

Auf der anderen Seite gibt es noch immer (und auch in westlichen Staaten) Bestrebungen und gesetzliche Regelungen, die die Verwendung „*starker Kryptographie*“³ einschränken oder verbieten wollen. Hintergrund dafür ist, dass Geheimdienste und Regierungen um ihre nationale Sicherheit besorgt sind und befürchten, dass dadurch gerade dem organisierten Verbrechen oder dem internationalen Terrorismus in die Hände gespielt wird (vgl. [Schmeh], S. 206).

³ Für den Begriff „starke Kryptographie“ konnte ich keine exakte Definition finden. Es sind jedoch die modernen, öffentlich bekannten Verfahren gemeint, bei denen eine verschlüsselte Nachricht ohne Kenntnis des Schlüssels nicht in „akzeptabler Zeit“ (also in weniger als einigen Jahren) dechiffriert werden kann.

Beispiele hierfür sind:

- Der Erfinder des freien Verschlüsselungsprogramms PGP, Phil Zimmermann, geriet beispielsweise wegen des Exports von PGP mit dem amerikanischen Gesetz in Konflikt und musste damit rechnen, wie ein Waffenschmuggler verurteilt zu werden. Das Verfahren wurde 1996 eingestellt, offiziell mangels Beweisen. Die Exportbeschränkungen für Kryptographie wurden Ende der 90er Jahre zumindest gelockert (vgl. [Schmeh], S. 299f. und [WP:PGP]).
- In Großbritannien wurde 2007 ein Gesetz verabschiedet, das die Herausgabe von Passwörtern und Kryptographie-Schlüsseln erzwingen soll. 2008 kam es daraufhin zur Verhängung von ersten Haftstrafen (vgl. [Bachfeld] und [Wilkens]).

Das Computerprogramm CrypTool⁴ ist ein weitverbreitetes und preisgekröntes⁵ Lernprogramm zur Kryptographie mit „mediendidaktische[m] Anspruch“ (vgl. [Esslinger 1], S. 8). Es soll „ohne tieferes Kryptographiewissen verständlich“ sein und einen „spielerische[n]‘ Einstieg in moderne und klassische Kryptographie“ bieten. Zielgruppe sind „Studierende der Informatik, Wirtschaftsinformatik, Mathematik“ ebenso wie „Computernutzer und Anwendungsentwickler, Mitarbeiter, Schüler“, die über PC-Kenntnisse verfügen und „Interesse an Mathematik und Programmierung“ haben ([Esslinger 1], S. 24).

Seit Ende 2007 wird an einem Nachfolger für CrypTool gearbeitet. CrypTool 2⁶ befindet sich gegenwärtig in der Entwicklungsphase, seit 2008 sind einige Beta-Versionen erschienen.

1.1. Motivation und Zielsetzung der Arbeit

Das Gebiet der Kryptographie interessierte mich schon als Kind und Jugendlicher. Ich besaß einige (kindgerechte) Bücher, in denen „Geheimschriften“ behandelt

4 Homepage und Download unter: <http://www.cryptool.com> .

5 TeleTrusT Förderpreis (2004), IT-Sicherheitspreis NRW (2004) und Finalist beim European Information Security Award (2004). Außerdem war CrypTool im Jahr 2008 "ausgewählter Ort" bei der Standortinitiative "Deutschland – Land der Ideen"

6 Entwicklerseite und Download unter: <http://cryptool2.vs.uni-due.de> .

wurden und verwendete alt-ägyptische Hieroglyphen, um meine in leeren Filmdosen aufbewahrten „Kostbarkeiten“ zu kennzeichnen. Später tauschte ich mit einem Mitschüler während des Unterrichts Nachrichten aus, die als Schutz vor unerwünschten Mitlesern „verschlüsselt“ waren. Nach meinem Abitur machte ich eine Berufsausbildung und es bot sich in den folgenden 15 Jahren Arbeitsleben leider keine Möglichkeit, einen Kurs über Kryptographie zu besuchen. Da die Faszination für das Thema aber geblieben war, versuchte ich, meine Wissbegierde autodidaktisch über das Internet zu stillen. Dabei hätte mir ein freies E-Learning-Programm wie CrypTool sicher sehr geholfen.

Da sich CrypTool 2 noch in der Entwicklungsphase befindet, sehe ich durch meine Examensarbeit die Möglichkeit gegeben, dem CrypTool-Projekt Rückmeldung zur didaktischen Konzeption und der konkreten Umsetzung im Programm geben zu können. Dabei möchte ich nicht nur das bestehende Konzept betrachten, sondern gleichwohl auch Anregungen geben und Verbesserungsvorschläge ausarbeiten.

Eine besondere Herausforderung für diese Examensarbeit (und natürlich auch für CrypTool 2) stellen dabei die sehr heterogenen Zielgruppen des Programms dar. Wie bereits erwähnt soll CrypTool 2 für Laien wie für Profis, für Autodidakten ebenso wie für Schulungen, Vorlesungen oder Unterrichtsstunden im klassischen Sinne geeignet sein.

Um verwertbare Rückmeldungen aus verschiedenen Zielgruppen zu erhalten, erstellte ich einen Fragebogen mit Aufgaben zur Arbeit mit CrypTool 2, den ich von ausgewählten Probanden bearbeiten ließ. Die Antworten der Probanden fließen an den unterschiedlichsten Stellen dieser Arbeit mit ein⁷.

Im Folgenden möchte ich zunächst CrypTool 2 kurz vorstellen und dann meine didaktischen Überlegungen zur Kryptologie als Lerngegenstand⁸ festhalten. Dann betrachte ich den Aufbau und die einzelnen Elemente der aktuellen Programmversion aus didaktischem Blickwinkel, um schließlich weitergehende Ideen und Vorschläge zur Erweiterung um didaktisch sinnvolle Elemente bzw. Aspekte zu entwickeln.

7 Fragebogen und Antworten habe ich dem Anhang dieser Examensarbeit beigefügt.

8 Mit Blick auf CrypTool 2 und die von Prof. Esslinger in [Esslinger 1] genannten und bereits erwähnten Zielgruppen.

2. Programmbeschreibung: CrypTool 2

CrypTool 2 ist zur Zeit noch in der Entwicklungsphase (Beta-Version). Daher ist CrypTool 2 auch noch nicht als „fertig“ anzusehen, sondern lediglich als „Technology Preview“, die es ermöglichen soll, schon einen Einblick in die nächste Version von CrypTool zu bekommen (vgl. [CT_63]). Daher darf auch noch nicht erwartet werden, dass das Programm „komplett“ ist oder gar fehlerfrei funktioniert.

Das zugrunde liegende technische Design des Programms ist vollkommen modular. Daher ist fast jede Komponente von CrypTool 2 als Plug-in⁹ realisiert und kann unabhängig vom Rest des Programms gepflegt oder ausgetauscht werden. Auch Erweiterungen der Programmoberfläche können so leicht vorgenommen werden, beispielsweise durch im Rahmen von Seminaren oder Diplomarbeiten entstandene Projekte oder Module.

Die zum Zeitpunkt dieser Examensarbeit aktuelle Beta-Version ist CrypTool 2.0.3465a(beta), auf die ich mich daher auch in dieser Arbeit berufe. Eigenschaften, Programmteile oder Plug-ins, die in dieser Version (noch) nicht vorhanden sind, können also auch nicht betrachtet werden.

CrypTool 2 verfügt über eine neu entwickelte, grundlegend vom „alten“ CrypTool verschiedene Benutzeroberfläche¹⁰, die auf WPF (Windows Presentation Foundation) basiert, einem aus dem Hause Microsoft stammenden Graphik-Framework, das unter anderem die Trennung von Funktion und Design ermöglicht. Zum einen wurde das Programmfenster samt Haupt-Steuerelementen an den *2007 Microsoft Office System User Interface Design Guidelines* ausgerichtet, die von Microsoft nach der Neugestaltung der Benutzerschnittstelle von Office 2007 auch anderen Entwicklern mit einer gebührenfreien Lizenz zur Verfügung gestellt wird. Dabei ersetzt eine *Multifunktionsleiste* („Ribbon“) die vorherige Kombination aus Menü und Symbolleiste. Zum anderen erhält CrypTool 2 innerhalb des Programmfensters sein neues Kernelement, den Workspace zur visuellen Programmierung. Dabei handelt es

⁹ Aus dem Englischen von „to plug in“, im Deutschen also etwa „einstöpseln“. Gemeint ist hierbei, dass modulare Programmteile leicht über Schnittstellen eingebunden werden können und so den Funktionsumfang des eigentlichen Programms erweitern.

¹⁰ Auch GUI genannt für „Graphical User Interface“.

sich um eine Arbeitsfläche, auf der einzelne Bausteine (z.B. Algorithmen) zu einem mehr oder weniger komplexen Gesamtlauf zusammengestellt werden können (vgl. [Südmeyer]).

Die Planungen für die neue Programmversion beinhalten weitere Visualisierungen und Demonstrationen sowie Erweiterungen durch neue Algorithmen und Werkzeuge. Aus didaktischer Sicht interessant sind, neben der bereits oben erwähnten „visuellen Programmierung“, vor allem auch die geplanten „Einstiegsansichten für Anfänger und Experten“ , die in der betrachteten Programmversion leider noch nicht enthalten sind (vgl. [CT_46]).

2.1. Ziele des Programms

CrypTool wurde ursprünglich für IT-Sicherheits-Schulungen einer deutschen Großbank entwickelt. Durch die Veröffentlichung, zunächst als Freeware, dann als Open-Source unter einer freien Lizenz, fand CrypTool weitere Verbreitung. CrypTool bezeichnet sich als „DAS E-Learning-Programm für Kryptologie“. Verschiedenste kryptographische Verfahren sollen vom Benutzer angewendet und analysiert werden können (vgl. [Esslinger 1], S. 8, S. 24, S. 106).

In einer persönlichen Mail bestätigte mir der Leiter des CrypTool-Projektes, Prof. Bernhard Esslinger, dass die Benutzung von CrypTool (und hier ist auch explizit die zweite, also neue Programmversion gemeint) auch ohne eine Kryptographievorlesung oder Hilfestellung durch eine Lehrperson zugänglich sein soll und dass das Programm gerade im didaktischen Bereich verbessert werden soll.

Darüber hinaus bemüht sich das CrypTool-Projekt auch um ein breites Informations- und Unterstützungsangebot. So wurde im Jahr 2008 das *Cryptoportal für Lehrer* initiiert, eine Internetplattform, auf der Lehrer¹¹ Erfahrungen, Informationen und Unterrichtsmaterialien (wie Arbeitsblätter, Präsentationen oder Animationen) austauschen und diskutieren können. Außerdem existiert seit diesem Frühjahr die Webseite CrypTool-Online. Dieses Portal richtet sich an Einsteiger und junge Leute, denen im Internetbrowser (also ohne Softwareinstallation) „Appetit“ auf das Thema Kryptographie gemacht werden soll (vgl. [CT_42]).

¹¹ Gemeint sind hier vor allem Mathematik- und Informatiklehrer der allgemeinbildenden Schulen.

2.2. Leistungsumfang

CrypTool 2 ist noch bei weitem nicht so leistungsfähig wie die erste Programmversion. Fehlende oder unvollständige Programmteile, die meiner Einschätzung nach noch ergänzt werden sollen, sind insbesondere:

- Eine umfassende Online-Hilfe, also eine programmweite und kontextsensitive Hilfefunktion, die dem Benutzer bei der Lösung seines Problems behilflich ist.
- Eine deutschsprachige Programmoberfläche bzw. die Funktion, die Sprache umzuschalten.
- Die Visualisierungen der verschiedenen kryptographischen Algorithmen, ebenso bei den meisten Plugins eine Beschreibung des Plugins.
- Einige kryptographische Verfahren: Unter den noch fehlenden Algorithmen befinden sich auch bedeutsame wie *RSA*, *ECC* (Elliptic Curve Cryptography), *MARS*, *RC6* oder *Serpent*. Aber auch die Implementierung des Plugins *Enigma* ist noch nicht vollständig.
- Algorithmen zu digitalen Signaturen wie *DSA*, die *Schnorr-Signatur* oder die *Merkle-Signatur*.
- Einige Analysefunktionen: Im Navigationsfenster (*Navigation pane*) finden sich unter *Cryptoanalysis* lediglich die statistischen Hilfsmittel Häufigkeitsanalyse, Friedman- und Kasiski-Test sowie *Attack on the WEP protocol*. Die weiteren drei Elemente in dieser Rubrik sind eher Hilfsmittel bei der visuellen Programmierung. Unter *Tools* finden sich weitere Programmierbausteine wie auch ein Primzahltest und ein *Factorizer*, der eine Zahl in einen Primteiler und einen Rest faktorisiert.

Voll funktionsfähig dagegen wirkt die Programmoberfläche mit dem „*Workspace*“, also dem Arbeitsplatz, auf dem die durch Piktogramme (*Icons*) stilisierten Algorithmen angeordnet und untereinander verbunden bzw. kombiniert werden können. Dadurch entsteht ein „visuelles Programm“, das mittels *Play*, *Pause* und *Stop* gestartet und beendet werden kann. Es ist ebenfalls möglich, die so erstellten „visuellen Programme“ auf dem Computer zu speichern, um sie später erneut

aufzurufen. CrypTool 2 bringt bereits verschiedene *SampleProjects* (also gespeicherte visuelle Programme) mit, die einfach aufgerufen werden können.

Durch die Möglichkeit der visuellen Programmierung dürfte es mit CrypTool 2 recht einfach werden, sogenannte Hybrid-Verfahren (z.B. RSA-AES) selbst aufzubauen. Dieses Vorgehen vereint die Vorteile beider Verfahren. Asymmetrische Verfahren (oder auch Public-Key-Verfahren) können in unsicheren Umgebungen (z.B. Internet) aufgrund ihrer Funktionsweise sicher Nachrichten austauschen, sie sind aber rechenaufwändig und daher langsam. Symmetrische Verfahren wiederum sind recht schnell, benötigen aber einen sicheren Kanal zum Schlüsseltausch. Kombiniert man beide Techniken, so wird der Schlüssel des symmetrischen Verfahrens (hier AES) mit dem asymmetrischen Verfahren (hier RSA) verschlüsselt und kann damit über ein unsicheres Medium (wie das Internet) sicher ausgetauscht werden. Die eigentliche Nachricht wird dann symmetrisch (hier mit AES) verschlüsselt.

Weiterhin ermöglicht es die visuelle Programmierung auch Verfahren zur Kryptoanalyse nach eigenen Vorstellungen selbst zusammenzustellen. Hier kann ein Geheimtext¹² beispielsweise mit verschiedenen Analyse-Plugins betrachtet werden. Aber auch komplexere Abläufe sind möglich, wie das integrierte Projekt „Caesar_CipherTextOnly-Attack_de.cte“ zeigt. Hier wird versucht einen Caesar-chiffrierten Geheimtext systematisch mit verschiedenen Schlüsseln zu „entschlüsseln“, bis der (meistens immer noch unlesbare) „Klartext“ mindestens die vorgegebene Anzahl von Wörtern enthält, die in einem Wörterbuch zu finden sind. In dem Beispiel werden also (automatisiert) solange Schlüssel ausprobiert, bis etwas Sinnvolles dabei herauskommt – ein sogenannter *Brute-Force-Angriff*.

Informationen zu den einzelnen Modulen kann man mit der Taste F1¹³ erhalten, oder aber durch Auswahl von *Show Plugin description* im Einstellungsfenster der Plugin Eigenschaften *Algorithm Settings*.

¹² Der Begriff *Geheimtext* meint in der gesamten Hausarbeit ein Kryptogramm, also einen verschlüsselten Text. Der unverschlüsselte Text, also der eigentliche Inhalt des Geheimtextes (mathematisch gesehen das Urbild des Geheimtextes), heißt *Klartext*.

¹³ Die F1-Taste ruft traditionell die Hilfe-Funktion eines Programms auf.

Weitere Informationen erhält man in der sogenannten „*Präsentation*“ eines Algorithmus, indem man auf das Symbol eines Moduls innerhalb eines visuellen Programms doppelklickt.

Besonders interessant ist auch ein zweites, in CrypTool 2 integriertes Programm mit dem Namen *Primes*, oder auf deutsch *Die Welt der Primzahlen*. Damit können verschiedene zahlentheoretische Grundlagen oder Sätze praktisch „ausprobiert“ und graphisch dargestellt werden.

2.3. Vergleich von CrypTool 2 mit CrypTool 1.4.30 - Beta 04

CrypTool 2 ist keine Weiterentwicklung des bestehenden CrypTool 1.4.xx, sondern eine Neuentwicklung. Die technischen Aspekte sind für didaktische Betrachtungen nicht sonderlich interessant, die wesentlichen technischen Neuerungen wurden bereits kurz unter dem Gliederungspunkt 2. *Programmbeschreibung* zusammengefasst dargestellt.

2.3.1. Programmoberfläche

Bei CrypTool 1 ist das Programmfenster recht einfach gestaltet. Das Hauptprogrammfenster beinhaltet weitere Fenster („*Dokumente*“), in denen Text eingegeben werden kann oder aber die Resultate einer gewählten Aktion oder Transformation betrachtet werden können. Wird eine Aktion durchgeführt, bekommt man üblicherweise das Ergebnis dieser Aktion in einem neuen „*Dokument*“ präsentiert, während das ursprüngliche erhalten bleibt. Das Aufrufen einiger Funktionen führt dazu, dass weitere Fenster mit spezifischen Konfigurationsmöglichkeiten oder interaktive Flussdiagramme geöffnet werden. Insbesondere die verschiedenen Visualisierungen

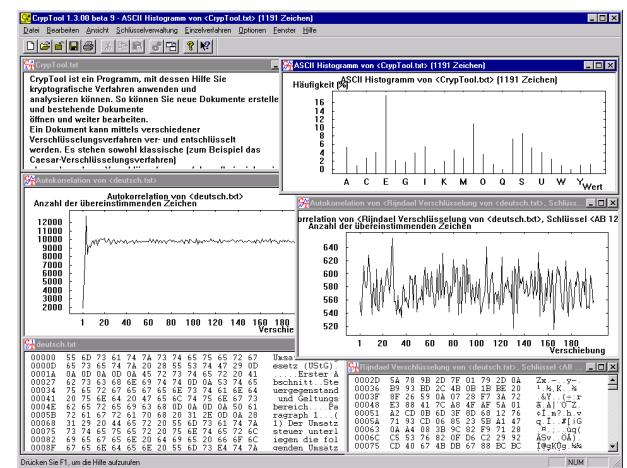


Abbildung 1: Ein Bildschirmfoto von CrypTool 1.4.xx [CT_48]

neuen „*Dokument*“ präsentiert, während das ursprüngliche erhalten bleibt. Das Aufrufen einiger Funktionen führt dazu, dass weitere Fenster mit spezifischen Konfigurationsmöglichkeiten oder interaktive Flussdiagramme geöffnet werden. Insbesondere die verschiedenen Visualisierungen

von komplexen Sachverhalten sind wiederum in externen Programmen oder interaktiven Präsentationen umgesetzt.

Der gesamte Funktionsumfang des Programms ist über Menüs in der Kopfzeile des Hauptfensters zugänglich, wobei die Menütiefe bis zu fünf Ebenen erreicht. Man muss sich also, um zum Ziel zu kommen, durch bis zu vier Untermenüs navigieren.

Bei CrypTool 2 wurde die gesamte Programmoberfläche neu entworfen, es erscheint moderner und ansprechender. In der Mitte des Arbeitsplatzes befindet sich der „*Workspace*“, auf dem visuelle Programme (ähnlich Ablaufdiagrammen) selbst erstellt werden können. Die dazu nötigen Algorithmen und weitere Module findet man im Navigationsfenster im linken Bildschirmbereich. Die komplexen Menüs und die minimalistische Symbolleiste wurden (wie von Microsoft im Office Paket 2007 vorgemacht) durch eine *Multifunktionsleiste (Ribbon)* ersetzt.

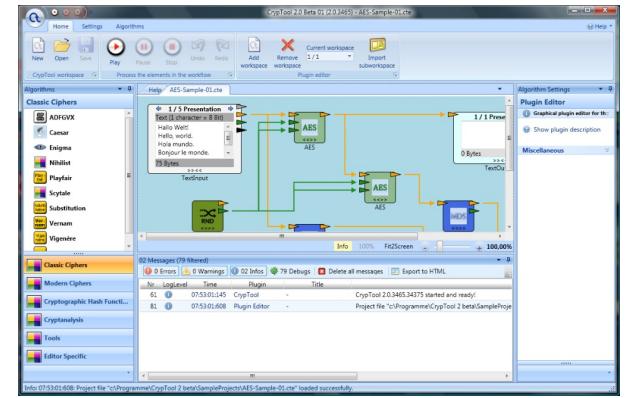


Abbildung 2: Ein Bildschirmfoto von CrypTool 2

2.3.2. Bedienung

Die Neuerungen der Programmoberfläche führen zu grundlegend veränderten Abläufen und einem neuen Bedienkonzept. Durch die visuelle Programmierung können eigene Abläufe viel freier gestaltet (und auch gespeichert) werden. Die Eingaben erfolgen in den jeweiligen Modulen, die nach eigenen Vorlieben angeordnet werden können. In CrypTool 2 können also nicht nur, wie in der Vorgängerversion, die verschiedenen Algorithmen ausprobiert werden, sondern es muss zuvor ein visuelles Programm erstellt werden, das die Aufgaben im Sinne des Benutzers löst. Dafür ist es in CrypTool 2 auch leicht möglich, komplexere Abläufe zu erstellen und anschließend auszuführen.

2.3.3. Zugaben

Die ursprüngliche Version von CrypTool enthielt viele Zugaben, die das Programm ergänzten und abrundeten. Ich gehe davon aus, dass ein Großteil davon auch in der finalen Version von CrypTool 2 enthalten sein wird, daher beschränke ich mich hier auf eine Nennung und kurze Beschreibung der einzelnen Ergänzungen:

- Am nächsten stehen dem eigentlichen Programm die Programmhilfe sowie das CrypTool-Skript ([Esslinger 2]) und die CrypTool-Präsentation ([Esslinger 1]). In der Programmhilfe sind Tutorials eingearbeitet, die Erklärungen und Anleitungen zu den einzelnen Verfahren enthalten. Das CrypTool-Skript bietet dem Anwender weiterführendes Wissen zur Mathematik und den kryptographischen Verfahren, während die CrypTool-Präsentation Informationen über das CrypTool Projekt beinhaltet und auch viele Anwendungsbeispiele bereit hält.
- Interessant sind auch die Animationen, die die Funktionsweise der einzelnen Algorithmen visualisieren. In Adobe-Flash werden Enigma und Rijndael anschaulich gemacht, elliptische Kurven (und die darauf definierten Punktaddition) kann man mit der in Java geschriebene ECC-Demo ausprobieren. Weitere animierte Visualisierungen von Algorithmen sind mit Animal (einem Java-basiertem Animationswerkzeug, das an der TU Darmstadt betreut wird) verwirklicht.
- AES-Tool ist ein alleine lauffähiges Programm und verschlüsselt eine Datei mit dem AES-Algorithmus.
- Ebenfalls alleine lauffähig ist das Authorware-Programm ZT (das zahlentheoretische Grundlagen zur asymmetrischen Verschlüsselung erklärt) sowie der TextZahlWandler.
- Zu guter Letzt möchte ich noch das Programm *Zahlenhai* (ein Kinderspiel zur Zahlentheorie), die beiden Kurzgeschichten zur Zahlentheorie im PDF-Format (*Das Chinesische Labyrinth* und *Der Dialog der Schwestern*) sowie Beispieldateien und *Crypto challenges* (verschlüsselte Geheimtexte zum ausprobieren) erwähnen.

2.4. Bisherige Arbeiten zu CrypTool 2

Auch wenn CrypTool 2 noch ein junges Projekt ist, so sind bereits mehrere Arbeiten entstanden, die sich mit dem zugrunde liegenden Konzept und dessen Realisierung beschäftigt haben. Da ich die didaktischen Aspekte der Umsetzungen später ansprechen möchte, stelle ich hier die beiden betreffenden Arbeiten kurz vor:

2.4.1. Diplomarbeit zum Editor für CrypTool 2

In seiner Diplomarbeit entwickelt und beschreibt Thomas Schmid den in CrypTool 2 verwendeten Editor ([Schmid]). Dazu widmet er sich zunächst der visuellen Programmierung im Allgemeinen¹⁴, dann der (eher technischen) Plugin-Struktur und schließlich der Entwicklung des Editors für CrypTool 2. Dieser Editor ermöglicht das Entwerfen und Ausführen visueller Programme in CrypTool 2, er stellt also damit den eigentlichen Workspace als Benutzerschnittstelle zur Verfügung.

Thomas Schmid implementiert nicht nur technische Aspekte, sondern betrachtet auch Didaktik und Usability. Er verwendet Farbcodierungen für verschiedene Datentypen und implementiert zudem eine farbliche Rückmeldung an den Benutzer über die Funktion der einzelnen Plugins in den Ampelfarben Rot, Gelb und Grün¹⁵.

Die von einem Plugin berechneten Daten können als „Präsentation“ in einem neuen Fenster geöffnet oder als „QuickWatch“-Ansicht im vergrößerten Symbol eines Algorithmus angezeigt werden.

Um die Komplexität zu reduzieren, führt er vier „Detail level“ ein, nach deren Einstellung verschiedene Ein- und Ausgänge der Plugins angezeigt bzw. verborgen werden. Die Idee dabei war, dass eine große Anzahl von Ein- und Ausgängen vor allem für Anfänger verwirrend ist, während fortgeschrittene Benutzer die Möglichkeiten voll ausschöpfen möchten.

Weiterhin führt er einen sogenannten „Play-Mode“ ein, der nötig wurde, um komplexere Aufgaben wie Schleifen oder automatisierte Vorgänge visuell

¹⁴ Hier stellt er auch die Vor- und Nachteile der visuellen Programmierung gegenüber.

¹⁵ Färbt sich das Symbol des Algorithmus grün, so gab es keine Probleme, gelb drückt eine Warnung aus und rot weist auf aufgetretene Fehler hin.

programmieren zu können. Daher muss die Ausführung des visuellen Programmes mit „*Play*“ gestartet und mit „*Stop*“ beendet werden. Während des *Play*-Modes sind einige Veränderungen, zum Beispiel an den Einstellungen eines Algorithmus, nicht möglich.

2.4.2. Diplomarbeit zu *Primes – Die Welt der Primzahlen*

Das in CrypTool 2 integrierte Standalone-Programm „*Die Welt der Primzahlen*“ wurde von Timo Eckhardt in seiner Diplomarbeit entwickelt. Sein Ziel war es, die Rolle von Primzahlen in der Kryptographie darzustellen und ihre Eigenschaften zu visualisieren (vgl. [Eckhardt]). Auch wenn ein paar zahlentheoretische Funktionen Einzug in das Programm gefunden haben, so liegt der Schwerpunkt in der Darstellung der Primfaktorzerlegung, diverser Primzahltests sowie der Verteilung der Primzahlen. In seiner Diplomarbeit stellt er die mathematischen sowie die technischen Hintergründe ausführlich dar und beschreibt den Aufbau seines Programms.

3. Didaktische Analyse

Didaktik ist, einer allgemein formulierten Definition zufolge, die „Theorie und Praxis des Lehrens und Lernens“ (vgl. [Jank/Meyer], S.16). CrypTool 2 ist ein Computer-Lernprogramm, das den Anspruch erhebt, Wissen und Fähigkeiten auf dem Gebiet der Kryptographie zu vermitteln. Daher möchte ich nun die didaktisch relevanten Besonderheiten des Lerngegenstandes Kryptologie analysieren und dabei an geeigneten Stellen die Gegebenheiten von CrypTool 2 berücksichtigen. Dabei betrachte ich im Wesentlichen die Aspekte, die auch bei der Planung bzw. Analyse einer konventionellen Unterrichtsstunde untersucht werden¹⁶.

3.1. Lerngruppenanalyse

Wie ich bereits zuvor betont habe, ist CrypTool 2 nicht für eine genau eingrenzbare Zielgruppe konzipiert; das Programm soll vielmehr von ganz unterschiedlichen Gruppen von Menschen angewendet werden können: Jemand, der sich privat für Kryptographie interessiert, soll ebenso angesprochen werden wie Gruppen, die Kenntnisse in der Kryptographie in beruflichen Kontexten benötigen (Mitarbeiter z.B. von Banken) oder diese Kenntnisse im Rahmen ihrer Ausbildung erlernen sollen (Schüler, Informatik- bzw. Mathematikstudenten).

Diese Tatsache bedeutet, dass zum einen die Motivation, sich mit der Materie der Kryptographie zu befassen, bei den verschiedenen Nutzergruppen sehr unterschiedlich sein wird, und dass zum anderen – was noch schwerwiegendere Implikationen für eine Lernsoftware haben müsste – die Vorkenntnisse der Nutzer in Mathematik und in der Anwendung von Computerprogrammen extrem voneinander abweichen können.

Studenten¹⁷ aus den Bereichen Mathematik und Informatik besuchen wahrscheinlich parallel zur Nutzung von CrypTool 2 eine themenverwandte Vorlesung, in der sie eine Einführung in Kryptographie, Hintergrundwissen und die

¹⁶ Ich orientiere mich hierbei an den *Ratschlägen für Stundenentwürfe* nach Jank/ Meyer, S. 408 – 420.

¹⁷ Die männliche Form wird nur des besseren Leseflusses wegen verwendet. Es sind jedoch immer weibliche wie auch männliche Personen gleichermaßen gemeint.

nötigen mathematischen Kenntnisse erhalten. Ein Mathematikstudent weiß, wie er mathematische Probleme selbst angehen kann, hat aber unter Umständen keine Erfahrung mit Programmierung. Er möchte bei der Benutzung von CrypTool 2 ein Werkzeug, das ihm bei der Lösung der Übungsaufgaben behilflich ist und ihn verschiedene Algorithmen ausprobieren und vergleichen lässt. Außerdem ist er möglicherweise an einer Verdeutlichung der zahlentheoretischen Grundlagen interessiert. Ein Informatikstudent wird darüber hinaus vermutlich eher an der Implementierung und dem praktischen Nutzen der Algorithmen interessiert sein. Für ihn ist es wichtig nachzuvollziehen, wie ein Algorithmus arbeitet und auch, die Möglichkeit zu haben, selbst einen Algorithmus zu programmieren. Auch er weiß, wie er sich – aus und neben der Begleitveranstaltung – benötigte Informationen zugänglich machen kann.

Ein Schüler (beispielsweise einer Realschule oder eines Gymnasiums¹⁸), der im Rahmen des Unterrichtes CrypTool 2 nutzt, hat weniger Vorwissen, das ihm aber ebenfalls von einem Lehrer vermittelt und auch erläutert wird. Es ist für ihn auch nicht wichtig, einen vollständigen Überblick über das Gebiet der Kryptographie zu haben, es reicht, wenn er exemplarisch die prinzipielle Funktionsweise kryptographischer Algorithmen versteht. Er braucht leicht zu verstehende und leicht zu bedienende Abläufe und Darstellungen. Einen Lernanreiz könnten kurze Geschichten, knifflige Rätsel oder die Möglichkeit, mit Freunden „echte“ Geheimbotschaften austauschen zu können, bieten. Betrachtet man darüber hinaus den Lehrplan Informatik für die Oberstufe in Rheinland-Pfalz ([MBWJK 1]), so werden hier die Themen *Sicherheitsziele*, *Moderne Verfahren zur Verschlüsselung* und *Signierung*¹⁹ sowie *Sicherheitsinfrastruktur*²⁰ verbindlich vorgeschrieben. Die *Prüfungsanforderungen in der Abiturprüfung* ([MBWJK 2]) beinhalten darüber hinaus Fragen nach der prinzipiellen Funktionsweise von asymmetrischen Verfahren

18 In Rheinland-Pfalz finden sich kryptographische Inhalte ausschließlich im Lehrplan des Faches Informatik für die Oberstufe. Da Geheimsprachen u. ä. jedoch ein spannendes Thema für Schüler sind und Aspekte wie die Sicherheit der eigenen Daten z. B. bei der persönlichen Computernutzung eine große Relevanz in der Lebenswirklichkeit der Schüler haben, ist der Lerngegenstand m. E. aber auch bei jüngeren Schülern, beispielsweise im Rahmen einer Projektwoche oder AG, zumindest in den Grundzügen behandelbar.

19 Insbesondere mit Blick auf asymmetrische Verfahren wie RSA und die Verwendung aktueller Werkzeuge wie „z.B. GnuPG“.

20 Hier sollen kursintern Schlüssel ausgetauscht und signiert werden.

(und Unterschiede zu den symmetrischen) sowie gesellschaftliche Aspekte.

Die dritte Zielgruppe sind allgemein an Kryptographie interessierte Computernutzer, deren mathematischen Schulkenntnisse möglicherweise schon recht verstaubt sind. Motivation einer solchen Privatperson könnte z. B. sein, erfahren zu wollen, wie Kryptographie funktioniert, beispielsweise weil er wissen möchte, wie sicher Online-Banking oder mobiles Telefonieren ist. Ein solcher Nutzer des Programms hat keinen Lehrer und weiß unter Umständen auch nicht, wie er an Hintergrundinformationen kommt. Daher benötigt er einen motivierenden und leicht verständlichen Überblick, allgemeinverständliche (und nicht zu technische oder mathematische) Vertiefungen und hilfreiche Beispiele, bei denen er selbst aktiv werden kann.

Mitarbeiter von Unternehmen aus Branchen, in denen Verschlüsselungstechniken eingesetzt oder gar entwickelt werden (wie z.B. Banken, Versicherungen, diverse Telekommunikationsdienstleister u.ä.), werden wahrscheinlich im Rahmen von Fortbildungen mit CrypTool 2 konfrontiert werden. Esslinger betont die Wichtigkeit, dass Kunden und Mitarbeiter „ein Mindestverständnis und Bewusstsein (Awareness) für IT-Sicherheit besitzen“ (vgl.[Esslinger 1], S. 6). Auch hier ist der Kenntnisstand der Benutzer sehr unterschiedlich; ein Programmierer aus der IT-Abteilung hat ein anderes Vorwissen als ein Sachbearbeiter oder jemand aus dem Kundendienst.

3.2. Sachanalyse

CrypTool bezeichnet sich als „DAS E-Learning-Programm für Kryptologie“ (vgl. [Esslinger 1], S. 106). Hier stellt sich die Frage, welche Inhalte das Thema *Kryptologie* umfasst und welches Wissen mit Hilfe von CrypTool 2 vermittelt werden kann und soll.

Zum einen lassen sich *Kryptographie* und *Kryptoanalyse* voneinander unterscheiden, also das Schreiben und das Analysieren bzw. „Knacken“ von verschlüsselten Botschaften. Aber auch die *Steganographie*, das „Verstecken“ von Nachrichten, gehört in den Bereich der Kryptologie und hat nicht nur historische Bedeutung, denn allein die Tatsache, dass eine Kommunikation stattfindet, kann verräterisch und verhängnisvoll sein (vgl. [Schröder]).

Den drei in der Einleitung erläuterten Hauptzielen der Kryptographie, dem Garantieren von Vertraulichkeit, Integrität und Authentizität der übermittelten Botschaften, lassen sich drei verschiedene Typen von Algorithmen zuordnen (vgl. [WP:WPK]):

- Verschlüsselungsverfahren gewährleisten die Vertraulichkeit. Hier lassen sich zunächst klassische von modernen, aber auch symmetrische von asymmetrischen Verfahren unterscheiden. Während die klassischen Methoden zumeist Substitution und Transposition verwenden, sind die modernen Verfahren eher mathematischer Natur. Insbesondere bei den asymmetrischen Verfahren (zum Verschlüsseln wird ein anderer Schlüssel verwendet als zum Entschlüsseln) finden zahlentheoretische Probleme eine praktische Anwendung. Außerdem werden Blockchiffren (es werden immer ganze Blöcke von n Zeichen verschlüsselt) von Stromchiffren (jedes Zeichen kann sofort beim Eintreffen verschlüsselt werden, z.B. bei Telefongesprächen im Mobilfunk oder bei Funknetzwerken) unterschieden.
- Die Integrität von Daten kann durch sogenannte Hash-Algorithmen gewährleistet werden. Ein Hash-Wert ist gewissermaßen eine Prüfsumme festgelegter Größe. Wird die Eingabe (auch nur geringfügig) geändert, so ergibt sich ein vollkommen anderer Hash-Wert. Werden Dateien über das Internet verbreitet, so wird häufig auch ein Hash-Wert dazu veröffentlicht. Der Empfänger der Datei kann nun den Hash-Wert der heruntergeladenen Datei berechnen und mit dem veröffentlichten Wert vergleichen. Bei Übereinstimmung der beiden Werte wurde die Datei korrekt übertragen.
- Signaturverfahren basieren auf denselben theoretischen Grundlagen wie asymmetrische Verschlüsselungsverfahren. Nur der Besitzer des geheimen Schlüssels kann aus einer Nachricht eine gültige digitale Signatur erstellen, die wiederum anhand des öffentlichen Schlüssels überprüft werden kann. Die eigentliche Nachricht wird dabei jedoch nicht verschlüsselt, sondern dient dem Signatur-Algorithmus lediglich als Eingabe. Wird die Nachricht danach verändert, so passt (ähnlich wie bei den Hash-Algorithmen) die originale Signatur nicht mehr zu der Nachricht, die Manipulation fällt auf.

Bedeutsam bei der Auswahl (und möglicherweise auch bei der Entwicklung) von kryptographischen Verfahren ist das *Kerckhoffs'sche Prinzip*, das besagt, dass die Sicherheit eines kryptographischen Verfahrens einzig auf der Geheimhaltung des Schlüssels beruhen soll. Man könnte zwar meinen, es sei besser, gleich das gesamte Verfahren geheim zu halten, doch die Vergangenheit (und Gegenwart) zeigt, dass dies nicht richtig ist. So wurden z.B. *Enigma* oder *Purple* (im Zweiten Weltkrieg) oder der Mobilfunkstandard GSM gebrochen, obwohl die Verfahren geheim gehalten wurden. Der Grund dafür ist, dass der Erfinder eines Verfahrens die entscheidenden Schwachstellen schlicht übersieht. Wird der Algorithmus hingegen offengelegt, also der kritischen Beurteilung durch Experten zugänglich, so hat er nur dann Bestand, wenn keine solchen Schwachstellen gefunden werden. Somit ist ein Verfahren, dass trotz Offenlegung nicht gebrochen ist, sicherer als ein geheimes (vgl. [Beutelspacher], S. 15f.).

Bei den Verfahren zur *Kryptoanalyse* muss zunächst unterschieden werden, welche Möglichkeiten bestehen, das Kryptosystem anzugreifen: Steht nur ein Geheimtext zur Verfügung (*known ciphertext attack*), besteht die Möglichkeit, Klartext und Geheimtext zu vergleichen (*known plaintext attack*) oder gar beliebige Klartexte in Geheimtexte verwandeln zu lassen (*chosen plaintext attack*), um daraus Schlüsse auf die Funktionsweise des Algorithmus ziehen zu können (vgl. [Beutelspacher], S. 16)?

Es stehen verschiedene Möglichkeiten zur Verfügung, einen Geheimtext zu analysieren. Die meisten sind statistischer Natur, wie eine Mustersuche oder die Betrachtung von Buchstabenhäufigkeit oder -verteilung. Namentlich zu nennen sind hier die Häufigkeitsanalyse, der Kasiski-Test und der Friedman-Test. Es existieren aber auch spezialisierte Analysemethoden, mit denen man versuchen kann, bestimmten Verschlüsselungsalgorithmen das Geheimnis zu entlocken (vgl. [WP:WPK]).

Das große Problem der *symmetrischen Verschlüsselungsverfahren*²¹ ist der Austausch des geheimen Schlüssels über einen „sicheren Kanal“. Wird der Schlüssel abgefangen oder mitgelesen, so kann auch der Angreifer die geheime Botschaft entschlüsseln.

21 Derselbe Schlüssel wird zum Ver- und Entschlüsseln des Geheimtextes verwendet.

Anders bei den *asymmetrischen Verfahren*: Bei asymmetrischen Kryptoverfahren existieren zwei verschiedene Schlüssel. Einer der beiden wird für jedermann sichtbar veröffentlicht, daher heißt er „*öffentlicher Schlüssel*“, der andere bleibt wie gewohnt geheim, er wird „*privater Schlüssel*“ genannt. Das Verfahren wird wegen des veröffentlichten Schlüssels auch als „*Public-Key-Verfahren*“ bezeichnet. Möchte man jemandem eine geheime Nachricht zukommen lassen, so verschlüsselt man die Nachricht mit dem öffentlichen Schlüssel des Empfängers und verschickt den Geheimtext über ein öffentliches Medium. Der Empfänger wiederum verwendet zum Entschlüsseln der Nachricht seinen geheimen *privaten Schlüssel*. Ein Vergleich aus der Alltagswelt ist der Briefkasten, in den jeder eine Nachricht einwerfen kann, den jedoch nur der Schlüsselinhaber öffnen und die für ihn bestimmten Nachrichten lesen kann. Auch elektronische Signaturen werden auf diese Weise ermöglicht. Der Besitzer des geheimen Schlüssels kann eine Nachricht signieren und jeder, der Zugriff auf den zugehörigen öffentlichen Schlüssel hat, kann diese Signatur überprüfen (vgl. [Beutelspacher], S. 93 – 101).

Die Funktionsweise und damit die Sicherheit der asymmetrischen Algorithmen liegt in der Zahlentheorie begründet. Es gibt verschiedene mathematische Probleme, die hierzu verwendet werden können; dabei handelt es sich um „*Einwegfunktionen*“. Eine Einwegfunktion ist eine Funktion, die relativ einfach aus einem Klartext einen Geheimtext berechnen kann. Allerdings ist die Umkehrfunktion dazu, also die Ermittlung des Klartextes aus dem Geheimtext, nur mit unvertretbar hohem Aufwand an Zeit, Speicherplatz und Rechenleistung zu berechnen. Bisher konnte noch bei keiner Funktion streng bewiesen werden, dass sie eine solche Einwegfunktion ist – allerdings gibt es genügend viele Funktionen, die für praktische Zwecke hinreichend gute Einweg-Eigenschaften haben. Doch muss es für den Empfänger der Nachricht eine effiziente Möglichkeit geben, die Umkehrfunktion zu ermitteln. Dies geschieht mit Hilfe von geheimer Zusatzinformation, weshalb man von einer „*Einweg-Funktionen mit Falltür*e“ spricht (vgl. [Bauer], S. 156 – 160).

Die beiden prominentesten Beispiele für solchen „*Einweg-Funktionen mit Falltür*e“ sind die Multiplikation ganzer Zahlen (invers: Faktorisierung von großen Zahlen) sowie die Exponentiation über GF(p) (invers: diskreter Logarithmus). Die Anwen-

dungen dazu sind RSA und das ElGamal-Kryptosystem (vgl. [Bauer], S. 158 -168).

Die zugrunde liegende Mathematik ist zwar nicht sonderlich schwer, für Laien aber dennoch nicht eingängig und auch nicht gut überschaubar. Vor allem sind Kenntnisse über das Rechnen in endlichen Körpern nötig, also auch über das Rechnen mit Restklassen („Modulo-Rechnung“). Darüber hinaus sind für das Verständnis von RSA und den Umgang damit Kenntnisse folgender Sätze, Verfahren und Zusammenhänge wichtig: Der ggT²², der (erweiterte) Euklid'sche Algorithmus, der Chinesische Restsatz, Primfaktorzerlegung und Primzahlerzeugung (Primzahltests), die Eulersche φ -Funktion, der kleine Satz von Fermat sowie der Satz von Euler-Fermat. Für ElGamal sind vor allem zwei Algorithmen zu nennen, der Square and Multiply-Algorithmus zum schnellen Potenzieren und der Baby-Step Giant-Step Algorithmus²³ zur Berechnung des diskreten Logarithmus (vgl. [Buchmann], [Schröder]). Auf diese zahlentheoretischen Grundlagen möchte ich jedoch, ebenso wie auf die einzelnen kryptographischen Algorithmen, nicht näher eingehen, da dies den Rahmen dieser Arbeit sprengen würde.

3.3. Didaktisch-methodische Überlegungen

Die didaktische Analyse nach Wolfgang Klafki soll klären, „ob sich das, was man da den Schülern anzubieten hat, überhaupt lohnt!“, also „welcher Bildungsgehalt in den Unterrichtsinhalten stecken könnte“ ([Jank/Meyer], S. 133). Diese didaktische Analyse ist immer an eine konkrete Lerngruppe gebunden und daher so allgemein gar nicht durchführbar. Von Interesse allerdings dürften die fünf Grundfragen Klafkis sein, die nach *Gegenwarts- und Zukunftsbedeutung*, *Sachstruktur* sowie *exemplarischer Bedeutung* und *Zugänglichkeit des Lerninhaltes* fragen (vgl. [Jank/Meyer], S. 133).

Didaktik soll also eine Brücke bauen zwischen dem Einzelnen bzw. der Lerngruppe und dem theoretischen und abstrakten Wissen der Lehre. Dabei müssen inhaltliche Schwerpunkte gesetzt und potentielle Lernschwierigkeiten erkannt werden. Außerdem bedarf es einer, auf die Lerngruppe zugeschnittenen, didaktischen

22 Gemeint ist der größte gemeinsame Teiler.

23 Von D. Shanks.

Reduktion. Im Folgenden diskutiere ich Klafkis Grundfragen, bezogen auf die in der *Lerngruppenanalyse (3.1.)* erläuterten Ziel- bzw. Nutzergruppen von CrypTool 2, im jeweils letzten Absatz zu jeder Grundfrage werde ich die thematisch passenden Lernangebote der aktuellen Programmversion von CrypTool 2 darstellen.

3.3.1. Gegenwartsbedeutung

Verschlüsselungstechniken sind in unserem modernen und vernetzten Leben längst allgegenwärtig – und ihre Bedeutung wird mit dem stetigen Fortschritt in der Kommunikationstechnologie weiter zunehmen. Die meisten Menschen nutzen täglich mehrfach kryptographische Verfahren zur Gewährleistung von Vertraulichkeit, Integrität und Authentizität, oft allerdings ohne sich dessen bewusst zu sein.

Auf der anderen Seite sind die genannten Hauptziele der modernen Kryptographie oft nicht bekannt und es mangelt am Interesse für die technischen Hintergründe. Dadurch ist die subjektiv empfundene Bedeutung von Kryptographie sehr gering.

In CrypTool 2 wird zur Zeit nicht an die alltäglichen Anwendungen bzw. Vorkenntnisse angeknüpft und auch die Hauptziele der Kryptographie werden ausschließlich in der CrypTool Präsentation (vgl. [Esslinger 1], S. 7) angesprochen. Auch im CrypTool Skript [Esslinger 2] fehlt dieser Einstieg.

3.3.2. Zukunftsbedeutung

Die Frage nach der Bedeutung, die die Kryptographie in der Zukunft des Lernenden haben sollte, beantwortet Esslinger damit, dass „die Nutzer (Kunden, Mitarbeiter) ein Mindestverständnis und Bewusstsein (Awareness) für IT-Sicherheit besitzen“ ([Esslinger 1], S. 6). Dies trifft meines Erachtens jedoch auf jeden Menschen zu, der kryptographische Verfahren im Rahmen moderner Kommunikation anwendet.

Ausgehend von den Bedürfnissen moderner Kommunikation ist es enorm wichtig, ein Bewusstsein für Sicherheitsrisiken und Angriffsmöglichkeiten zu entwickeln. Natürlich sind hier Mitarbeiter von Firmen, die entsprechend sensible Daten verarbeiten, besonders betroffen. Doch auch ein Laie, der beispielsweise lediglich

eine Online-Überweisung tätigen möchte, sollte die Warnmeldung seines Internetbrowsers richtig interpretieren können, wenn dieser ihn auf ein ungültiges (also möglicherweise gefälschtes) Zertifikat hinweist. Daher wird dieser Awareness-Aspekt bei den später zu formulierenden Lernzielen eine wichtige Rolle spielen.

Ein grober Überblick über die verschiedenen (klassischen wie modernen, symmetrischen wie asymmetrischen) Techniken der Kryptographie ist für alle Anwender zumindest informativ oder gar interessant. Darüber hinaus sollen Schüler, Studenten und auch angestellte Programmierer Grundlagen, Aufbau und Hintergründe der Algorithmen nachvollziehen können und verstehen.

Auch zu den Aspekten Awareness, Überblick und Verwendung kryptographischer Verfahren im Alltag gibt es zur Zeit in CrypTool 2 keine Anknüpfungspunkte oder Lernangebote. Die Funktionsweise eines Algorithmus kann nur vereinzelt nachvollzogen werden, es ist lediglich möglich, die implementierten Verfahren anzuwenden. Im CrypTool Skript der Programmversion 1.4.30 ([Esslinger 2]) finden sich jedoch ein Überblick und Ausführungen zu den einzelnen Verfahren.

3.3.3. Sachstruktur

Das Sachgebiet der Kryptologie ist sehr komplex und es gibt verschiedene Möglichkeiten, dieses zu strukturieren. Alle Strukturierungen haben jedoch Vor- und Nachteile, so dass es für einen umfassenden Überblick unumgänglich ist, die verschiedenen Strukturierungen miteinander zu verbinden.

Es ist möglich, die Entwicklung der Kryptographie geschichtlich nachzuzeichnen und so neben Anekdoten und Exkursen zu geschichtlichen Ereignissen den Einsatz und die Bedeutung von Geheimcodes in verschiedenen Zeitaltern und Kulturen darzustellen. Interessant ist auch der Wettlauf zwischen dem Erfinden und Brechen kryptographischer Verfahren. Diese Struktur ist recht organisch und vor allem für Laien kurzweilig und motivierend. Allerdings haben hier die modernen Verfahren nur eine geringe Bedeutung und kommen daher zu kurz.

Eine weitere Möglichkeit besteht in der Strukturierung nach den Typen und Aufgaben der verschiedenen Verschlüsselungsverfahren. Zum einen sind dies die symmetrischen Algorithmen mit den Prinzipien Substitution und Permutation, aber

auch Block- und Stromchiffren müssen unterschieden werden. Zum anderen sind die asymmetrischen Verfahren zu nennen, die zahlentheoretische Probleme zur Basis haben und so eine *public key - Kryptographie* ermöglichen. Auch können Signatur- und Hashalgorithmen die genannten Kategorien erweitern. Diese Einteilung ist jedoch recht technisch und für Personen ohne Vorwissen recht trocken. Auch müssen die entsprechenden Grundlagen schrittweise erarbeitet werden.

Mir scheint es plausibler, von den bereits mehrfach erwähnten Hauptzielen der Kryptographie auszugehen. So lassen sich die, aus didaktischer Sicht wichtigen, Bedürfnisse der modernen Kommunikation und der damit verwandte *Awareness*-Aspekt gut integrieren. Andererseits betont diese Struktur die modernen asymmetrischen Verfahren, während die klassischen Verschlüsselungen, aber auch die modernen symmetrischen Algorithmen nur eine geringe Bedeutung haben oder ganz aus dem Schema fallen.

CrypTool 2 ordnet die verschiedenen Algorithmen in die sechs Kategorien *Classic Ciphers*, *Modern Ciphers*, *Cryptographic Hash Functions*, *Cryptoanalysis* sowie *Tools* und *Editor Specific*. Somit wählt CrypTool hauptsächlich die technische Einteilung, wenn auch mit Einfluss der geschichtlichen Strukturierung. Besonders die beiden letzten Kategorien lassen aber auch erkennen, dass der Schwerpunkt der Arbeit mit CrypTool 2 auf der visuellen Programmierung liegt.

3.3.4. Exemplarische Bedeutung

Klafkis Frage nach *der exemplarischen Bedeutung* eines Lerninhaltes zielt darauf, welche allgemeinen Schlüsse aus einem konkreten Beispiel gezogen werden können und ob es geeignet ist, den dahinter stehenden Gesamtzusammenhang erkennbar zu machen. So kann man am Beispiel einer Online-Banking-Sitzung die Bedürfnisse moderner Kommunikation darstellen. Die Funktionsweise einer asymmetrischen Verschlüsselung lässt sich dann beispielsweise anhand des RSA-Algorithmus deutlich machen.

In der gegenwärtigen Version von CrypTool 2 existieren keine Lerneinheiten oder Beispiele, die für Personen ohne Vorwissen hilfreich wären²⁴. Ebenso wenig gibt es

²⁴ Die vorhandenen gespeicherten visuellen Programme ermöglichen diesem Nutzerkreis keinen

eine Anleitung oder andere Formen der Hilfestellung, die einem Kryptographie-Neuling Orientierung gäben oder die Gelegenheit, allgemeine Prinzipien an einem konkreten Beispiel nachzuvollziehen. Soll CrypTool 2 es dem Anwender ermöglichen, selbständig Zusammenhänge und Prinzipien der Kryptographie zu erkennen, so müssen eine solche Orientierung und leicht verständliche Beispiele noch ergänzt werden.

3.3.5. Zugänglichkeit

Hier sind motivierende Einstiegsmöglichkeiten (Probleme, Beispiele, Geschichten) oder leicht verständliche Fragen oder Impulse gemeint, die den Lernenden für das Thema begeistern oder interessieren können²⁵. Hier sehe ich zwei eher affektive und eine eher sachlich-nüchterne Möglichkeit:

Schüler werden von Geheimnissen angezogen. Die Geschichte der Kryptographie ist voll von solchen mysteriösen Geschehnissen oder kniffligen Rätseln. Auch interessierte Computernutzer und Laien sind mit kurzweiligen Erzählungen oder Knobeleien zu begeistern. Daher wird diese Art der Darstellung auch gerne von populärwissenschaftlicher Literatur oder Software²⁶ gewählt.

Ebenso stellt sich vor allem für Computernutzer ohne Vorerfahrungen die Frage, ob und wie ein Angreifer persönliche Daten abfangen kann und wie man sich davor schützen kann. Proband 8 wünscht sich beispielsweise eine leicht verständliche, aber ausführlich erläuterte Darstellung einer „typischen Bankverschlüsselung“. Dabei fragt er sich, ob ein Hacker nicht doch die Verbindung entschlüsseln kann. Daher wäre es bei einer solchen Darstellung auch reizvoll, wenn Angriffsmöglichkeiten aufgezeigt und erläutert würden.

Eine dritte eher sachliche Möglichkeit in das Themengebiet einzusteigen, bietet sich über die Sicherheitsziele der modernen Kommunikation an. Hier können die

Lernzuwachs.

25 Bei der CD *The Code Book on CD-ROM* von Simon Singh ([Singh]) beispielsweise startet das Programm mit einem schwarzen Bildschirm, auf dem als Hintergrund zu dem gerade erscheinenden Logo ein verschlüsselter Geheimtext aufgebaut wird, während dabei eine Sequenz aus Morsezeichen zu hören ist. Für ein ernsthaftes E-Learning-Programm wie CrypTool sind solche Effekte jedoch nicht sinnvoll, da sie bereits nach kürzester Zeit lästig werden.

26 Wie beispielsweise die CD *The Code Book on CD-ROM* von Simon Singh ([Singh]).

Prinzipien der Vertraulichkeit, Integrität und Autentizität erläutert werden und wie die moderne asymmetrische Kryptographie diese Ziele erreichen kann.

CrypTool 2 berücksichtigt zur Zeit leider noch keine dieser Einstiegsmöglichkeiten. Es ist scheinbar bewusst nüchtern und sachlich gehalten, der Anwender kann sofort den Workspace zur visuellen Programmierung nutzen.

3.4. Befragung von Probanden zur Arbeit mit CrypTool 2

Um konkrete Hinweise auf Probleme im Umgang mit CrypTool 2 oder auch Verbesserungsvorschläge zu erhalten, entwarf ich einen Fragebogen²⁷, den ich einer heterogenen Probandengruppe zur Bearbeitung vorlegte. Dazu wählte ich als Probanden zwölf Mathematikstudenten oder -lehrer (einige davon besuchten eine Kryptographievorlesung, andere einen Programmierkurs) und dreizehn andere Personen verschiedenen Alters, die Mathematik lediglich als Schulfach hatten und die verschiedene Berufe ausüben²⁸.

Ziel war es, die Probanden zunächst durch die Bearbeitung von „Arbeitsblättern²⁹“ mit dem Programm vertraut werden zu lassen, um sie dann selbstständig ein „visuelles Programm“ gestalten zu lassen, das einen Geheimtext (bei angegebenem Verfahren und Schlüssel) wieder entschlüsselt. Die dadurch gewonnenen Erfahrungen im Umgang mit CrypTool 2 wurden anschließend abgefragt. Von besonderem Interesse waren für mich die hierbei auftretenden Probleme, die Beurteilung der Oberfläche und Verbesserungsvorschläge.

Beim Erstellen der Arbeitsblätter wollte ich eine breite Auswahl von Algorithmen verwenden. Dabei kam es leider zu Problemen, so dass ich meine Ziele den Gegebenheiten anpassen musste:

27 Der Fragebogen und die Antworten der Probanden sind im Anhang angefügt.

28 Das Spektrum reicht vom Oberstufenschüler bis zum Rentner, vom Krankenpfleger über Versicherungskaufmann bis hin zum Netzwerkadministrator.

29 Gemeint sind hier von mir entworfene *visuelle Programme*, also bereits vorgefertigte Ablaufdiagramme zu verschiedenen Verfahren und Aufgabenstellungen. Diese „Arbeitsblätter“ verbreitete ich als in CrypTool 2 aufrufbare .CTE-Dateien. Bildschirmfotos dieser Arbeitsblätter finden sich im Anhang.

- In der angegebenen Version von CrypTool 2 sind noch keine asymmetrischen Verschlüsselungsverfahren (wie RSA oder El Gamal) implementiert. Daher sind leider keine Aufgaben dazu möglich. Das ist insbesondere bedauerlich, da dadurch auch die bereits mehrfach erwähnten Hauptziele der Kryptographie sowie die mathematischen Grundlagen nicht durch die Probanden getestet werden konnten. Also entschied ich mich, als abschließende, selbständige zu lösende Aufgabe einen mit Enigma verschlüsselten Text entschlüsseln zu lassen.
- Mir fielen einige fehlerhafte oder unvollständig implementierte Plugins auf. Beispielsweise gab es bei *Enigma* nicht unterstützte Einstellungsmöglichkeiten, ein AES-verschlüsselter Text konnte mit einem falschen Schlüssel erfolgreich entschlüsselt werden und die Analysewerkzeuge *Kasiski-Test* und *Frequency-Test* zeigten sachlich falsche Analyseergebnisse an. Die gefundenen Fehler habe ich an Professor Esslinger gemeldet, damit das CrypTool-Entwicklerteam diese in den kommenden Versionen beheben kann, doch durch die fehlerhaften Ausgaben und Funktionen wurden verschiedene von mir geplante Aufgabenstellungen unmöglich gemacht bzw. erschwert.
- Des Weiteren fielen mir mehrere potentielle Schwierigkeiten³⁰ auf, die die Arbeit der Probanden erschwerten, so dass ich die Aufgaben mit einer sehr kleinschrittigen Anleitung zum Umgang mit dem Programm ausstatten musste, um diese Hürden zu umschiffen. Im Verlauf des Fragebogens reduzierte ich die Hilfestellungen und erwartete mehr Eigenleistung der Probanden.

Dadurch entstanden insgesamt fünf Aufgaben zu den Verfahren *Caesar*, *Vigenère* und *Enigma*, bei denen Ver- und Entschlüsselungen ausprobiert und Analysewerkzeuge benutzt werden sollten. Zu dem Verfahren *AES* war es auf Grund der beschriebenen Problematik leider nicht möglich, eine gute Aufgabe zu entwerfen,

³⁰ Namentlich der (zu) kleine Arbeitsplatzbereich kann mit der Taste F11 maximiert werden; um einen Algorithmus in Gang zu setzen muss man das *Start*-Symbol drücken und zum Ändern der Einstellungen dann *Stop*. Außerdem gab ich einen Hinweis darauf, wie die Größe der Säulendiagramme von *Frequency-Test* und *Kasiski-Test* so zu ändern ist, dass sie in den dafür vorgesehenen Anzeigenbereich passen.

doch in Hinblick auf die selbständig zu lösende *Enigma*-Aufgabe beließ ich das Grundgerüst des visuellen Programms zu *AES* als (für die Probanden unbewusste) Anregung in der Aufgabenstellung.

Obwohl ich von vielen Probanden im Vorfeld eine Zusage erhalten hatte, CrypTool 2 zu testen, war die Rücklaufquote der Fragebögen nur wenig befriedigend. Von fünf Probanden erhielt ich die Antwort, dass das von ihnen genutzte Betriebssystem nicht den Anforderungen von CrypTool 2 entspräche³¹. Ein weiterer Proband besaß nur einen langsamen Modemzugang zum Internet und konnte das nötige Framework nicht auf seinem Rechner installieren³².

Schließlich erhielt ich von neun Probanden überhaupt keine schriftliche Antwort. Davon entschuldigten sich drei wegen Zeitmangel mündlich, zwei gaben an, zwar CrypTool 2 installiert zu haben, dann aber nicht zurecht gekommen zu sein.

Die verwertbaren zwölf Antworten sind aber erfreulicherweise sowohl von Mathematikstudenten (sieben Antworten) als auch von anderen Probanden (fünf Antworten). Zunächst erwartete ich, dass die Bewertung von CrypTool 2 entlang dieser Nutzergruppengrenze signifikant unterschiedlich ausfallen würde, doch auch wenn sich dies zum Teil bewahrheitete, wurde ich eines Besseren belehrt: Zwei Mathematikstudenten hatten massive Probleme mit der Bedienung von CrypTool 2 (Probanden 4 und 12, zum Teil nur mündlich geäußert), während zwei der Probanden ohne fortgeschrittene Mathematikkenntnisse relativ gut zurecht kamen (Probanden 6 und 11).

Interessant ist ebenfalls, dass aus beiden Nutzergruppen ähnliche Bewertungen und Verbesserungsvorschläge gemacht wurden³³, was mich schließlich zu der Überzeugung gelangen lässt, dass die Schwierigkeiten in der Bedienung von CrypTool 2 unabhängig vom individuellen Vorwissen ist.

31 CrypTool 2 benötigt Windows XP oder neuer (zuzüglich .NET Framework der Version 3.5 SP 1). Drei Probanden besaßen lediglich einen MAC, zwei weitere arbeiteten ausschließlich mit Linux.

32 Auch nachdem ich ihm die nötigen Programme (inklusive des 231.5 MB großen *Microsoft .NET Framework 3.5 Service pack 1 (Full Package)*) auf CD-ROM zukommen ließ, klagte er darüber, dass das Installationsprogramm eine Internetverbindung benötige und brach die Installation ab. Einige Zeit später berichtete ein weiterer Proband, dass er vor dem *Microsoft .NET Framework 3.5 Service pack 1* zunächst den *Windows Installer 3.1* installieren musste, so dass ich denke, dass dies auch das Problem des o.g. Probanden war.

33 Diese werde ich später bei den jeweiligen Aspekten einfließen lassen.

Die Rückmeldungen zur Benutzeroberfläche von CrypTool 2 waren sehr durchwachsen: Während ein Teil der Probanden offensichtlich überfordert war und sich über den „extrem unübersichtlich[en]“³⁴ bzw. „verwirrend[en] und irritierend[en]“³⁵ Aufbau des Programmfensters beklagten, empfanden andere die graphische Aufbereitung des Arbeitsplatzes als „ansprechend ... [und] modern“³⁶ „optisch gut aufbereitet“³⁷ oder aber als „trocken“³⁸.

Den meisten Probanden war die Omnipräsenz von kryptographischen Verfahren (zumindest ansatzweise) bewusst. Das größte Interesse wurde gegenüber Onlinebanking, Anwendungen und Geschichte der Kryptographie sowie den Möglichkeiten von Hackern bekundet, weshalb sich diese Aspekte gut als Einstieg in die Thematik eignen.

3.5. Lernziele

Die Darstellung der Nutzertypen lässt die Vielzahl der unterschiedlichen Erwartungen erahnen. Sowohl Vorkenntnisse, Erwartungen und Arbeitsweise der Nutzer als auch der Grad der Unterstützung außerhalb des Programms sind grundlegend verschieden und müssen individuell berücksichtigt werden. Daher möchte ich zusammenfassend folgende Lernziele formulieren, die sich individuell an Motivation und Intention der Zielgruppen orientieren:

- Studenten sollen
 - die Bedürfnisse moderner Kommunikation erkennen und ein Bewusstsein für IT-Sicherheit bekommen.
 - praktische Erfahrungen mit verschiedenen Algorithmen und Analyseverfahren sammeln sowie die dazugehörigen mathematischen Hintergrundkenntnisse vertiefen.

34 Proband 2.

35 Proband 4.

36 Proband 6.

37 Proband 8.

38 Proband 10.

3. DIDAKTISCHE ANALYSE

- moderne Kryptographie-Algorithmen schrittweise nachvollziehen und die Möglichkeit haben, diese selbst zu reimplementieren.
- Ideen zu eigenen Algorithmen und Ablaufdiagrammen umsetzen.
- Schüler sollen
 - ausgehend von den Sicherheitsproblemen unverschlüsselter elektronischer Kommunikation die Vorteile der Verwendung von Kryptographie erkennen.
 - einen groben Überblick über symmetrische und asymmetrische Techniken der Kryptographie erhalten und exemplarisch nachvollziehen.
 - selbst Nachrichten ver- und entschlüsseln bzw. signieren. Dabei soll der Umgang mit privatem und öffentlichen Schlüssel geübt werden.
- Interessierte Laien und Mitarbeiter von Firmen sollen
 - ein Bewusstsein für Sicherheitsrisiken (bei der Kommunikation aber auch bei der Datenspeicherung) bekommen und die Notwendigkeit der Verwendung moderner kryptographischer Verfahren erkennen.
 - selbst mit kryptographischen Algorithmen arbeiten und dabei Erfahrungen sammeln.
 - Angriffsmöglichkeiten und Fehlerquellen verstehen und Warnmeldungen (z.B. des Internetbrowsers) richtig interpretieren können.

4. Betrachtung von CrypTool 2

Da einer persönliche Bewertung oder Einschätzung stets individuelle Vorerfahrungen zugrunde liegen, sehe ich mich veranlasst, die beiden wesentlichen auf mich wirkenden Einflüsse kurz darzustellen.

Ein wesentlicher Punkt ist, dass die letzte auf meinem privaten Rechner installierte Windows-Version Windows 98SE war. Seitdem verwende ich eine GNU/Linux Distribution mit der Benutzeroberfläche Gnome. Das Gnome-Projekt ist bemüht, die Benutzeroberfläche einfach, übersichtlich und benutzerfreundlich zu halten. Dazu wurden die *Gnome Human Interface Guidelines* ([Gnome HIG]) entwickelt, welche (unter anderem) Richtlinien zu Usability-Prinzipien wie Konsistenz, Fehlertoleranz, Einfachheit oder unmittelbaren Datenänderungen enthalten.

Ein weiterer Einfluss stammt von Donald Norman. Im Buch *Dinge des Alltags* [Norman 1] fordert er vor allem, dass sich das Design am Zweck orientieren soll und dass Strukturen vereinfacht sowie Sachverhalte sichtbar gemacht werden sollen. Außerdem warnt er vor der „schleichenden Seuche der Leistungsmerkmale“. Im späteren Buch *Emotional Design* [Norman 2] betrachtet er das Phänomen, warum billiger Wein in edlen Gläsern besser schmeckt und warum attraktive Dinge besser funktionieren.

4.1. Installation und Programmstart

4.1.1. Installationsvoraussetzungen

CrypTool 2 ist eine neu entwickelte Software, die auf aktuellen Entwicklungsgeräten basiert. Daher wird das (von Microsoft kostenlos erhältliche) .NET Framework 3.5 mit Service Pack 1 benötigt, welches seinerseits Windows XP oder neuer benötigt.

Da dieses Framework zunächst nicht in Windows enthalten ist³⁹, muss es aus dem Internet heruntergeladen und installiert werden. Die Dateigröße beim Download des .NET Frameworks beträgt bis zu 231,5 MB, was mit einem Modem etwa

³⁹ Weder in Windows XP noch in Vista. Ab Windows 7 wird .NET 3.5 vermutlich integriert sein.

inakzeptable neuneinhalb Stunden dauert, auch mit DSL sind es noch etwa fünfeinhalb Minuten.

Diese Installationsvoraussetzungen sind recht hoch, wodurch ein großer Teil potentieller Nutzer, ebenso wie mindestens sechs meiner Probanden (siehe auch *Befragung von Probanden zur Arbeit mit CrypTool 2 (3.4.)*), von vorneherein ausgeschlossen wird.

Da die Verwendung von WPF⁴⁰ und des .NET Frameworks eine entwicklungs-technische Grundsatzentscheidung ist (vgl. [Südmeyer]), kann ich hier keinen Verbesserungsvorschlag machen. Durch die Integration des .NET Frameworks 3.5 in Windows 7 wird dieses Hemmnis vermutlich in wenigen Jahren an Bedeutung verlieren. Für die Nutzer anderer Betriebssysteme könnte eventuell die plattform-unabhängige Java Version des CrypTool Projektes, JcrypTool, eine Alternative werden.

4.1.2. Programmstart

Der Start von CrypTool 2 dauert (im Vergleich zu CrypTool 1.4.30) sehr lange. In dieser Zeit wird dem Benutzer jedoch ein *Splash Screen* angezeigt, so dass erkennbar ist, dass das Programm geladen wird. Später erscheint ein Fortschrittsbalken und graphisch ansprechend gestaltete Textmeldungen informieren den Benutzer über den Startvorgang und das Laden der einzelnen Plugins.



Abbildung 3: Der *Splash Screen* von CrypTool 2

Diese Lösung ist begrüßenswert. Dadurch erhält der Nutzer eine direkte Rückmeldung über den Programmstart und denkt nicht etwa nach einigen Sekunden, das CrypTool 2 abgestürzt sei. Jedoch ist die weiße Schrift auf hellblauem, mit weißem Muster durchsetztem Hintergrund nicht gut lesbar (siehe Abbildung 3). Eine Probandin teilte mir mündlich mit, das sie die vorbeieilenden Textmeldungen (siehe

40 Windows Presentation Foundation.

Abbildung 4) verwirrend fand, da sie diese Darstellung nicht von anderen Programmen kannte und sie nicht wusste, ob die Meldungen für sie relevant sind. Hier ließe sich eventuell statt der Logbuch-artigen Darstellung eine Statuszeile mit der aktuell durchgeführten Aktion unter der Fortschrittsanzeige integrieren. Auch die Wahl einer dezenteren Farbe verdeutlicht die geringe Bedeutung dieser Meldungen für den Anwender.



4.2. Graphische Oberfläche von CrypTool 2

Das nach dem Start des Programms erscheinende Fenster ist nicht maximiert⁴¹ und besteht aus fünf Elementen (siehe Abbildung 5):

- Die Multifunktionsleiste (auch *Ribbon* genannt) befindet sich im Kopfbereich des Fensters.
- Ein Fenster mit der Überschrift *Algorithms*⁴² findet sich auf der linken Seite, hier können die einzelnen Algorithmen ausgewählt werden.
- Ein Fenster mit der Überschrift *Algorithm Settings* ist auf der rechten Seite,
- das Logbuch (*Messages*) im unteren Bildschirmbereich sowie
- der eigentlichen Workspace zur visuellen Programmierung in der Mitte. Beim ersten Programmstart ist hier die Beispieldatei „AES-Sample-01.cte“ geöffnet.

⁴¹ Zumindest auf meinem Laptop mit WXGA Auflösung.

⁴² In Microsoft Outlook wird dieses Fenster *Navigation pane* oder auch *Navigationsfenster* genannt.

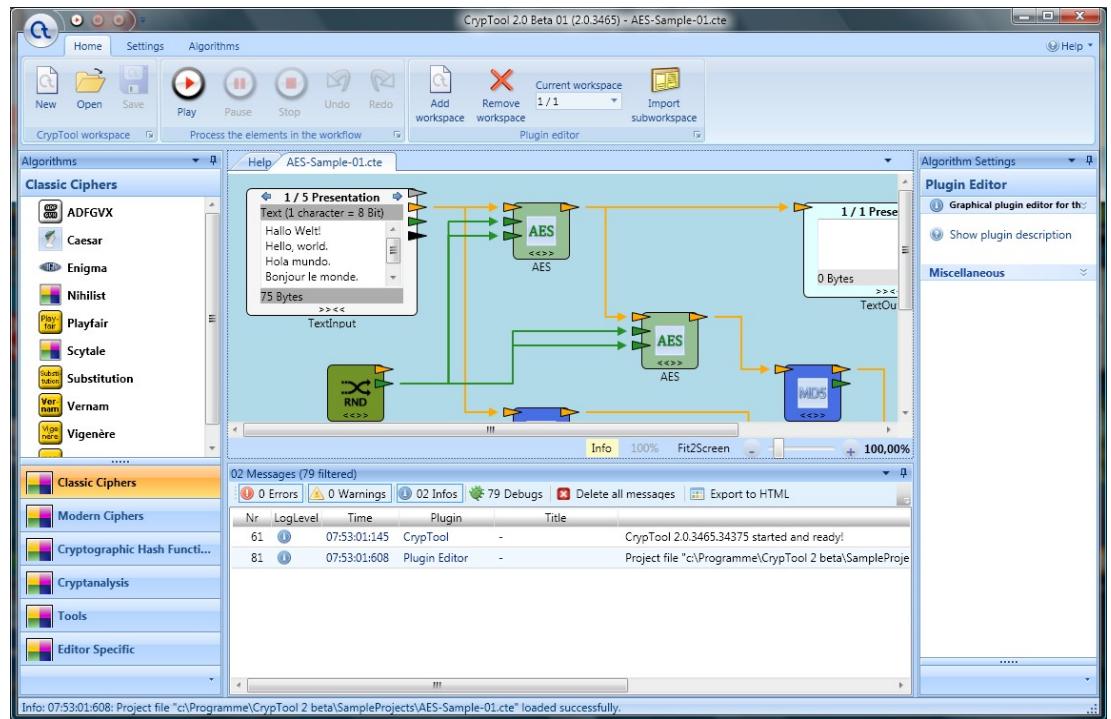


Abbildung 5: CrypTool 2 nach dem Programmstart

Der prinzipielle Aufbau von CrypTool 2 soll an ein typisches Office Programm (wie beispielsweise Word) erinnern, es können Dokumente (visuelle Programme) erstellt, bearbeitet, gespeichert (als CTE-Dateien) und wieder geöffnet werden.

Das eigentliche Dokument befindet sich im CrypTool Editor Plugin in der Mitte des Fensters. In Anbetracht der Aufgabe bzw. auch der Bedeutung des Workspaces zur visuellen Programmierung ist der ihm zugemessene Platz deutlich zu klein. Es können nicht einmal einfache visuelle Programme erstellt werden, ohne die Ansicht zu verkleinern oder sowohl horizontal als auch horizontal scrollen zu müssen. Dadurch werden die Vorteile der visuellen Programmierung⁴³ zunichte gemacht.

4.2.1. Die Multifunktionsleiste *Ribbon*

Die Multifunktionsleiste ist ein noch recht junges Bedienelement. Sie wurde von Microsoft mit der Veröffentlichung von Office 2007 eingeführt und ersetzt sowohl die Menü- als auch die Symbolleiste. Um als Programmierer eine zu Office 2007 ähnliche Oberfläche verwenden zu dürfen, hat Microsoft die *2007 Microsoft Office System User Interface Design Guidelines* ([MS officeui]) veröffentlicht, die nach

⁴³ Wie beispielsweise das leichtere Erfassen komplexer Zusammenhänge und Abläufe.

einer Registrierung kostenlos abgerufen und lizenziert werden kann. Hierbei müssen verschiedene Elemente beachtet und implementiert werden, für andere gibt es Empfehlungen. Die wichtigsten dieser Elemente sind die Multifunktionsleiste mit ihren Registerkarten und Gruppen sowie das Anwendungs-Menü und die Schnellzugriffsleiste in der oberen linken Bildschirmecke bzw. in der Fenstertitelleiste.

Sowohl den meisten Probanden als auch mir selbst war die Multifunktionsleiste aus Office 2007 bisher nicht bekannt. Um den Workspace zu maximieren, bat ich die Probanden, die F11-Taste zu drücken. Dabei wird, anders als bei Word 2007, die Multifunktionsleiste ausgeblendet und kann daher von den Probanden nicht mehr beurteilt werden.

Generell sehe ich bei der Verwendung der Multifunktionsleiste keine Probleme, solange sie intuitiv und konsistent ist. Spezielle Funktionen, die von Office-Anwendungen her nicht bekannt sind, müssen aber leicht verständlich und einfach zu bedienen sein. Hier können sogenannte *ScreenTips* nützlich sein. Gemäß der 2007 *Microsoft Office System User Interface Design Guidelines* ([MS officeui])⁴⁴ sollen sie helfen, Lücken zwischen Benutzeroberfläche und Hilfesystem zu schließen. Die bisher in CrypTool 2 implementierten einzeiligen Tooltips bestehen nur aus wenigen Worten, die zwar häufig einen Anhaltspunkt über die Funktionsweise eines Bedienelementes geben, aber gerade für Anfänger nicht sonderlich hilfreich sind. Außerdem sind sie nach 2007 *Microsoft Office System User Interface Design Guidelines* lediglich bei reduzierter Breite des Hauptfensters für die Tabs der Multifunktionsleiste vorgesehen.

Bei der Umsetzung der 2007 *Microsoft Office System User Interface Design Guidelines* sollten noch zwei Details nachgebessert werden. Zum einen habe ich mich beim Erstellen des Arbeitsblatts gefragt, welche Bedeutung die in jeder Gruppe der Multifunktionsleiste vorhandenen *Dialog Box Launcher* (siehe Abbildung 6) haben, die sie sich zwar aktivieren und anklicken lassen, aber offensichtlich keine Funktion haben. Die Verwendung „blinder“, also funktionsloser *Dialog Box*

⁴⁴ S. 115, ScreenTips als optionales Element.

Launcher ist nach *2007 Microsoft Office System User Interface Design Guidelines*⁴⁵ zwar nicht explizit verboten, sie verwirren den Benutzer jedoch und sind auch nicht empfohlen.

Zum anderen sollten bei reduzierter Fensterbreite die verschiedenen Gruppen der Multifunktionsleiste als Symbol kollabiert dargestellt werden. Bei CrypTool 2 wird allerdings lediglich ein leeres Feld angezeigt, ein Symbol, das die angebotenen Funktionen anschaulich machen könnte, fehlt.



Abbildung 6: Dialog Box Launcher
der Multifunktionsleiste



Abbildung 7:
Symbol einer
kollabierten Gruppe

Weitere didaktisch sinnvoll verwendbare Möglichkeiten der *2007 Microsoft Office System User Interface Design Guidelines* sind *Contextual Tabs* sowie die *Mini Toolbar*. Darauf werde ich in *Die Darstellung der Algorithmen* (4.2.6) näher eingehen.

Betrachtet man die aktuell in CrypTool 2 verwendete Multifunktionsleiste, so finden sich darin zur Zeit drei Registerkarten⁴⁶: *Home*, *Settings* und *Algorithms*. Sie beinhalten einige Elemente, deren Bedeutung nicht ohne genauere Kenntnis der Programminternen erschlossen werden können.

Unter *Home* finden sich Bedienelemente zum Laden und Speichern von visuellen Programmen sowie zum Starten und Anhalten der dargestellten visuellen Ablaufketten. Darüber hinaus gibt die Möglichkeit, Workspaces hinzuzufügen, zu löschen bzw. zwischen mehreren umzuschalten.

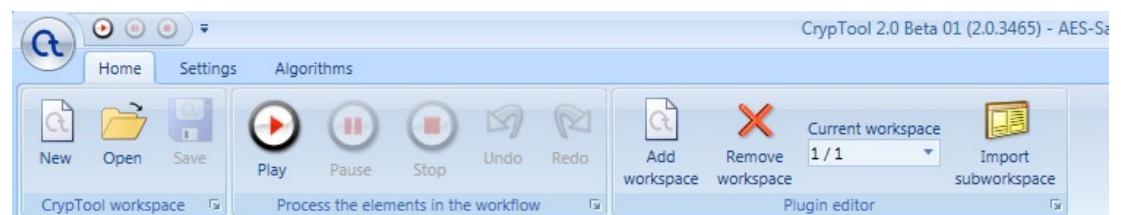


Abbildung 8: Multifunktionsleiste, Registerkarte Home

45 S. 26: „Dialog Box Launchers are NOT REQUIRED for every group.“

46 Auch *Tab* genannt.

Bei meiner ersten Begegnung mit CrypTool 2 war mir zunächst unklar, was mit den Funktionen *Öffnen* und *Speichern* bezweckt werden soll. Erst als ich verstanden hatte, dass im Gegensatz zu CrypTool 1.4.30 nicht einfach Algorithmen angewendet werden können, sondern dass man zuvor ein visuelles Programm gestalten muss, war auch klar, dass eben dieses visuelle Programm geöffnet und gespeichert werden kann.

Gleiches gilt für die Prozesskontrolle mittels der *Play*, *Pause* und *Stop* Symbole sowie *Undo* und *Redo*. Fast alle Probanden hatten Probleme mit dem in der *Diplomarbeit zum Editor für CrypTool 2* ([Schmid]) beschriebenen *Play-Mode* des CrypTool Editors. So kam es häufig vor, dass vergessen wurde, das *Start*-Symbol zu drücken und das visuelle Programm also auch nicht startete. Aber auch umgekehrt kann zwar der Text in den Textfeldern während des *Play-Modes* geändert werden, aber nicht die Einstellungen der Algorithmen, was ebenfalls für viele Probanden ein Stolperstein war.

Aus späterer Sicht fehlen mir hier die Standardfunktionen *Ausschneiden*, *Kopieren* und *Einfügen*. Zwar kann man statt ein Icon eines Algorithmus *auszuschneiden* und anschließend wieder *einzufügen* dieses auch leicht *verschieben*, eine Funktion zum *kopieren* eines Algorithmus fehlt jedoch. Es wäre außerdem sinnvoll, wenn diese Kopierfunktion die Einstellungen des Plugins gleich mitkopieren würde.

Nicht in der Aufgabenstellung für die Probanden verwendet habe ich Funktionen der Gruppe *Plugin Editor*. Hier können zusätzliche Workspaces hinzugefügt, ausgewählt bzw. wieder gelöscht werden. Diese Funktionen mögen für komplexere Anwendungen nützlich sein, doch mir fällt keine sinnvolle Anwendung dazu ein. Wesentlich interessanter dagegen finde ich die Idee, sogenannte *Sub-Workspaces* zu integrieren. Ein Sub-Workspace kann als „normales Icon“ in den Haupt-Workspace eingebaut werden, besteht aber seinerseits aus einem eigenen visuellen Programm. Ein solcher Sub-Workspace ist quasi ein visuelles Unterprogramm. Dieses kann einen Teil der Komplexität des Haupt-Workspace aufnehmen und dadurch dessen Übersichtlichkeit erhöhen. Es ist auch möglich, so erstellte Sub-Workspaces mehrfach in den Haupt-Workspace zu integrieren. Allerdings ist das Speichern und Laden von Sub-Workspaces noch nicht möglich. Die Funktion zum Speichern ist

sehr versteckt⁴⁷, es kann kein Dateiname eingegeben werden und es kommt zu Fehlermeldungen im Logbuch. Beim Importieren von Sub-Workspaces über die Schaltfläche in der Multifunktionsleiste kommt es ebenfalls zu Fehlermeldungen. Diese sinnvolle Funktion bedarf daher einer Fehlerbeseitigung und verbesserten Zugänglichkeit der *Speichern*-Funktion, z.B. in der Multifunktionsleiste neben dem *Import*-Symbol. In Anbetracht der Möglichkeiten, die dadurch eröffnet werden, wäre es schön, wenn sich Sub-Workspaces ebenso einfach wie der normale Workspace öffnen, bearbeiten und speichern ließen.

Unter der Registerkarte *Settings* lassen sich neue Plugins laden sowie der Umfang der angezeigten Ein- und Ausgänge der verwendeten Plugins mittels des *Detail level*⁴⁸ festlegen.

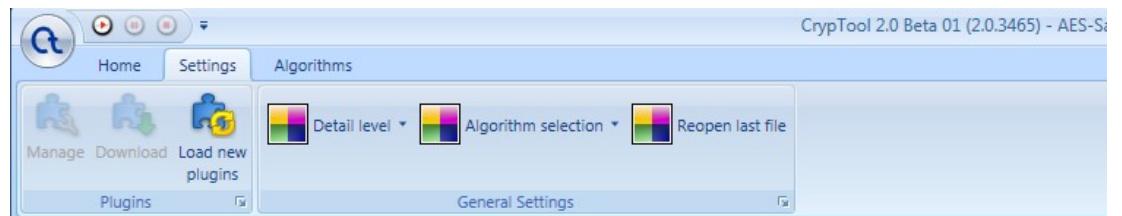


Abbildung 9: Multifunktionsleiste, Registerkarte Settings

Die Funktionen *Manage* und *Download* sind noch nicht implementiert, daher sind die Symbole deaktiviert dargestellt. *Load new plugins* sucht nach neuen Plugins im Pluginverzeichnis von CrypTool und lädt diese.

Diese Abstufung in verschiedene *Detail level* dient zwar der Steigerung der Übersichtlichkeit eines visuellen Programms, doch die Bezeichnungen *Beginner*, *Experienced*, *Professional* und *Expert* legen einen Zusammenhang zu den Vorerfahrungen der Nutzer nahe, der in keiner Weise gegeben ist. Die Schwierigkeiten, die ein Anfänger mit CrypTool 2 hat, sind nicht durch die Wahl des *Display levels Beginner* zu beheben, hier bedarf es ganz anderer Hilfestellungen. Auf der anderen Seite möchte auch ein erfahrener Nutzer manchmal nicht alle Eingänge der Plugins sehen. Daher möchte ich die Umbenennung der einzelnen *Detail level* in sinnvollere Bezeichnungen wie *einfach*, *reduziert*, *normal* und *erweitert* anregen.

47 Man muss auf eine leere Stelle im Workspace mit der rechten Maustaste klicken.

48 Vgl. Abschnitt 2.4.1. Diplomarbeit zum Editor für CrypTool 2.

Unter *Algorithm selection* kann man den Anzeigeort der Algorithmen (Fenster am linken Bildschirmrand bzw. in der Multifunktionsleiste) auswählen; das Symbol für *Reopen last file* ist funktionslos.

Schließlich stehen unter der (abschaltbaren) Registerkarte *Algorithms* dieselben Algorithmen wie im *Algorithms*-Fenster am linken Bildschirmrand zur Auswahl. Wählt man einen Algorithmus aus, so wird sein Icon im Workspace eingefügt.



Abbildung 10: Multifunktionsleiste, Registerkarte Algorithms

Im Gegensatz zum *Algorithms*-Fenster wirkt die Darstellung in der Multifunktionsleiste sehr unübersichtlich. Irritierend finde ich auch die doppelte Auswahlmöglichkeit der Plugins. Daher möchte ich die ersatzlose Streichung dieser Registerkarte vorschlagen.

4.2.2. Das Navigationsfenster *Algorithms*



Abbildung 11: Das Navigationsfenster

Die zweite, übersichtlichere Möglichkeit, Algorithmen auszuwählen und in den Workspace einzufügen, ist das Navigationsfenster am linken Bildschirmrand. Das Design dieses Fensters ist an Microsoft Outlook angelehnt. Hier finden sich in den verschiedenen Kategorien die zugehörigen Algorithmen. Unter *Tools* sind verschiedene nicht kryptographische Hilfsmittel aufgeführt und die Bausteine, die bei einem Sub-Workspace benötigt werden, sind unter *Editor Specific* zusammengefasst.

Ein Proband hatte zunächst Schwierigkeiten mit diesem Fenster, da es für ihn ungewohnt war, dass sich die Auswahl der Kategorien unter dem Fenster mit den Einträgen befindet. Zum Teil möchte ich ihm zustimmen, doch da es weit verbreitete Programme aus dem Hause Microsoft genauso handhaben, werden die meisten

Anwender hier jedoch problemlos zurechtkommen. Gleiches gilt für die Möglichkeiten, das Fenster schwebend anzuordnen oder einzelne Kategorien vor dem Benutzer zu verbergen.

Schön ist, dass die Algorithmen durch individuelle, leicht wiederzuerkennende Symbole repräsentiert werden. In einer neueren Version von CrypTool 2 wurden auch die Symbole vor den verschiedenen Kategorien überarbeitet.

4.2.3. Das Fenster *Algorithm Settings*

Möchte man die Einstellungen eines auf dem Workspace abgelegten Algorithmus ändern, so erledigt man dies im Fenster *Algorithm Settings* am rechten Bildschirmrand. In Abbildung 12 ist das Konfigurationsfenster für den Plugin Editor⁴⁹ zu sehen, also des Moduls, das die visuelle Programmierung ermöglicht. Der prinzipielle Aufbau ist jedoch auch bei den anderen Plugins der gleiche. Ein Klick auf die dritte Zeile (mit dem vorgestelltem Informationszeichen) offenbart den Autor des Plugins sowie weitere technische Informationen wie den Titel und die Version des Plugins. Der Eintrag *Show plugin description* öffnet (sofern hinterlegt) eine neue Registerkarte, auf der Hintergrundinformationen oder eine kurze Beschreibung⁵⁰ angezeigt werden. Darunter bieten die verschiedenen Plugins ihre Einstellungsmöglichkeiten an. Dies können Zeichencodierungen, Präsentationseinstellungen, eine Behandlung von Sonderfällen, Verschlüsselungsoptionen oder vieles andere mehr sein. Die Anzahl der zur Auswahl angebotenen Optionen soll ebenfalls durch die Einstellung des *Detail levels* in der Multifunktionsleiste⁵¹ beeinflusst werden können, doch dies funktioniert in der aktuellen Programmversion

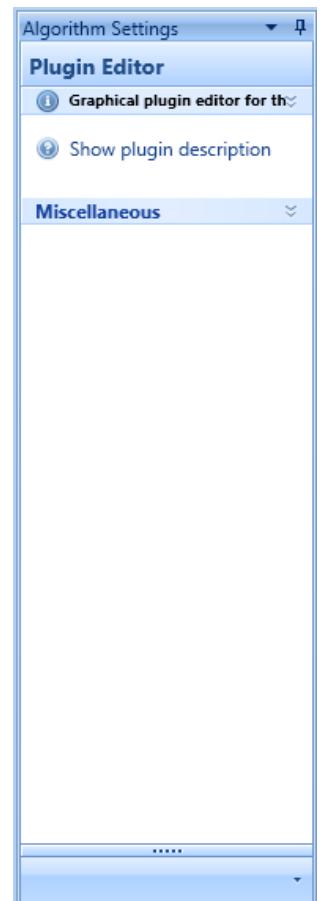


Abbildung 12: Das Konfigurationsfenster

⁴⁹ Vgl. 2.4.1. *Diplomarbeit zum Editor für CrypTool 2*.

⁵⁰ Häufig sind dies Ausschnitte aus entsprechenden Wikipedia-Artikeln oder Verweise darauf.

⁵¹ Siehe 4.2.1. *Die Multifunktionsleiste Ribbon*.

noch nicht richtig. Wird zur Zeit der *Detail level* geändert, so verschwinden alle Einstellungsoptionen und sie lassen sich auch nicht wieder einschalten.

Generell möchte ich aus verschiedenen Gründen dafür plädieren, das Fenster *Algorithm Settings* komplett zu entfernen:

- Es verkleinert den ohnehin knappen den Platz für das visuelle Programm erheblich⁵², auch Thomas Schmid betont den Platzbedarf visueller Programme (vgl. [Schmid]).
- Es überfordert neue Benutzer, die weder wissen, welches die wesentlichen Programmbestandteile von CrypTool 2 sind, noch wo sie eigentlich anfangen sollen. Hier ist in jedem Fall eine lernförderliche Reduktion gemäß des KISS-Prinzips⁵³ nötig.
- Die kontinuierliche Präsenz dieses Konfigurationsfenster ist nicht erforderlich.
- Es ist umständlich und behindert den Workflow, wenn im linken Navigationsfenster ein Modul ausgewählt werden muss, es im mittleren Bildschirmbereich abgelegt und verknüpft wird und schließlich im rechten Konfigurationsfenster eingestellt wird.

Eine alternative Möglichkeit dazu besteht darin, die Konfiguration über ein frei schwebendes Fenster vorzunehmen, das von der Multifunktionsleiste aus aufgerufen werden kann. Weiterhin bieten die *2007 Microsoft Office System User Interface Design Guidelines* ([MS officeui]) die Verwendung von *Contextual Tabs* und *Mini Toolbars* an. Auf diese Ideen werde ich in *Die Darstellung der Algorithmen* (4.2.6.) näher eingehen.

4.2.4. Das Logbuch (*Messages*)

Am unteren Bildschirmrand befindet sich das Logbuch. Hier werden alle Meldungen von CrypTool 2 und sämtlichen Plugins chronologisch protokolliert. Die Meldungen werden nach Wichtigkeit in vier verschiedene Gruppen unterteilt, die

⁵² Siehe auch Abbildung 5.

⁵³ KISS ist ein aus der Informatik stammendes Designprinzip und steht für: Keep it small and simple.

gruppenweise angezeigt bzw. ausgeblendet werden können: *Debugs*, *Infos*, *Warnings* sowie *Errors*. Außerdem kann das Logbuch gespeichert werden.

02 Messages (79 filtered)				
! 0 Errors	! 0 Warnings	! 02 Infos	! 79 Debugs	<input type="checkbox"/> Delete all messages <input type="button" value="Export to HTML"/>
Nr	LogLevel	Time	Plugin	Title
61	!	07:53:01:145	CrypTool	-
81	!	07:53:01:608	Plugin Editor	-

Abbildung 13: Das Logbuch

Ein solches Logbuch ist bei der Softwareentwicklung sehr nützlich und hilft, bei auftretenden Fehlern die Ursache zu finden und abzustellen. Es wundert mich aber, dass die Entwickler von CrypTool 2 dieses Logbuch als derart wichtig erachten, dass es standardmäßig kontinuierlich angezeigt wird. Da ich nach ersten Tests mit einem der ersten Probanden befürchtete, alle weiteren Probanden zu irritieren, kam mir die Funktion, den Workspace durch Drücken der F11-Taste auf Kosten von Multifunktionsleiste, Konfigurationsfenster sowie Logbuch zu maximieren, sehr entgegen und ich empfahl sie daher in meiner Aufgabenstellung.

Mit denselben Argumenten wie beim Konfigurationsfenster plädiere ich auch hier dringend dafür, das Logbuch erst bei Bedarf, das heißt durch Drücken eines entsprechenden Symbols in der Multifunktionsleiste, zu öffnen. Dabei darf es ruhig frei schwebend sein, so dass der Benutzer es individuell dorthin platzieren kann, wo es keine wichtigen Teile des visuellen Programms überdeckt.

Durch das Weglassen der beiden genannten Fenster vergrößert sich der Workspace auf über die doppelte Fläche⁵⁴, womit auch dem in der Diplomarbeit zum Editor für CrypTool 2 ([Schmid]) thematisierten Platzbedarf eines visuellen Programmes Rechnung getragen wird. Aus didaktischer Sicht bekommt der Workspace damit den Raum (und auch die Beachtung des Benutzers), der ihm als dem Hauptelement von CrypTool 2 zusteht, denn hier sollen Anwender eigene Ideen entwickeln, arbeiten und gleichzeitig den Überblick behalten.

54 Bei dem Startbildschirm sind es 225%, vergleiche Abbildung 5.

Eine Möglichkeit, Fehlermeldungen hilfreich und dezentral darzustellen werde ich in *Der Workspace zur visuellen Programmierung* (4.2.5) vorstellen.

4.2.5. Der *Workspace* zur visuellen Programmierung

Wie zuvor⁵⁵ erwähnt, hatten die meisten Probanden Schwierigkeiten mit dem *Play-Mode* des CrypTool-Editors⁵⁶. Dies wird zum Teil auch daran liegen, dass keine Informatiker in der Probandengruppe waren, denn für diese dürfte es intuitiver sein, ein Programm starten zu müssen. Leider verstehe ich zu wenig von den zugrunde liegenden konstruktionsbedingten Details und programmiertechnischen Möglichkeiten, doch frage ich mich, ob der Play-Mode in dieser Form sein muss.

Natürlich benötigt ein „komplexes“ Programm (mit Schleife oder anderen rekursiven Elementen) einen Befehl zum Starten. Bei dem Wunsch auf den *Play-Mode* zu verzichten denke ich vor allem an einfache, sequenzielle Abläufe wie beispielsweise das Ver- (oder Ent-)schlüsseln eines Textes mit Hilfe eines ausgewählten Algorithmus und eines eingegebenen Passworts. Immer, wenn ein Parameter (Text, Optionen oder Passwort) geändert wird, müsste der Algorithmus dann automatisch neu starten. Möglicherweise lässt sich eine Funktion integrieren, die bei Verwendung der ersten Rekursion die automatische Ausführung stoppt, dabei eine Informationsmeldung ausgibt und auf das manuelle Starten des Programms mittels *Start*-Symbol wartet.

Ein weiterer Wunsch, der aus den Rückmeldungen der Probanden zu erkennen ist, ist, dass der Play-Mode nach dem Terminieren des Programms automatisch wieder beendet wird. Dadurch entfällt der Schritt, zunächst das *Stop*-Symbol drücken zu müssen, um eine Änderung durchzuführen. Außerdem entspricht dies auch der Vorerfahrung all jener, die schon einmal in einer Programmiersprache programmiert haben, auch hier beendet sich das Programm von selbst, wenn der Programmcode abgearbeitet ist und wartet nicht etwa noch zusätzlich auf einen Stop-Befehl.

Auch wenn es aus Sicht eines unerfahrenen Anwenders nicht klar ist, so werden bei

⁵⁵ Unter 4.2.1. *Die Multifunktionsleiste Ribbon*.

⁵⁶ Siehe 2.4.1. *Diplomarbeit zum Editor für CrypTool 2*.

der Programmierung verschiedene Datentypen⁵⁷ benötigt. In CrypTool 2 werden die verwendeten Datentypen durch farblich gekennzeichnete „Anschlüsse“ an den Symbolen der Algorithmen auf dem Workspace markiert. In meinem Arbeitsauftrag für die Probanden war eine Konstruktionsaufgabe zu lösen, bei der unter anderem verschiedene Datentypen vorkamen. Dabei stellte sich heraus, dass die farbliche Kennzeichnung sehr hilfreich war und die „passenden“ Verbindungen ganz intuitiv hergestellt werden konnten. Umso interessanter fand ich bei Nachfragen, dass den Probanden noch nicht einmal bewusst war, dass sie es mit Datentypen zu tun hatten. Dennoch möchte ich einen Verbesserungsvorschlag unterbreiten: Verschiedene Plugins unterstützen mehrere Datentypen, der jeweils zu verwendende Datentyp lässt sich in den Einstellungen des Plugins auswählen. Auf der Suche nach einem passenden Ausgabe-Plugin hatte ich nicht an die Möglichkeit der Auswahl des Datentyps gedacht und wunderte mich, warum nur ein Plugin zur Ausgabe von Stream-Daten existierte und keines für Text-Daten. Ein anderes Beispiel ist das TextInput-Plugin, das vier verschiedene Ausgänge hat, für jeden unterstützten Datentyp einen. Hier wäre eine einfachere Handhabung wünschenswert. Es sollten alle unterstützten Datentypen mit Hilfe einer automatischen Erkennung an nur einem Ein- bzw. Ausgang angenommen werden können. Ein solcher „Multi-Datentyp-Ein- oder Ausgang“ sollte schwarz (wie bei TunnelInput und TunnelOutput von Sub-Workspaces), mehrfarbig (z.B. mit den akzeptierten Farben) oder transparent gestaltet sein, so dass seine Fähigkeiten gleich zu erkennen sind.

Eine weitere Anregung betrifft die visuelle Gestaltung der Datenkanäle. Gut und intuitiv ist, dass die Eingänge der Plugins links angeordnet sind und die Ausgänge rechts. Ich fände es begrüßenswert, wenn statt des einstellbaren *Detail levels* (oder auch zusätzlich dazu) die obligatorischen Kanäle eines Plugins von den fakultativen visuell unterschieden werden könnten. Von mir bevorzugt ist eine etwas vergrößerte Darstellung der „Pflichteingänge“, während die fakultativen Eingänge etwas kleiner dargestellt werden sollten. Damit ist die jeweilige Bedeutung eines Kanals intuitiv und leichter zu erfassen.

Der beim Überfahren von Ein- bzw. Ausgängen angezeigte *Tooltip*, eine kurze Erklärung, ist sehr kurz und technisch gehalten. Sollen auch vermehrt Anfänger mit

57 Beispiele für Datentypen: *Ganzzahl, einzelnes Zeichen, Stream, Block-Text, Wahrheitswerte etc. .*

CrypTool 2 arbeiten, wären leichter verständliche Hinweise wünschenswert.

Die Linien, die einen Ausgang des einen Plugins mit einem Eingang eines anderen verbinden, sind eine leicht verständliche Darstellung der logischen Verknüpfung. Leider ist nicht immer ganz eindeutig, wo Verbindungen bestehen und wo sich Linien ohne Verbindung lediglich überschneiden. In Abbildung 14 kann man diese mit etwas Erfahrung zwar noch unterscheiden, doch lassen sich ohne Mühe beliebig unklare Beispiele konstruieren. Daher möchte ich einen Vorschlag zur Verbesserung machen, der einer elektrischen Schaltskizze nachempfunden ist. Abzweigungen und verbundene Linien sollten mit einem Punkt gekennzeichnet werden, während bei unverbundenen Kreuzungen ein Bogen den nicht existierenden Kontakt verdeutlicht (siehe Abbildung 15).

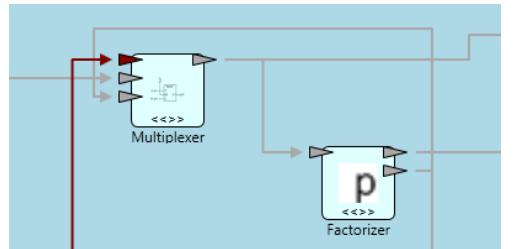


Abbildung 14: Unklare Verbindungen in Factorisation-Sample.cte

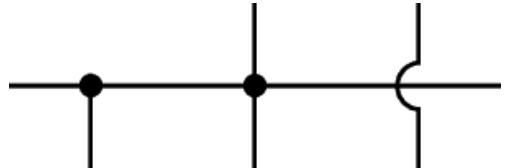


Abbildung 15: Vorschlag für klarere Abzweigungen und Kreuzungen

Ein weiterer Fall von unklaren Verbindungen liegt vor, wenn die Linien über (oder unter) anderen Symbolen verlaufen. Da die Linien automatisch berechnet und gezeichnet werden, der Benutzer also keinen Einfluss auf den Verlauf hat, müsste hier der Algorithmus zur automatischen Linienberechnung und -zeichnung nachgebessert werden. Beide Probleme sind mir, vor allem bei platzeffizienter Anordnung der Symbole, immer wieder begegnet und ich musste daher zur besseren Nachvollziehbarkeit immer wieder den Aufbau des visuellen Programms ändern.

Wird ein visuelles Programm ausgeführt, so färbt sich der Hintergrund des Symbols des jeweiligen Plugins in Abhängigkeit von auftretenden Fehlern oder Warnungen grün, gelb oder rot. Die entsprechende Fehlermeldung erscheint allerdings nur im Logbuch. Ist das Logbuch (z.B. aus Platzgründen) ausgeblendet, so muss dieses erst wieder geöffnet werden. Werden mehrere Algorithmen mit demselben Namen verwendet, so erschwert sich außerdem die Zuordnung des Fehlers, da diese nicht unterschieden werden können. Daher wäre es hilfreich, wenn

das betroffene Symbol auf dem Workspace, also am „Ort des Geschehens“, bei Fehlern und Warnungen ebenfalls die Meldung ausgeben würde. Als Form finde ich eine comicartige Sprechblase geeignet, da so der Ort des Fehlers exakt zu bestimmen ist und das Element „Sprechblase“ den meisten Nutzern als angebotene Hilfestellung des „Hilfe-Assistenten“ von Microsoft Office vertraut sein dürfte.

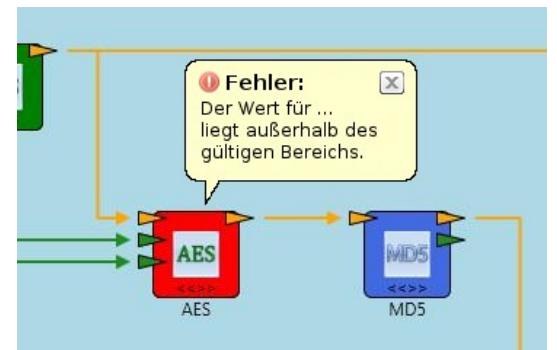


Abbildung 16: Vorschlag für eine lokale Fehlermeldung im visuellen Programm

Der CrypTool Editor bietet Unterstützung für mehrere Workspaces mit jeweils mehreren Registerkarten (auch Tabs genannt). Den Nutzen multipler Workspaces habe ich bereits in *Die Multifunktionsleiste Ribbon* (4.2.1) in Frage gestellt, doch das Konzept der Tabs erscheint mir zeitgemäß und intuitiv zu bedienen. Der CrypTool Editor ist in der Handhabung von Registerkarten allerdings noch sehr schwerfällig. Möchte man ein neues Projekt öffnen, so wird das gerade verwendete (inklusive aller weiteren geöffneten Tabs) zwangsweise beendet. Die Verwendung der rechten Maustaste ist inkonsistent: Manche Kontextmenüs bieten eine Option zum Schließen des Tabs, andere nicht. Andere Registerkarten bieten die *Schließen*-Funktion zusätzlich am rechten Rand der Workspace Kopfzeile an⁵⁸, wieder andere sind gar nicht zu schließen⁵⁹. Hier wünsche ich mir eine konsistente und einfache Bedienung: Ein Tab sollte als ein Dokument betrachtet werden. Öffnet oder lädt man ein neues Dokument, so wird einfach ein neuer, in der Größe anpassbarer Tab hinzugefügt. Die einzelnen Dokumente sollten unabhängig voneinander geöffnet, gespeichert oder geschlossen werden können, hier bietet sich außerdem die konsequente Verwendung eines *Schließen*-Symbols an, das auf jeder Registerkarte angezeigt wird. Dadurch erhält der Benutzer die Kontrolle über seine Dokumente. Als Vergleich und Vorbild möchte ich die Verwendung von Registerkarten in modernen Internetbrowsern

⁵⁸ Z.B. die Plugin Beschreibungen (*Description*).

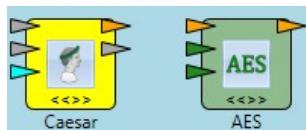
⁵⁹ Z.B. der Tab *Help*.

anführen, die den Benutzern vertraut⁶⁰ ist. Daher erleichtert auch eine ähnliche Implementierung in CrypTool 2 dessen Bedienbarkeit.

Eine weitere, aus Office-Programmen bekannte, Funktion ist die Möglichkeit der Skalierung der Darstellungsgröße. Durch die in CrypTool 2 eingeblendeten Fenster *Algorithm Settings* und *Logbuch* sind die Elemente zur Ansichtssteuerung jedoch nicht am gewohnten Platz, auf der rechten Seite der Statuszeile, sondern in der Mitte des Bildschirms, unterhalb des Workspaces zu finden⁶¹. Da beide Fenster nicht nötig sind und entfernt werden sollten⁶², können diese Kontrollelemente wieder an den gewohnten Ort in der Statusleiste zurückkehren (vgl. [MS officeui], S. 78). Dies erleichtert die intuitive Bedienbarkeit und vergrößert erneut den Workspace.

Eine große Erleichterung, gerade für Einsteiger, könnte die Möglichkeit bieten, Bilder, Texte und Verweise in den Workspace einzufügen. Beispielsweise ließe sich so bei einem modernen Verschlüsselungsverfahren auf einfache Weise darstellen, welche Vorgänge auf den Rechnern der beiden Kommunikationspartner ablaufen und welche Daten durch das „unsichere Medium“ ausgetauscht würden. So könnte zusätzlich zum visuellen Programm eine Strukturierungshilfe für den Anwender geschaffen werden. Auch wäre die Verwendung von motivierenden Graphiken, sei es für die Charaktere Alice und Bob, die die Standardrollen in der Kryptographie symbolisieren (vgl. [WP:AliceBob]) oder aber für historische Details wie die verwendeten Chiffrier-Werkzeuge aus didaktischer Sicht sinnvoll⁶³.

4.2.6. Die Darstellung der Algorithmen



*Abbildung 17:
Beispiele für Symbole
von Algorithmen*

Auf dem Workspace zur visuellen Programmierung werden die abgelegten Algorithmen durch Symbole dargestellt. Dadurch sind sie schnell zu erfassen und leicht wiederzuerkennen. Die Hintergrundfarbe zeigt die Zugehörigkeit zu einer Algorithmengruppe. So bedeutet ein gelber Hintergrund beispielsweise, dass es sich um ein

60 Der Internetbrowser wird, auch bei den Probanden, häufiger genutzt als ein Office-Programm.

61 Siehe Abbildung 5.

62 Vgl. 4.2.3. Das Fenster Algorithm Settings und 4.2.4. Das Logbuch (Messages).

63 Ein Beispiel hierfür ist in Abbildung 34 dargestellt.

klassisches Verfahren handelt, Grün steht für moderne kryptographische Algorithmen, Blau für Hashfunktionen und so fort. Wird das visuelle Programm gestartet, so ändert sich bei den angeschlossenen Plugins die Farbe in Abhängigkeit von Ausführungsfehlern in Rot, Gelb oder Grün, so dass ein Fehler oder eine Warnung daran direkt erkannt und dem richtigen Plugin zugeordnet werden kann. Zusätzlich werden diese Fehler, Warnungen und Meldungen im Logbuch angezeigt. Auf der linken Seite des Symbols befinden sich die Eingänge des Plugins, auf der rechten die Ausgänge. Die Farben der Ein- und Ausgänge repräsentieren verschiedene Datentypen⁶⁴ und beim Überfahren mit der Maus wird ein *Tooltip* angezeigt, also eine Kurzbeschreibung, wofür der Kanal verwendet wird. Der Name des Algorithmus steht unterhalb des Symbols und lässt sich leicht ändern. Die spitzen Klammern „<>“ sollen andeuten, dass sich das Symbol vergrößern lässt, falls man darauf klickt. Diese vergrößerte Ansicht nennt sich *QuickWatch* und erlaubt, die an den einzelnen Kanälen anliegenden Daten (z.B. zur Fehlersuche) oder aber eine in dieses Plugin integrierte Präsentation anzuzeigen. Mit den Pfeilen in der Kopfzeile können die verschiedenen Anzeigen umgeschaltet werden. Die spitzen Klammern kehren sich um „><“ und sollen andeuten, dass das Plugin wieder als Symbol verkleinert angezeigt werden kann. Außerdem bieten die einzelnen Plugins über das Fenster *Algorithm settings* Einstellmöglichkeiten sowie eine Beschreibung des Plugins an, die sich in einer neuen Registerkarte öffnet.

Die Symbole der Algorithmen sind gelungen und einer schnellen Orientierung sehr dienlich. Den Vorteil, den das Erkennen der Algorithmengruppe anhand der Hintergrundfarbe bringt, sehe ich nicht, allerdings schadet es auch nicht. Zu den Aspekten Fehlermeldungen sowie Ein- und Ausgänge habe ich mich bereits geäußert⁶⁵.

Zur Zeit gibt es drei verschiedene Aspekte, die zu jedem Plugin verfügbar sein sollten: Die Einstellungen, die Beschreibung und die Präsentation. Wird ein Symbol auf dem Workspace mit der linken Maustaste angeklickt und damit markiert, so erscheinen zeitgleich die Einstellungen im rechten Fenster *Algorithm settings*, von wo auch die Plugin-Beschreibung aufgerufen werden kann. Zur Präsentation eines

⁶⁴ Siehe 4.2.5. *Der Workspace zur visuellen Programmierung*.

⁶⁵ Siehe 4.2.5. *Der Workspace zur visuellen Programmierung*.

Plugins gelangt man durch einen Doppelklick⁶⁶ auf sein Symbol. Sowohl die Präsentation als auch die Beschreibung werden in einer eigenen Registerkarte angezeigt.

Wie zuvor ausgeführt⁶⁷, möchte ich das Fenster *Algorithm settings* entfernen. Dabei bietet sich die Gelegenheit, die Bedienung der Algorithmen auf dem Workspace zu überdenken. Der Benutzer soll einfach, schnell und intuitiv seine Vorhaben umsetzen können. Dabei spielen individuelle Voraussetzungen eine große Rolle, die hier nicht erfasst werden können. Doch es gibt einen „kleinsten gemeinsamen Nenner“, nämlich die Gepflogenheiten des Betriebssystems Windows: Der Benutzer klickt einmalig auf eine Datei, um sie zu markieren; um ihren Inhalt zu betrachten oder zu ändern, öffnet er diese mit einem Doppelklick. Diese Gewohnheit sollte auch CrypTool 2 beachten. Auch daher ist das Fenster *Algorithm settings* nicht zweckmäßig, da es nicht der Intuition entspricht.

Mein erster Gedanke zur Verbesserung war die Verwendung einer *Mini Toolbar*, wie sie in Microsoft Office 2007 eingesetzt wird. Wird ein Text markiert, so erscheint oberhalb der letzten Mausposition eine kleine, freischwebende Werkzeugeiste mit den üblichsten Befehlen. Allerdings ist sie gemäß der 2007 *Microsoft Office System User Interface Design Guidelines* ([MS officeui], S. 107) explizit für Text gedacht und nicht für Symbole. Außerdem ist sie für nur zwei Funktionen auch etwas überdimensioniert.

Ein guter Ansatz zur Verbesserung der Benutzerführung ist die Unterscheidung von „Markieren“ und „Öffnen“ eines Algorithmus. Das *Markieren* eines Symbols fügt der Multifunktionsleiste einen *Contextual Tab*⁶⁸ hinzu, der neben der Beschreibung des Algorithmus noch weitere Funktionen bereitstellen kann⁶⁹. Das durch einen Rechtsklick auf das zugehörige Symbol aufgerufene Kontextmenü eines Algorithmus sollte ebenfalls keine Einstellmöglichkeiten beinhalten, da dies ohnehin nur eine Auswahl sein kann und auf der anderen Seite den Blick auf das Wesentliche verstellt. Hier sind die Funktionen *Öffnen*, *Umbenennen*, *Ausschneiden*, *Kopieren*, *Löschen*

66 Mit der linken Maustaste.

67 In 4.2.3. *Das Fenster Algorithm Settings*.

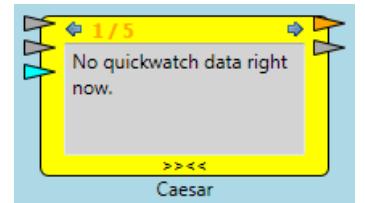
68 Genau wie das Markieren eines Bildes in Microsoft Word 2007 (vgl. [MS officeui], S. 89).

69 Zur weiteren Verwendung dieses *Contextual Tab* siehe 5.3. *Lernebenen*.

sowie *Eigenschaften*⁷⁰ die bessere Wahl, da sie aus der Bedienung von Windows bekannt und gewohnt sind.

Zum *Öffnen* eines Algorithmus könnte sich eine neue, nicht maximierte Registerkarte öffnen, die die Konfiguration des Plugins ermöglicht. Diese hat, abgesehen von ihrem temporären Charakter und einer unmittelbaren visuellen Rückmeldung, die gleichen Nachteile wie das feste Fenster *Algorithm settings*: Sie lenkt die Aufmerksamkeit des Benutzers auf eine neue Bildschirmposition außerhalb des visuellen Programms und unterbricht so den Gedankenfluss.

Als besser empfände ich es daher, wenn durch das *Öffnen* eines Algorithmus die *QuickWatch* Ansicht⁷¹ aktiviert würde. Diese müsste daher überarbeitet und erweitert werden. Die Konfiguration des Algorithmus würde in die *QuickWatch* Ansicht integriert und wäre die Standardansicht. Das *QuickWatch* Fenster ist bereits in seiner Größe änderbar, die Größe nach dem *Öffnen* müsste noch etwas zunehmen, so dass die Einstellmöglichkeiten darin übersichtlich Platz finden. Die Verwendung eines vertikalen Scrollbalkens halte ich hierbei vertretbar, ein horizontaler hingegen sollte vermieden werden. Um weiterhin Zugriff auf die bestehenden Funktionen erhalten zu können, finde ich den Einsatz von entsprechenden und intuitiven Symbolen in der Kopfzeile sinnvoll. Ein weiteres Symbol sollte das Schließen der *QuickWatch* Ansicht ermöglichen, so dass wieder das kleine Symbol des Algorithmus angezeigt wird; die zu diesem Zweck vorhandenen und noch aus der Computer-Steinzeit stammenden spitzen Klammern „><“ würden entfallen. Ein Nebeneffekt dieses Umbaus wäre, dass die Präsentation eines Algorithmus nur noch in der *QuickWatch*-Ansicht vorhanden ist. Da die Präsentation aber lediglich die zur Laufzeit erzeugten Daten visuell ansprechend darstellen soll, halte ich dies für ausreichend. Außerdem kommt es in der gegenwärtigen Implementierung zu Konflikten und Fehlermeldungen, wenn eine Präsentation in der *QuickWatch*-Ansicht angezeigt wird und dann (durch Doppelklick) in einem Fenster geöffnet



⁷⁰ Unter *Eigenschaften* sollten Informationen zum Plugin wie Autor, Version, Art des Algorithmus sowie eine Kurzbeschreibung zu finden sein.

⁷¹ Siehe Abbildung 18.

werden soll. Diese Probleme würden somit ebenfalls entfallen.

In Abbildung 19 habe ich versucht, meine Ideen zur Erweiterung der *QuickWatch*-Ansicht

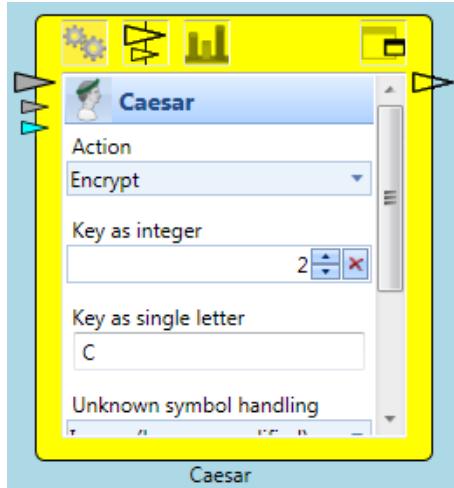


Abbildung 19: Vorschlag zur Erweiterung der QuickWatch-Ansicht.

Ansicht (und die damit verbundene Integration der Einstellungen des Algorithmus) graphisch darzustellen. In der Kopfzeile befinden sich drei Symbole, die Zugriff auf die Einstellungen des Algorithmus (Zahnräder), Anzeige der Werte von Ein- bzw. Ausgängen (Symbol eines Ein-/Ausgangs) sowie die Präsentation (Säulendiagramm) ermöglichen. In der Kopfzeile rechts ist das Symbol zur Verkleinerung der *QuickWatch*-Ansicht zur minimierten Ikone angebracht. Mit diesem Symbol bin ich noch nicht ganz zufrieden, schöner wäre eine Miniaturdarstellung der

Workspace-Ikone, doch hier gelang es mir nicht, ein aussagekräftiges und doch einfaches Piktogramm zu erstellen. Ebenfalls zu erkennen sind die unterschiedlich großen Ein- bzw. Ausgänge⁷² und der transparent gestaltete „Multi-Datentyp-Ausgang“ (rechts)⁷³. Da der Name des Plugins (beliebig) geändert werden kann, der Nutzer aber immer wissen sollte, welchen Algorithmus er konfiguriert, halte ich die Integration des ursprünglichen Plugin-Namens und dessen Symbols in der *QuickWatch*-Ansicht für unverzichtbar („Überschrift“ unter der Kopfzeile). Den Konfigurationsdialog habe ich unverändert hineinmontiert.

Die Beschreibung eines Plugins ist gegenwärtig ebenfalls über das Fenster *Algorithm settings* zu erreichen⁷⁴ und wird in einer eigenen Registerkarte auf dem Workspace geöffnet. Häufig sind Verweise auf Wikipedia integriert, meines Erachtens bleibt aber vielfach unklar, ob der referenzierte Artikel auf Wikipedia zitiert wird oder ob er zusätzlich als Lektüre empfohlen wird. Auch wenn meine persönliche Einschätzung zur Allgemeinverständlichkeit von Wikipedia-Artikeln

⁷² Die mandatorischen Datenkanäle sind größer dargestellt als die optionalen.

⁷³ Vergleiche 4.2.5. *Der Workspace zur visuellen Programmierung*.

⁷⁴ Eine Alternative dazu stelle in 5.3. *Lernebenen* vor.

eine andere ist, so empfinden die meisten Probanden Wikipedia-Artikel als hilfreich und informativ.

Sehr irritierend und umständlich finde ich die Bedienung der Plugin-Beschreibung

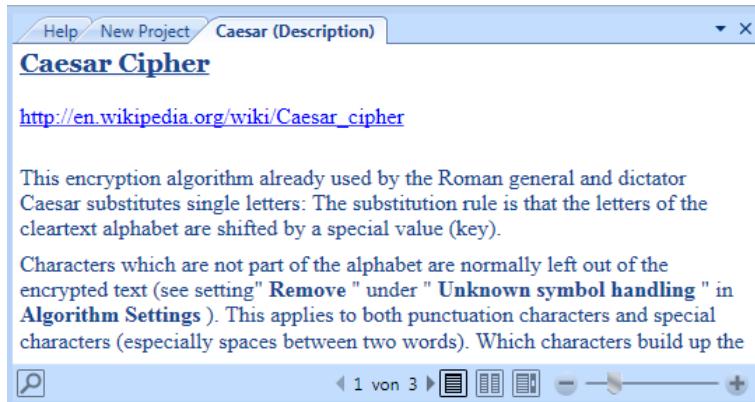


Abbildung 20: Die Plugin-Beschreibung

mit Hilfe der Elemente in der Fußzeile des Tabs (siehe Abbildung 20). Die Suchfunktion (Symbol Lupe) mag nützlich sein, vor allem bei langen Texten⁷⁵, ebenfalls die Möglichkeit, die Größe des Textes zu verändern⁷⁶.

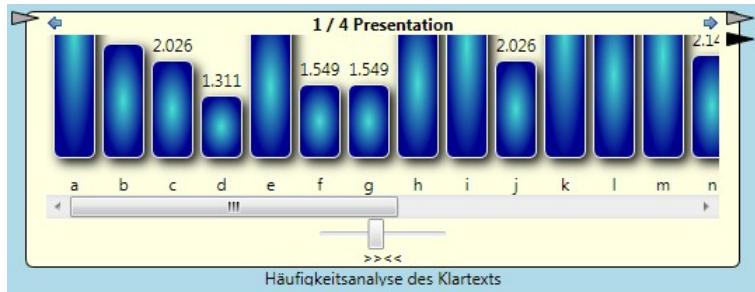
Warum man sich jedoch die Beschreibung in mehreren Spalten anzeigen lassen sollte, liegt jenseits meiner Vorstellungskraft. Die Funktion zur nächsten Seite der Beschreibung weiter zu blättern ist im Vergleich zu einer vertikalen Scrollleiste sehr umständlich zu bedienen und behindert ein zügiges Arbeiten. Der Benutzer eines Internetbrowsers oder eines Textverarbeitungsprogrammes wird ganz intuitiv die Scrollleiste benutzen wollen. Daher ist es empfehlenswert, Suche und Skalierung in die Statusleiste zu verschieben und die Spalten- und Blätterfunktion zugunsten einer Scrollleiste zu entfernen.

Zum Schluss dieses Abschnitts verschiebt sich mein Fokus von den allgemeinen Aspekten der Darstellung von Algorithmen auf die konkrete Implementierung einiger Plugins:

Zwei bestehende Module, der Kasiski-Test und die Häufigkeitsanalyse (Frequency Test), können bisher ihre Auswertung graphisch als Säulendiagramm darstellen. Dies lässt eine Analyse durch den Betrachter auf den ersten Blick zu. Allerdings leiden beide Präsentationen unter einem Schöhnheitsmangel, die Darstellung der Präsentation in der *QuickWatch* - Ansicht muss jedesmal aufs Neue von Hand auf die richtige

75 Die Plugin-Beschreibungen sind meistens jedoch kurz gehalten.

76 Diese Funktion gehört jedoch, wie bereits in 4.2.5. *Der Workspace zur visuellen Programmierung* ausgeführt, in die Statuszeile des Programmfensters.



Größe skaliert werden. Hier wäre eine Funktion, die anhand der Größe der *QuickWatch* - Ansicht automatisch den optimalen Skalierungsfaktor

berechnen und einstellen würde, äußerst hilfreich.

Der Begriff *Präsentation* wird von den Autoren der Plugins von CrypTool 2 sehr unterschiedlich interpretiert und ausgefüllt. Die Ein- bzw. Ausgabeplugins präsentieren ihren Text in einem schmucklosen Textfenster, die beiden oben genannten Plugins zeigen ein Balkendiagramm als Auswertung ihrer Daten an und bei den meisten Plugins ist gar keine Präsentation integriert. Ganz anders das Plugin *PRESENT*. Hier existieren sechs Unter-Karteikarten⁷⁷, mit denen dieser Algorithmus

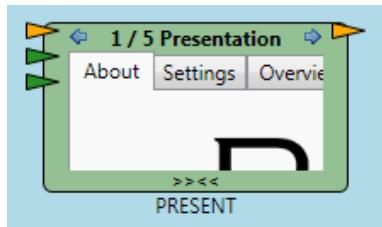


Abbildung 22: Präsentation des Plugins PRESENT in der QuickWatch-Ansicht

vorgestellt werden soll. So erfreulich dies auf der einen Seite ist, so problematisch ist es auch, da hier Gewohnheiten in der Bedienung des Programms gebrochen werden. Zum einen sprengt dieser Umfang die QuickWatch-Ansicht des Algorithmus, für den sie offenbar nicht gemacht ist (siehe Abbildung 22), zum anderen läuft CrypTool 2 hier Gefahr, in der Bedienung und im Leistungsumfang

inkonsistent zu werden. Für ein Lernprogramm ist es enorm wichtig, dass sich der Benutzer, der zunächst einmal kein Fachmann ist, nicht in jedes Plugin neu einarbeiten muss, sondern dass die Bedienung von CrypTool 2 ebenso wie das Lernangebot homogen strukturiert und verlässlich ist.

Ein didaktisches Problem sehe ich bei dem Plugin *Stream Comparator*. Hier werden zwei Datenströme verglichen und das Ergebnis graphisch als Symbol dargestellt. Allerdings ist bei der Ausführung des visuellen Programmes das Symbol auch bei ungleichen Datenströmen grün hinterlegt (siehe Abbildung 23), was mich

⁷⁷ Namentlich Home, Settings, Overview, Key Schedule, Encryption und Trace.



mehrfach irritiert hat. Durch die grüne Farbe soll der CrypTool Editor anzeigen, dass es hier keine technischen Fehler gegeben hat. Besser wäre es jedoch, die technische Fehlerfreiheit wie auch bei anderen Plugins auf den Rahmen des Symbols zu beschränken und den negativen Vergleich deutlicher darzustellen, beispielsweise durch einen roten Hintergrund innerhalb des grünen Rahmens.

Zur Vereinfachung der Handhabung von Ein- und Ausgabeplugins möchte ich anregen, die verschiedenen Input-Plugins⁷⁸ und die verschiedenen Output-Plugins⁷⁹ in jeweils ein universelles Ein- bzw. Ausgabe-Modul zusammenzufassen, das entsprechende Konfigurationsmöglichkeiten bietet. Weiterhin hätte ich beim Erstellen der Arbeitsblätter für die Probanden gerne ein Plugin angewendet, das als Präsentation lediglich die durchgeleiteten Daten anzeigt. Hier wäre ein „normales“ universelles Ausgabe-Modul mit einem zusätzlichen Ausgang hilfreich⁸⁰.

Bezüglich der mathematischen Inhalte und Plugins hat CrypTool 2 leider noch nicht viel zu bieten. Außer einem Primzahltest und einem Faktorisierer⁸¹ sind noch keine mathematischen Plugins implementiert⁸², so dass ich sie auch nicht testen oder näher betrachten kann. Neben den Plugins zu den asymmetrischen Verschlüsselungsverfahren wünsche ich mir insbesondere eine Sammlung von Plugins als mathematische „Basisausstattung“. Hier sind zu nennen ein „Modulo-Rechner“ zum Rechnen mit Restklassen, der zusätzlich zu den Grundrechenarten auch das Potenzieren unterstützt, ein Plugin, das die Eulersche φ -Funktion für große Zahlen⁸³ berechnet sowie ein „Binär-Hex-Dezimal-Wandler“, der eine gegebene Zahl in ein anderes Zahlensystem umrechnet. Zusammen mit den beiden vorhandenen Plugins können so der Euklidsche Algorithmus, der Square-and-Multiply-Algorithmus und der Baby-Step Giant-Step Algorithmus sowie die beiden

⁷⁸ Namentlich: *ClipboardInput*, *FileInput*, *NumberInput* und *TextInput*.

⁷⁹ Namentlich: *ClipboardOutput*, *FileOutput* und *TextOutput*.

⁸⁰ In 5.5. Beispiel: RSA und Abbildung 34 habe ich ein solches Plugin verwendet.

⁸¹ Beide sind leider ohne Einstellmöglichkeiten, ohne Präsentation und ohne Beschreibung.

⁸² Auch die asymmetrischen Verschlüsselungsverfahren oder Protokolle, die auf zahlentheoretischen Problemen basieren, sind leider noch nicht in CrypTool 2 enthalten.

⁸³ Natürlich nur im Rahmen der Rechenleistung des verwendeten Computers.

wichtigsten asymmetrischen Verschlüsselungsverfahren ElGamal und RSA visuell implementiert werden.

4.3. Das Programm Die Welt der Primzahlen

Das Programm *Die Welt der Primzahlen* von Timo Eckhardt (vgl. [Eckhardt]) ist in CrypTool 2 in dem Navigationsfenster unter dem Punkt *Tools* zu finden. Klickt man es an, so öffnet es sich als Registerkarte im Workspace und überdeckt dadurch das gerade bearbeitete Dokument. *Die Welt der Primzahlen* verfügt über eine eigene Kopfzeile⁸⁴ sowie eine ausblendbare Navigation in der linken Spalte, die vier Unterpunkte zeigt:

- Mit der *Faktorisierung* einer Zahl wird diese in ihre Primfaktoren zerlegt. Dazu stehen zwei Methoden zur Verfügung: *Probdivision* und *Das quadratische Sieb*.
- Der Eintrag *Primzahltest* stellt drei verschiedene Verfahren mit diesem Ziel zur Auswahl: *Das Sieb des Eratosthenes*, *den Miller/Rabin-Test* sowie *das Sieb des Atkin*. Außerdem gibt es die Möglichkeit, Primzahlen einer bestimmten Stellenzahl zu generieren oder eigene Formeln zum Erzeugen von Primzahlen auszuprobieren.
- Die *Verteilung der Primzahlen* kann ebenfalls auf unterschiedliche Arten veranschaulicht werden. Hier bietet das Programm die Unterpunkte *Zahlenstrahl*, *Zahlengrid* (eine Art graphische Gitterdarstellung), *Anzahl der Primzahlen* (Eulers Primzahlsatz sowie das logarithmische Integral werden graphisch mit der wirklichen Primzahlanzahl $\pi(n)$ verglichen), *Die Ulam-Spirale*, sowie eine graphische Darstellung zur *Goldbach-Vermutung*.
- Unter dem Punkt *Zahlentheorie* sind drei weitere Darstellungen zusammengefasst. *Potenzieren modulo einer Zahl im Kreis*, *Zahlentheoretische Funktionen* sowie *Primitivwurzeln von Primzahlen*.

In dem Programm selbst sind viele Hilfetexte hinterlegt, die durch Drücken eines der vielen Fragezeichensymbole kontextbezogen aufgerufen werden können.

⁸⁴ Mit den Einträgen *Zurück*, *Vorwärts*, *Optionen* und *Navigation ausblenden*.

Darüber hinaus sind vielfach Links auf Internetseiten der deutschsprachigen Wikipedia vorhanden, die zu den einzelnen Sachverhalten Auskunft geben.

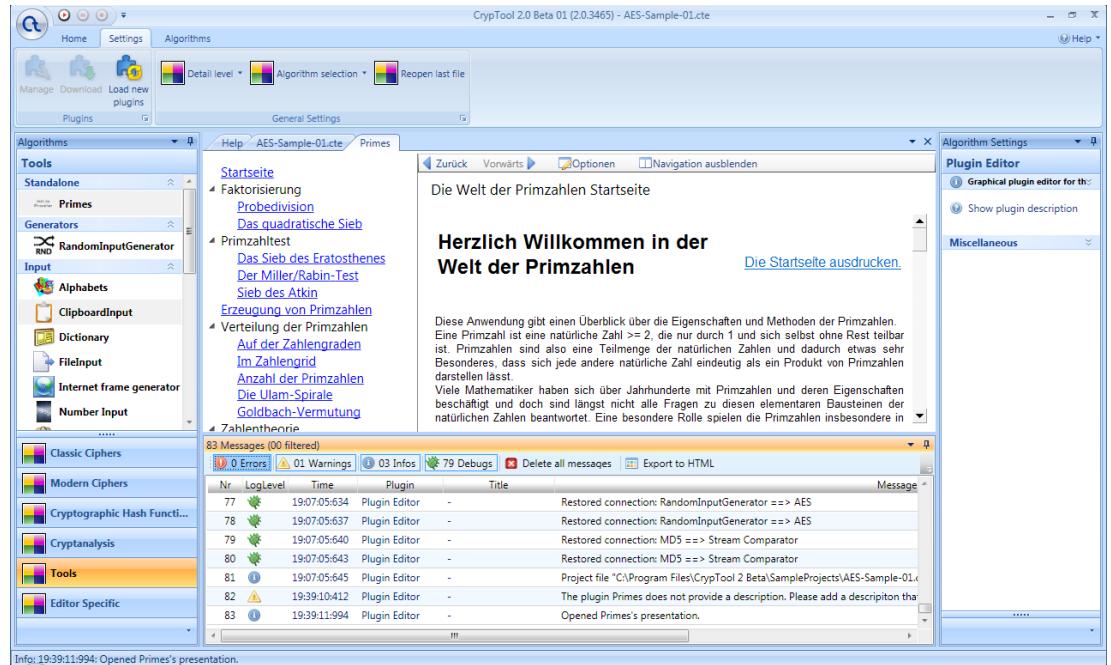


Abbildung 24: Bildschirmfoto von „Die Welt der Primzahlen“

In der Standardansicht wirkt *Die Welt der Primzahlen* im Workspace gefangen. Die Einordnung in die Kategorie *Tools* zusammen mit allerlei Algorithmen zur visuellen Programmierung wird ihm ebenso wenig gerecht wie die Platzbeschränkung durch die Fenster *Algorithm Settings* und *Messages*. Umso bedauerlicher ist es, dass die Navigation auf der linken Seite, ebenso wie die verschiedenen Einträge rechts, nicht scrollbar ist. Korrigiert man die Darstellung mittels der bereits mehrfach erwähnten F11-Taste, so wird das Programm benutzbar.

Die Hilfetexte sind meist kurz und informativ⁸⁵, zumindest, wenn man über mathematisches Vorwissen verfügt. Für einen Laien erschließt sich der Sinn trotz Einführung und kontextsensitiver Hilfe nur schwer. Die Funktion zum Drucken der Hilfetexte wirkt unnatürlich⁸⁶ und der Schriftzug *Diese Seite drucken* (vgl. Abbildung 26) auf den einzelnen Seiten ist weder intuitiv noch zeitgemäß. Die Druckfunktion ist ohnehin besser zentral in der Multifunktionsleiste aufgehoben, von wo aus man alle Seiten und Workspaces von CrypTool 2 drucken können sollte.

85 Der Hilfetext zu *Die zu testende Zahl generieren* unter *Primzahltests* ist nicht hinterlegt.

86 Warum sollte man einen zweizeiligen Hilfetext auf eine ganze DIN-A4 Seite drucken?

Inkonsistent ist auch die Verwendung von Fenstern, in denen die „*Onlinehilfe*“ angezeigt wird. Während CrypTool 2 seine Hilfe (und auch das Programm *Primes* selbst) in Registerkarten auf dem Workspace anzeigt, öffnet die Hilfe von *Die Welt der Primzahlen* eigene Fenster, die sogar außerhalb der Programminstanz von CrypTool 2 sind. Verwirrend sind auch die Navigationssymbole (Vorwärts und Zurück) in den Fenstern der kontextbezogenen Hilfe, da diese das Konzept der Kontextsensitivität in Frage stellen.

Die bereits erwähnte Kopfzeile bringt außer der *Optionen*-Funktion im gegenwärtigen Umfeld keinen Funktionsgewinn, sie verwirrt nur. Erklären lässt sich die Kopfzeile durch den ebenfalls modularen Aufbau von *Die Welt der Primzahlen*, aus dem CrypTool 2 zur Zeit allerdings keinen Nutzen zieht. So wäre es beispielsweise möglich, die einzelnen Visualisierungen von den unterschiedlichsten Positionen in CrypTool 2 direkt aufzurufen. Damit könnte von einer Erklärung eines CrypTool 2 - Algorithmus aus (wie beispielsweise RSA) das nötige mathematische Wissen (wie beispielsweise zahlentheoretische Funktionen: Eulersche Phi-Funktion) zugänglich gemacht werden.

Ein weiterer Kritikpunkt ist die Umsetzung der verschiedenen Links, also Verknüpfungen zu weiterführenden Textstellen. Zum einen öffnen Internetlinks⁸⁷ den Microsoft Internet Explorer und nicht den Standardbrowser des Betriebssystems, was weder konsistent mit CrypTool 2 noch akzeptabel für Nutzer alternativer Browser ist. Zum anderen ist nicht erkennbar, auf welche Seite ein Link führt, es ist noch nicht einmal erkennbar, ob ein Link auf ein Ziel innerhalb der Programmhilfe zeigt oder ob er in das Internet führt. Hier wäre die Statuszeile oder ein kurzer Hilfetext in Form eines *Tooltip* sehr hilfreich. Weiterhin sind Links, die lediglich den Namen „hier“⁸⁸ tragen, nicht nützlich.

Um *Die Welt der Primzahlen* gewinnbringend anwenden zu können, muss man über ein umfangreiches Vorwissen aus dem Bereich der Zahlentheorie verfügen. So ist die Darstellung für einen Mathematikstudenten, der eine Vorlesung zur Zahlentheorie gehört hat, sicherlich hilfreich. Doch bereits für einen

⁸⁷ In *Die Welt der Primzahlen*, nicht in CrypTool 2.

⁸⁸ Z.B. bei der Hilfe zu *Der Miller/Rabin-Test*.

Informatikstudenten (und erst recht für die anderen Nutzergruppen) dürfte nicht klar werden, was die Darstellung zum Ausdruck bringen soll. Ein sehr großer Teil der Probanden gab bei der Beantwortung des Fragebogens zwar an, sich mit den Artikeln von Wikipedia schnell einen Überblick über neue oder bislang unbekannte Sachverhalte verschaffen zu können, doch möchte ich dies anzweifeln. Weiterhin muss in Anlehnung an die didaktische Analyse von Klafki⁸⁹ die Frage gestellt werden, warum sich jemand damit beschäftigen sollte und welche Bedeutung das Thema, hier also die Visualisierungen zur Zahlentheorie, in der Gegenwart oder der Zukunft hat. Diese Verknüpfung kann zumindest beim selbst organisierten Lernen am besten durch das Einbetten in einen sinnstiftenden Kontext hergestellt werden. Daher sollte es, wie bereits angedeutet, möglich sein, von den betreffenden Algorithmen aus direkt auf die einzelnen Darstellungen zuzugreifen. So wird beispielsweise bei RSA und dem ElGamal-Kryptosystems die Funktion $a^b \mod c$ benötigt, also sollte von dort aus auch die Visualisierung *Potenziieren modulo einer Zahl im Kreis* aufgerufen werden können.

Leider sind die Erklärungen und Hintergrundinformationen, die *Die Welt der Primzahlen* sowohl bei der Visualisierung als auch in der Onlinehilfe anbietet, für einen mathematischen Laien nicht ausreichend. Da eine systematische und

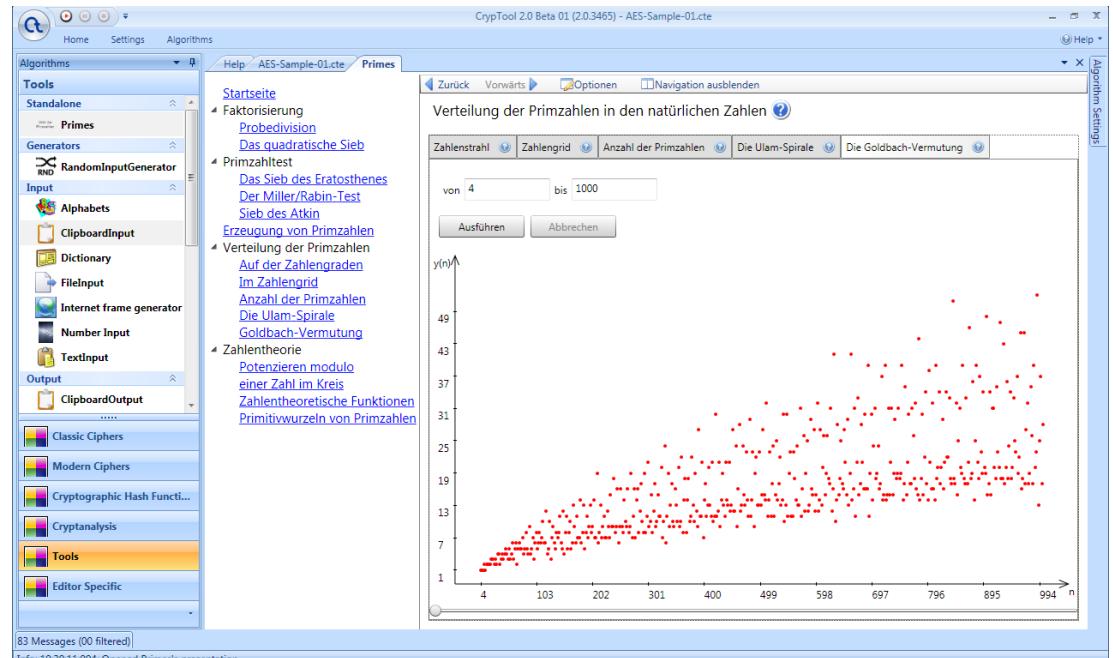


Abbildung 25: Visualisierung zur Goldbach-Vermutung

89 Siehe auch 3.3. Didaktisch-methodische Überlegungen sowie [Jank/Meyer], S. 133.

detaillierte Betrachtung aller Visualisierungen von *Die Welt der Primzahlen* den Umfang dieser Examensarbeit strapazieren würde, möchte ich die Problematik exemplarisch am Beispiel der *Visualisierung zur Goldbach-Vermutung*⁹⁰ darlegen. Nachdem man den entsprechenden Menüpunkt ausgewählt hat, kann ein Intervall durch Eingabe zweier gerader Zahlen zwischen 4 und 100.000 bestimmt werden, für das die Visualisierung durchgeführt werden soll. Nachdem die Ausführung gestartet wurde, baut sich ein Diagramm auf. Allerdings wird an keiner Stelle klar, was in der Visualisierung eigentlich graphisch dargestellt wird. Die Vermutung Goldbachs wird

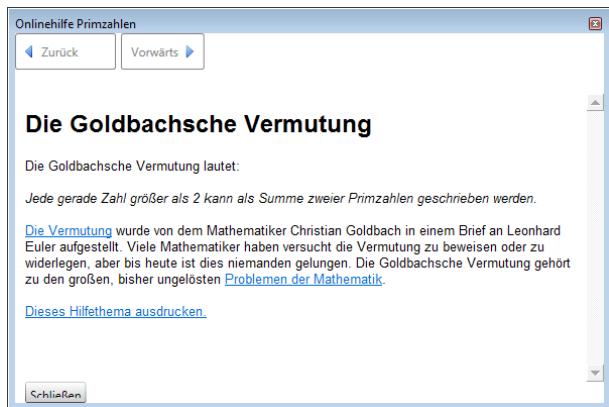


Abbildung 26: Hilfetext zur Goldbach-Vermutung

in der Onlinehilfe⁹¹ zwar kurz zitiert, doch auch hier wird für Nicht-Mathematiker nicht deutlich, was die Graphik aussagen soll und nach welcher mathematischen Funktion sie gezeichnet wurde. Es fehlt die Erklärung, dass der Funktionswert $y(n)$ einer Zahl n die Anzahl der möglichen Zerlegungen von n in seine

additiven Primfaktoren (nach Goldbachs Vermutung) darstellt. Zur Verdeutlichung dieser mehrfachen Goldbachzahlen und damit verbunden das Zustandekommen des Funktionswertes der Visualisierung sollte mit kleinen Zahlen gezeigt werden⁹². Für einen Laien, der nicht mit mathematischen Formulierungen und Denkweisen vertraut ist, stellt sich auch die Frage, warum nur „gerade Zahlen größer als 2“ in Goldbachs Vermutung betrachtet und in der Visualisierung dargestellt werden. Hier sollte aus didaktischen Gründen unbedingt erläutert werden, dass zwei die kleinste und einzige gerade Primzahl ist. Somit müsste jede ungerade Zahl die Summe aus zwei und einer ungeraden Primzahl sein, was wiederum bedeutete, dass jede ungerade Zahl eine Primzahl wäre. Da dies nicht so ist, gilt die Goldbachsche Vermutung nur für gerade Zahlen. Für ungerade Zahlen ergibt sich daher auch immer ein Funktionswert $y(n)$

90 Siehe Abbildung 25.

91 Siehe Abbildung 26.

92 Beispielsweise: $4 = 2 + 2$, nur eine Möglichkeit, also $y(4) = 1$; $8 = 3 + 5$, also $y(8) = 1$; $16 = 3 + 13 = 5 + 11$, zwei Möglichkeiten, also $y(16) = 2$; $24 = 5 + 19 = 7 + 17 = 11 + 13$, also $y(24) = 3$.

von 0 (wenn $n-2$ nicht prim ist) oder 1 (wenn $n-2$ prim ist). Dieser Grund für das „Ignorieren“ ungerader Zahlen sollte auch einem Nicht-Mathematiker klar werden.

Auch wenn sich dieses Teilprogramm *Die Welt der Primzahlen* nennt, so sind auch weitere zahlentheoretische Elemente enthalten. Bezuglich der Verwendung im Zusammenhang mit Kryptographie sehe ich noch Bedarf an weiteren, bisher nicht implementierten Bereichen aus der Zahlentheorie. Zum Bereich der Primzahlen gehört zweifelsfrei der ggT, der mit Hilfe des *Euklidschen Algorithmus* visualisiert werden kann, doch auch die Darstellung des *erweiterten Euklidschen Algorithmus* wäre wünschenswert. Zur Restklassenrechnung gehört meines Erachtens auch ein *Taschenrechner* (Addition, Multiplikation und Potenzrechnung), der die Ergebnisse ebenfalls „im Kreis“ anzeigen kann sowie der *Chinesische Restsatz*. Im Hinblick auf spätere Verbesserungsvorschläge⁹³ wäre die Integration und Visualisierung der mathematischen Zusammenhänge von Shanks Babystep-Giantstep Algorithmus, des Square and Multiply-Algorithmus⁹⁴ sowie die zahlentheoretischen Grundlagen von RSA, ElGamal sowie elliptischer Kurven wünschenswert.

⁹³ Siehe 5.1. Lernebenen.

⁹⁴ Zum schnellen Potenzieren, auch binäre Exponentiation genannt.

5. Fazit und Erweiterungsvorschläge

Im vorherigen Abschnitt habe ich die aktuelle Version von CrypTool 2 vor allem unter den Aspekten Konsistenz, Einfachheit bzw. Intuitivität sowie Erwartungskonformität betrachtet, da diese für Anwender aller Zielgruppen wichtige Lernvoraussetzungen darstellen.

Von noch nicht implementierten, aber vorgesehenen Funktionen⁹⁵ und Programmfehlern abgesehen, hat sich für mich durch die Rückmeldung der Probanden und meine eigene eingehende Betrachtung von CrypTool 2 gezeigt, dass das bestehende CrypTool 2 vor allem für Anwender geeignet ist, die bereits Erfahrungen mit Programmierung haben. Interessant ist allerdings, dass eine Mathematikstudentin große Schwierigkeiten mit CrypTool 2 hatte, obwohl sie bereits einen Java-Programmierkurs absolvieren musste. Ein Versicherungskaufmann hingegen, der lediglich vor 20 Jahren mit einem Commodore C64 Erfahrungen sammelte, kam nahezu problemlos damit zurecht. Daher sind es wohl nicht die Programmierkenntnisse, die eine Rolle spielen, sondern vielmehr die Vertrautheit mit allgemeinen Konzepten von Programmierung.

Probanden, die nicht über dieses Programmierwissen verfügten, hatten die größten Schwierigkeiten, die gestellten Aufgaben zu bewältigen. Dabei fiel es nicht allein schwer, ein eigenes visuelles Programm zu erstellen, sondern bereits das Interpretieren und Bedienen von mir vorgefertigter „Arbeitsblätter“ sorgte zum Teil für erhebliche Probleme⁹⁶.

Zunächst war es meine Absicht, CrypTool 2 mit Hilfe einschlägiger Literatur⁹⁷ zu evaluieren. Davon habe ich jedoch wieder Abstand genommen, da meines Erachtens das Hauptproblem von CrypTool 2 aus didaktischer Sicht die selbst proklamierte äußerst heterogene Zielgruppe ist und CrypTool 2 diesbezüglich jedoch keinerlei Differenzierung in der Bedienung oder bei Hilfestellungen anbietet.

⁹⁵ Z.B. C# Inline-editor, Sprachumschaltung.

⁹⁶ Zwei weitere Probanden äußerten nur mündlich, dass sie mit der Bedienung der Oberfläche überfordert waren.

⁹⁷ Z.B. von Peter Baumgartner, Rolf Schulmeister, Michael Kerres oder Andreas Holzinger.

Daher möchte ich mich nun stattdessen darauf konzentrieren, wie das Programm für die unterschiedlichen Nutzertypen, also auch die ohne Programmierwissen, zugänglich gemacht werden kann. Hier möchte ich mich jedoch gegen eine Unterteilung in verschiedene Betriebsmodi wie einen *Anfängermodus* oder einen *Expertenmodus* aussprechen. Zum einen ist es möglich, dass der Benutzer beispielsweise *Anfänger* bei der Programmierung ist und *Experte* bezüglich der Zahlentheorie, zum anderen hat mich bei anderen Programmen diese Selbsteinschätzung oft überfordert. Außerdem vermisste ich beispielsweise bei einem Plugin von CrypTool 2 eine Funktion zum Ändern des Datentyps eines Eingangs und dachte, dass diese nicht implementiert sei. Auf die Idee, dass diese Option durch eine Steigerung des *Detail level* angezeigt werden könnte, wäre ich nicht gekommen.

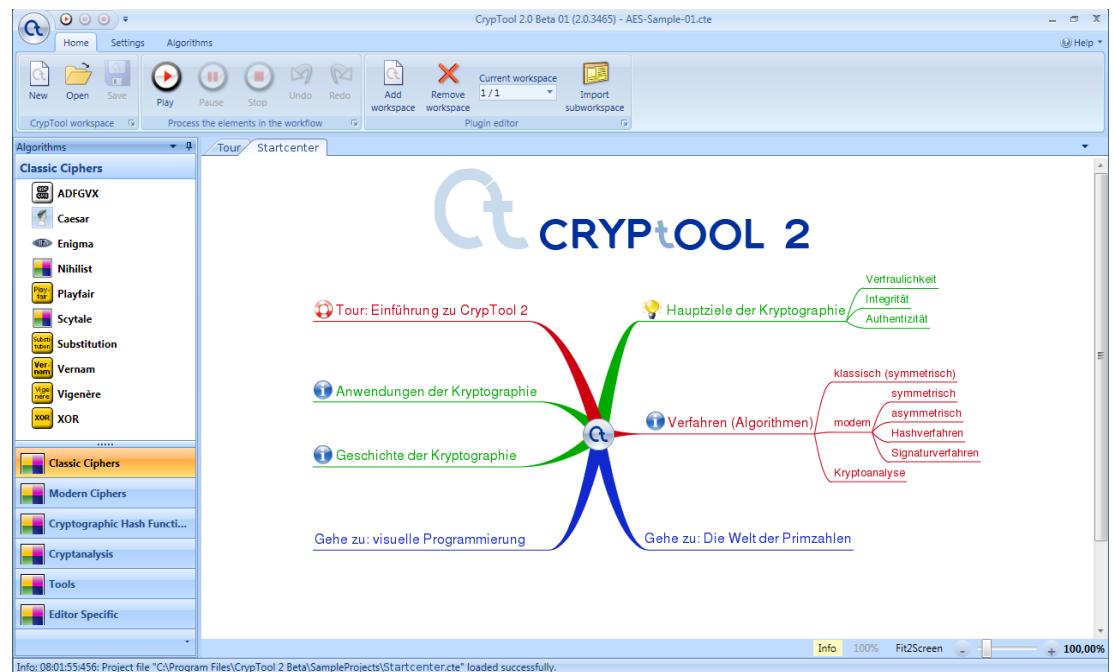
Daher empfinde ich die Einteilung in verschiedene Level oder Modi als unnatürlich, irreführend und kompliziert. Ich wünsche mir vielmehr eine Oberfläche, die auf einfache Weise die gewünschten Informationen und Möglichkeiten anbietet und trotzdem für einen absoluten Laien intuitiv und verständlich ist. Weiterhin ist es meine Überzeugung, dass sich das Thema Didaktik nicht in einem eigenen Modul oder Plugin unterbringen oder an einzelnen Stellen hinzufügen lässt. Hier gilt, wie so oft, dass die Kette so stabil ist wie ihr schwächstes Glied. Daher muss der Gestaltung von CrypTool 2 ein ganzheitliches, differenzierendes und verlässliches Konzept zugrunde gelegt werden, das vielfältige Hilfestellungen auf unterschiedlichsten Niveaus programmweit anbietet und zum selbständigen Lernen anregt.

Im folgenden möchte ich Vorschläge entwickeln, die diese Gedanken aufgreifen und umsetzen. Die Ansätze sind nach ihrem zeitlichen Auftreten bei einem Programmstart gegliedert, da diese Reihenfolge auch einem neuen Benutzer begegnet.

5.1. Startcenter

Zur Zeit öffnet sich nach einem Programmstart der Workspace zur visuellen Programmierung. Es fehlt ein allgemeinverständlicher Einstieg, der eine generelle Orientierung erlaubt. Dabei denke ich vor allem an eine übersichtliche Einführung in den grundsätzlichen Nutzen, die Anwendungsbereiche und die drei Hauptziele der

Kryptographie. Der Inhalt dieses Startcenters, das immer dann angezeigt werden sollte, wenn CrypTool 2 direkt aufgerufen wird⁹⁸, muss sich an den Lernzielen und Erwartungen der verschiedenen Nutzergruppen orientieren, Zugang zu einer Einführung in das Programm und den wichtigsten CrypTool 2 Funktionen bieten und trotzdem ansprechend, schlank und übersichtlich gestaltet sein. Um die Funktionalität der Multifunktionsleiste zu erhalten und so die Bedienung konsistent zu halten, möchte ich vorschlagen, das Startcenter als normalen Workspace mit Text, Graphiken und Links, allerdings ohne ein visuelles Programm zu realisieren.



In Abbildung 27 ist ein Vorschlag zur Gestaltung eines solchen Startcenters zu sehen⁹⁹. Die Darstellung als Mindmap habe ich gewählt, da hier die verschiedenen Aspekte zur Kryptographie ansprechend und intuitiv visualisiert werden können. Die einzelnen Punkte sollten als Link gestaltet werden und jeweils zu einer Seite mit weiteren Informationen führen. So entsteht ein Lernangebot, das ähnlich einer Internetseite in sich vernetzt ist.

Die grün gefärbten Einträge sollen einen Einblick in die Ziele, die Anwendungen und die Geschichte der Kryptographie bieten und sind daher als leicht verständlicher

⁹⁸ Und nicht etwa durch einen Doppelklick auf eine CTE-Datei.

⁹⁹ Eine größere Darstellung findet sich im Anhang.

Einstieg in das Thema gedacht¹⁰⁰. Zur Motivation von Schülern und anderen nicht sonderlich technisch interessierten Anwendern sind auch Hintergrundinformationen und Exkurse zu Enigma, Geheimdiensten (NSA, Echelon), Computerspionage bei Unternehmen und Regierungen, aber auch zu den Beale-Chiffren, der Babington-Verschwörung, dem Voynich-Manuskript oder der Zimmermann-Depesche möglich.

Die rot gefärbten Einträge sind inhaltlich näher am jetzigen CrypTool 2 und sollen ein Arbeiten und Lernen mit ihm erleichtern. Auf die *Tour* gehe ich im nächsten Abschnitt ausführlicher ein, der Bereich *Verfahren* soll einen eher technischen Überblick über die einzelnen Algorithmen bieten. Auf den entsprechenden Unterseiten sollten aber auch weiterführende Themen¹⁰¹ behandelt werden, die hier der Übersichtlichkeit wegen weggelassen wurden.

Die blauen Einträge schließlich sind direkte Verweise auf die Bereiche von CrypTool 2, die für einen fortgeschrittenen Benutzer wichtig sind und die er zur Umsetzung seiner Ideen benötigt.

5.2. *Guided Tour*

Eine *geführte Tour* richtet sich an neue Benutzer eines Computerprogramms und soll ihnen einen leichten Einstieg in die Arbeit damit ermöglichen. CrypTool 2 verfügt bereits in der aktuellen Programmversion über einen sehr leistungsfähigen Workspace zur visuellen Programmierung.

Wie die Rückmeldungen der Probanden gezeigt haben, ist zumindest Nicht-Informatikern das Konzept der visuellen Programmierung oftmals nicht vertraut und bedarf einer Einführung. In der *geführten Tour* müssen daher die wesentlichen Aspekte der visuellen Programmierung leicht verständlich erläutert werden. Hierzu gehören vor allem der Sinn, Aufbau und die Arbeitsweise eines visuellen Programms, die verschiedenen Datentypen, der Play-Mode sowie die Verwendung

¹⁰⁰ Unter <https://www.cryptoportal.org/>, einer Seite, die zum CrypTool-Projekt gehört und Lehrern die Möglichkeit des Austauschs von Unterrichtsmaterialien bietet, hat H. Witten eine Powerpoint-Präsentation zur „Krypto-Entwicklung“ veröffentlicht. Möglicherweise lassen sich die Graphiken zur Einführung in die Geschichte bzw. die Anwendungen der Kryptographie verwenden. Die betreffenden Graphiken habe ich dem Anhang dieser Examensarbeit beigefügt.

¹⁰¹ Wie der Unterschied zwischen Strom- und Blockchiffren, Hybridverfahren, die verschiedenen Angriffskategorien und -methoden sowie Kerkhoffs Prinzip.

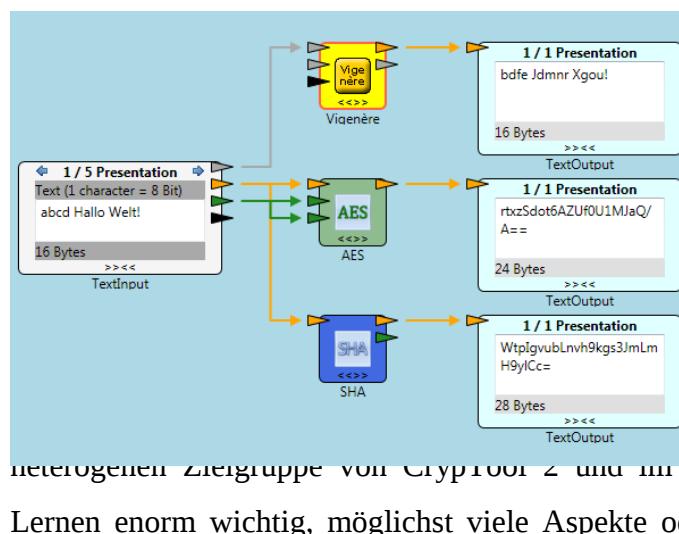
von Workspaces und Sub-Workspaces.

Ebenfalls hilfreich ist eine Einführung in die Bedienelemente *Multifunktionsleiste* und *Navigationsfenster* sowie den Leistungsumfang von CrypTool 2. Es sollte in der *geführten Tour* klar werden, welche Lernangebote CrypTool 2 beinhaltet und welche Ziele damit erreicht werden können.

Neben der Darstellung als bebildelter Text ist auch ein kurzes Einführungsvideo sinnvoll¹⁰², da hier neue Nutzer am leichtesten einen Einblick in die Funktionsweise und den Leistungsumfang von CrypTool 2 erhalten.

5.3. Lernebenen

Bereits CrypTool 1.4.xx bietet dem Nutzer Hilfestellung und Wissen aus verschiedenen Bereichen und auf unterschiedlichen Niveaus an¹⁰³. In CrypTool 1.4.xx sind diese Funktionen jedoch im Programm verteilt und stehen in keinem Zusammenhang zueinander. Zur Zeit werden in CrypTool 2 die Algorithmen nur als Symbol auf dem Workspace zur visuellen Programmierung dargestellt, ein paar kurze Informationen über das jeweilige Plugin können über *Algorithm settings* abgerufen werden. Da sich der Aufbau eines visuellen Programms in CrypTool 2 für



die verschiedenen Plugins stark ähnelt¹⁰⁴, werden Struktur und Funktionsweise des einzelnen Verfahrens für den Anwender nicht sichtbar, die vielen weiteren Aspekte eines Algorithmus kommen dabei finde ich es gerade bei der heterogenen Zielgruppe von CrypTool 2 und 3 im Sinne von selbst organisiertem Lernen enorm wichtig, möglichst viele Aspekte oder Ebenen zu einem Verfahren

¹⁰² Ähnlich des Screencasts zu CrypTool 1.4.21, das unter der Internetseite <http://www.cryptool.org/index.php/de/screencast-mediamedia-92.html> zu sehen ist.

¹⁰³ Zu nennen sind hier: Verfahren, Visualisierungen, Skript, CrypTool Präsentation, Szenarien (Tutorials), Onlinehilfe, ReadMe, Spiele, Kurzgeschichten.

¹⁰⁴ Eingabe, Verarbeitung im oft unbekannten Algorithmus, Ausgabe

darstellen zu können. Diese Lernebenen sollen es dem Nutzer ermöglichen, einem Algorithmus auf verschiedenste Arten näher zu kommen.

Im wesentlichen sehe ich zu jedem Algorithmus neun verschiedene Lernebenen, die ich im folgenden kurz darstellen möchte.

- *Geschichte(n):* Mit interessanten Hintergrundinformationen wie beispielsweise die Vorläufer, Erfindung und Nutzung der Vigenère-Verschlüsselung, statistische Auffälligkeiten im Geheimtext, Brechen des Verfahrens durch Babbage und Kasiski.
- *Einführung:* Eine leicht verständliche, nicht wissenschaftliche Einführung, die einem Laien genug Informationen bietet, den Algorithmus ohne Detailwissen zu verstehen und mit ihm zu arbeiten.
- *Skript:* Das CrypTool Skript ([Esslinger 2]) aus der Programmversion 1.4.xx bietet umfassende und wissenschaftliche Beschreibungen. Das Skript sollte jedoch nicht als Ganzes eingebunden werden, da es in seiner Gesamtheit mit weit über 200 Seiten nur für wenige Anwender interessant ist. Für wesentlich besser und unmittelbarer halte ich die Integration relevanter Abschnitte in logischer Nähe zum einzelnen Algorithmus.
- *Tutorial:* In der Programmversion 1.4.xx bietet das Tutorial eine bebilderte Anleitung zur Verwendung der einzelnen Verfahren. Meine Idee für ein Tutorial in CrypTool 2 geht darüber hinaus, die Anleitung zum Plugin sollte mit einer interaktiven Demo verbunden sein, um den Nutzer mit der Arbeitsweise des Algorithmus vertraut zu machen. Hier sollte der Anwender alle Eingänge und Einstellungen des Plugins direkt verändern und die daraus resultierenden Reaktionen verstehen können.
- *Visuelles Programm:* Die den einzelnen Verfahren zugrunde liegenden Algorithmen können jeweils als visuelles Programm dargestellt werden. Ich finde diese Darstellung nicht nur reizvoll, sondern auch aus didaktischer Sicht ausgesprochen lehrreich. Zum einen wird so die Funktionsweise des einzelnen Algorithmus wie an einem interaktiven Flußdiagramm deutlich und kann schrittweise nachvollzogen werden, zum anderen kann der Nutzer aus

der Betrachtung des Aufbaus eines Algorithmus wieder Anregungen für die Verwendung des Workspaces zur visuellen Programmierung bei eigenen Projekten mitnehmen¹⁰⁵.

- *Programmcode:* Die CrypTool 2 Roadmap ([Südmeyer]) verspricht einen *Inline Code Editor* für CrypTool 2, der C# Code kompiliert und ausführt. Leider ist dieser noch nicht integriert. Gerade für Informatikstudenten wäre es aber sicher hilfreich, wenn sie nicht nur eigenen Code testen, sondern auch bestehenden Referenzcode analysieren und modifizieren könnten. Hier besteht eine gute Gelegenheit, die eigenen Kenntnisse an bestehenden Algorithmen auszuprobieren.
- *Visualisierung:* Visualisierungen sind bereits in CrypTool 1.4.xx integriert und erklären das betreffende Verfahren schematisch, oft mit einer Animation oder in mehreren Schritten. Besonders für die mathematischen Algorithmen sind hier ergänzend auch Verweise zu entsprechenden Modulen von *Die Welt der Primzahlen* sinnvoll, wo die zahlentheoretischen Hintergründe beleuchtet werden können.
- *Übungen:* Mit Übungsaufgaben wird erlerntes Wissen praktisch angewendet. Meines Erachtens dürfte es schwierig sein, die Lösung freier Aufgaben (z.B. „Entwerfen Sie ein visuelles Programm, das ...“) automatisiert mit einem Computerprogramm zu überprüfen. Daher denke ich, dass solche Aufgaben weniger gut geeignet sind. Möglich und zur Selbsteinschätzung sinnvoll hingegen sind Fragen zu Geschichte und Funktionsweise eines Algorithmus sowie bei den asymmetrischen Verfahren zur zugrunde liegenden Mathematik, eventuell mit Zahlenbeispiel und Rechnung.

Darüber hinaus sind sogenannte *Crypto Challenges*, bei denen man versucht, gegebene Geheimtexte zu analysieren und zu entschlüsseln, eine beliebte Methode, die eigenen Fähigkeiten zu testen.

- *Kurzweiliges:* Die Idee zu dieser Lernebene stammt ebenfalls aus CrypTool 1.4.xx, hier sind das Spiel *Der Zahlenhai* sowie zwei *Kurzgeschichten zur*

¹⁰⁵ Ein Beispiel dafür ist in 5.5. *Beispiel: RSA* und in Abbildung 34 dargestellt.

Zahlentheorie zum Rätseln integriert. Natürlich wird man nicht zu jedem Algorithmus einen solchen Lernaspekt einfügen wollen, aber es sollte die Möglichkeit vorhanden sein, solche bestehenden Anregungen in geeigneter Weise zu integrieren.

Diese Vielfalt an Lernebenen und Auswahloptionen darf den Nutzer allerdings nicht überfordern und sollte daher gezielt und strukturiert angeboten werden. Die Zuordnung der Lernebenen zu den einzelnen Algorithmen ist nicht nur inhaltlich naheliegend, sondern auch für einen Nutzer intuitiv und natürlich, denn so kann er einem Verfahren aus den verschiedenen Blickwinkeln näher kommen.

Als geeignete Möglichkeit, die Lernebenen sowohl zentral als auch übersichtlich und unaufdringlich zu integrieren, scheint mir bei CrypTool 2 die Verwendung einer speziellen Registerkarte in der Multifunktionsleiste zu sein. Die *2007 Microsoft Office System User Interface Design Guidelines* ([MS officeui]) sehen sogenannte *Contextual Tabs* vor, wo bei der Markierung einiger spezieller Objekte¹⁰⁶ eine eigene Registerkarte in der Multifunktionsleiste erscheint, die alle Optionen, die zu dieser Art Objekt zusätzlich verfügbar sind, beinhaltet. Ebenso könnte in CrypTool 2 bei Auswahl eines Plugins die Lernebenen-Registerkarte eingeblendet werden. Es ist allerdings auch denkbar, die Lernebenen als konventionelle, immer eingeblendete Registerkarte einzubinden, bei der nicht zutreffende Einträge deaktiviert dargestellt werden. Die in meinem Vorschlag für einen Lernebenen-Tab (siehe Abbildung 29) verwendeten Graphiken sind der Sammlung des OpenClipart Projekt¹⁰⁷ entnommen.



Abbildung 29: Vorschlag eines Lernebenen-Tabs für die Multifunktionsleiste

106 In Microsoft Word beispielsweise Graphikobjekte.

107 Informationen dazu auf der Projekt Homepage unter <http://www.openclipart.org/>.

Die Lernebenen sollten auch bereits bei der Auswahl¹⁰⁸ eines Plugins im Navigationsfenster am linken Bildschirmrand zugänglich sein, um sich vor der Verwendung eines Algorithmus zunächst über ihn informieren zu können. Auch das bisher im Navigationsfenster nicht verwendete Kontextmenü¹⁰⁹ könnte neben einem Eintrag zum Ablegen auf dem Workspace die verschiedenen Lernebenen enthalten.

Die zuvor erwähnten *Crypto Challenges* sind üblicherweise freie und durchaus anspruchsvolle Wettbewerbe, unbekannte Geheimtexte zu entschlüsseln. Die Übungen zu den einzelnen Algorithmen sollten jedoch nicht zu schwierig sein, außerdem ist der verwendete Algorithmus aufgrund der Zuordnung klar, was ebenfalls eine Erleichterung darstellt. Daher möchte ich zusätzlich zu den Übungen eine Funktion *Lade Crypto Challenge* anregen, die in der *Home*-Registerkarte der Multifunktionsleiste beheimatet sein könnte. Einer Integration in CrypTool 2 steht allerdings der damit verbundene Aufwand entgegen, diesen Wettbewerb zu betreuen und regelmäßig neue Aufgaben zu stellen. Es gibt allerdings auch Projekte, die internationale und öffentliche *Crypto Challenges* durchführen, wie beispielsweise *Mystery-Twister*¹¹⁰, das vom Lehrstuhl für Kryptologie und IT-Sicherheit an der Ruhr-Universität Bochum betreut wird. Eventuell gibt es Möglichkeiten, diesen Wettbewerb via CrypTool 2 zu nutzen.

5.4. Sub-Workspaces

Wie bereits erwähnt, bieten die bisher leider nur rudimentär vorhandenen Sub-Workspaces eine gute Gelegenheit, Programmteile ähnlich eines Unterprogramms auszulagern. Die Idee dazu geht auf die Diplomarbeit von Thomas Schmid zum CrypTool Editor¹¹¹ zurück und ist auch gerade aus didaktischer Sicht gut zu verwenden. Zum einen kann ein Teil der Komplexität eines visuellen Programms ausgelagert werden, was die Übersichtlichkeit im Sinne einer didaktischen Reduktion deutlich erhöht und so den Blick auf das Wesentliche erleichtert. Zum anderen kann in solch einem Sub-Workspace ein komplexerer Algorithmus mit einfachen

108 Also nach einfachem Maus-Klick.

109 Das Kontextmenü wird üblicherweise durch Klicken mit der rechten Maustaste geöffnet.

110 Siehe <http://www.mystery-twister.com/>.

111 Vergleiche 2.4.1. *Diplomarbeit zum Editor für CrypTool 2*.

Grundbausteinen visuell programmiert werden, so dass der Anwender versteht, wie er funktioniert. Darunter leidet zwar die Ausführungsgeschwindigkeit, doch der visuell programmierte Algorithmus soll auch nicht regulär durchlaufen werden. Er dient, wie unter der Lernebene *Visuelles Programm* dargestellt¹¹², nur der schrittweisen Nachvollziehbarkeit und visuellen Anschauung. Trotzdem muss der visuell implementierte Algorithmus voll funktionsfähig sein und es dem Nutzer erlauben, die Konsequenzen der Änderung verschiedener Parameter nachzuvollziehen.

Diese Sub-Workspaces sollten sich, um effektiv damit arbeiten zu können, ebenso leicht öffnen, bearbeiten und speichern lassen wie normale Workspaces. Dazu sollten sie, wie bereits beschrieben, in einem eigenen Tab geöffnet und auch leicht in andere Workspaces eingefügt werden können.

5.5. Beispiel: RSA

Unter Berücksichtigung meiner bisherigen Verbesserungsvorschläge möchte ich hier exemplarisch einen Entwurf für ein visuelles Programm vorstellen, das den RSA Algorithmus visuell implementiert und somit leichter zugänglich macht. Die dazu benötigten und noch nicht in CrypTool 2 integrierten Algorithmen sind:

- Ein Modulo-Rechner, der umschaltbar addiert, multipliziert oder potenziert. Der oberste Eingang wird a zugeordnet, der mittlere b und der unterste c . Wird Eingang c nicht belegt, so wird in den natürlichen Zahlen \mathbb{N} gerechnet. Das Ergebnis der Rechnung wird über den Ausgang auf der rechten Seite ausgegeben.
- Die Euler'sche φ -Funktion gibt für jede gegebene natürliche Zahl die Anzahl der zu ihr teilerfremden Zahlen an, die kleiner sind als diese. Daher benötigt sie keine weiteren Argumente und hat nur einen Eingang und

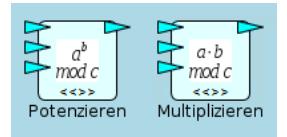


Abbildung 30:
Symbol des
Modulo-Rechners



Abbildung 31: Symbol der
Euler'schen Phi-Funktion

¹¹² Siehe 5.3. Lernebenen.

einen Ausgang. Das mathematische (und technische) Hauptproblem bei der Berechnung von φ ist die Faktorisierung der gegebenen Zahl, weshalb hier die Rechenleistung des verwendeten Computers berücksichtigt werden muss. Auch eine Fortschrittsanzeige könnte aus diesem Grund nützlich sein.

- Der einfache (und seit der Antike bekannte) Euklid'sche Algorithmus berechnet aus zwei ganzen Zahlen ($a, b \in \mathbb{Z}$) deren größten gemeinsamen Teiler ggT. Durch die modernere Erweiterung des Algorithmus kann der ggT als Linearkombination der beiden Ausgangszahlen dargestellt werden. Es werden also die Koeffizienten s und t der Gleichung $ggT(a, b) = s \cdot a + t \cdot b$ ermittelt. Die Eingänge lesen die Zahlen a und b ein, die Ausgänge liefern von oben nach unten genannt $ggT(a, b)$, s und t .

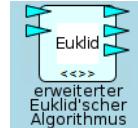
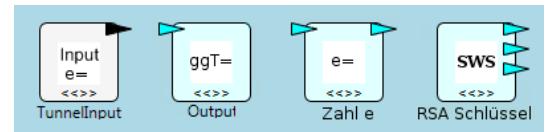


Abbildung 32: Symbol des erweiterten Euklid'schen Algorithmus

In der Zahlentheorie (und auch beim RSA-Algorithmus) macht man sich diesen erweiterten Algorithmus zunutze, da man mit seiner Hilfe in einem Restklassenring das inverse Element bestimmen kann.

- Die verbleibenden Symbole, die ich in meiner Skizze verwende, repräsentieren einige bereits in CrypTool 2 vorhandene Plugins, die ich lediglich dahingehend modifizierte, dass sie auch minimiert Variablennamen anzeigen. Zwar werden bei der visuellen Programmierung keine Variablennamen mehr benötigt, doch im Rahmen dieser eher mathematischen Darstellung erscheint mir dies zur Verbesserung der Orientierung dennoch sinnvoll¹¹³.



Das dritte Symbol von links gibt den Eingabewert unverändert aus, es wird lediglich benötigt, um darzustellen, dass der öffentliche Schlüssel im Internet zugänglich gemacht wird und dort abgerufen werden kann.

¹¹³ So können einzelne Elemente im Erläuterungstext benannt werden.

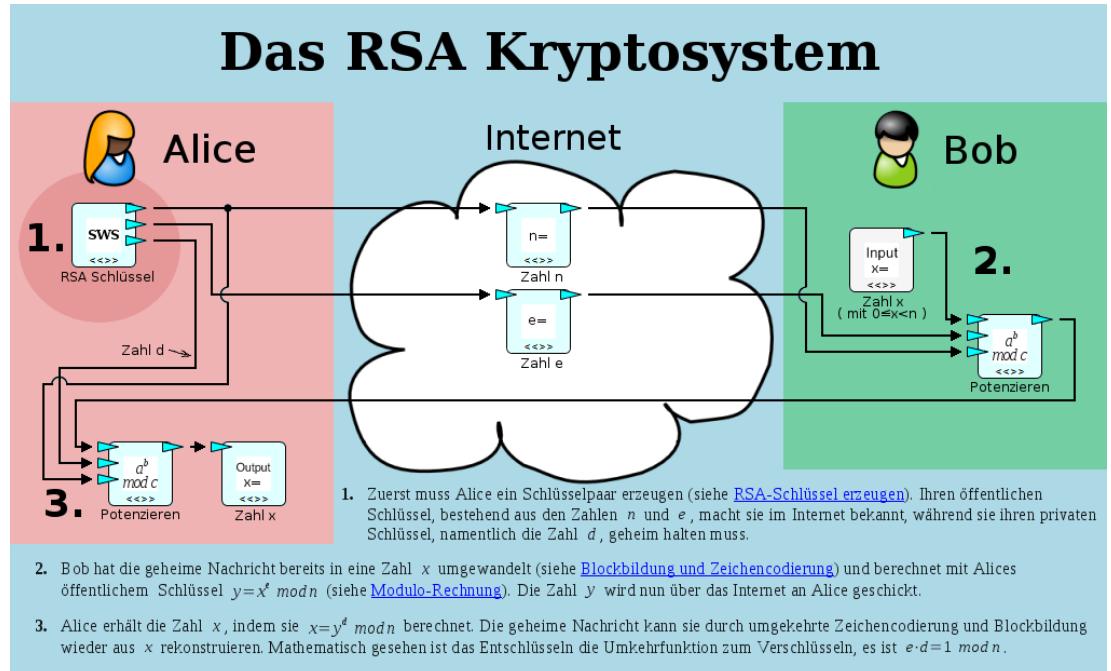


Abbildung 34 zeigt einen Workspace, der das RSA Kryptosystem vorstellt und die zugrunde liegenden Vorgänge des Ver- und Entschlüsselns einer Nachricht erläutert¹¹⁴. Die verwendeten Graphiken sind wieder der Sammlung des OpenClipart-Projekts entnommen, der besseren Sichtbarkeit wegen habe ich die Verbindungslien der Algorithmen schwarz gehalten.

Der RSA-Schlüssel wurde als eigener Sub-Workspace gestaltet und ausgelagert, da es zum einen die Komplexität der Darstellung reduziert, zum anderen aber auch verdeutlicht, dass der Schlüssel nicht für jede Nachricht neu generiert werden muss. So ist es für den Anwender zunächst einmal nicht wichtig, ob der Schlüssel erzeugt wird oder ob er lediglich in gespeicherter Form vorliegt. Wichtig ist jedoch, dass der RSA-Schlüssel aus einem Teil besteht, der veröffentlicht wird (*public key*) und aus einem anderen Teil, der geheim bei Alice verbleibt (*private key*).

Durch die Gruppierung der Symbole und die farbliche Unterlegung ist intuitiv klar, welche Prozesse wo stattfinden. Bei der Darstellung der zu übermittelnden Nachricht habe ich mich der besseren Übersicht wegen dagegen entschieden, die Blockbildung und Umwandlung in eine Zahl ebenfalls darzustellen. Dies kann besser in einer eigenen Darstellung verdeutlicht werden, die dann von mehreren Algorithmen aus

¹¹⁴ Eine größere Darstellung, die auch den weiteren Bedienelementen von CrypTool 2 beinhaltet, findet sich im Anhang.

verknüpft werden kann. Wie bereits erwähnt, sollen die Symbole, die „im Internet“ platziert sind, lediglich zeigen, dass der öffentliche Schlüssel publik gemacht werden soll.

Bei genauerer Betrachtung stellt man fest, dass das Ver- und Entschlüsseln mit RSA lediglich das Potenzieren einer Zahl in einem Restklassenring ist. Die entsprechenden Hintergrundinformationen können mittels Verknüpfungen direkt aufgerufen werden.

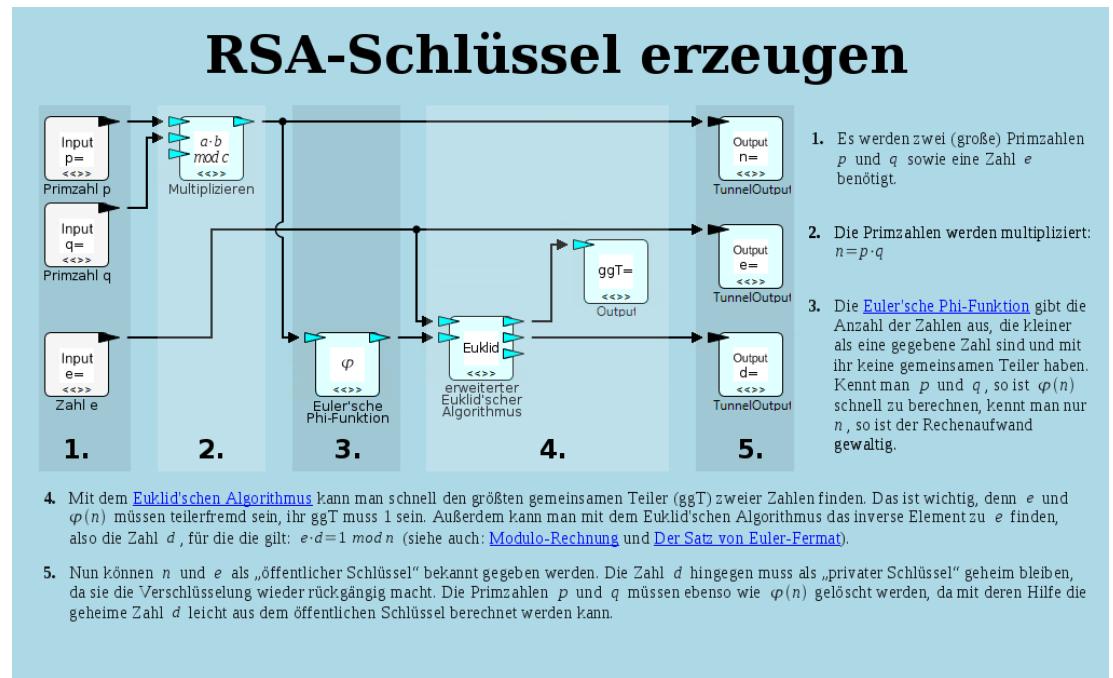


Abbildung 35: Workspace zur visuellen Erzeugung eines RSA-Schlüssels

Der Sub-Workspace zur Erzeugung eines RSA-Schlüssels (siehe Abbildung 35¹¹⁵) kann durch ein Klicken auf das Sub-Workspace-Symbol geöffnet werden. Ein weiterer Zugang dazu sollte über die Lernebene *visuelles Programm* des noch fehlenden CrypTool 2 - Plugins zum Generieren eines RSA-Schlüssels möglich sein.

Üblicherweise läuft die Erzeugung eines RSA-Schlüssels automatisiert ab. Um den Vorgang nachvollziehbar zu gestalten, ist es sinnvoll, die übliche Erzeugung von Pseudozufallszahlen sowie die Verifizierung der Gültigkeit der Eingaben zu entfernen. Möglicherweise kann das Eingabe-Plugin die Primalität der Eingabe überprüfen, aus didaktischen Gründen kann es aber auch durchaus sinnvoll sein, auch

115 Eine größere Darstellung, die auch den weiteren Bedienelementen von CrypTool 2 beinhaltet, findet sich im Anhang.

„verbotene“ zusammengesetzte Zahlen zuzulassen. Daher ist auch der Sonderfall $\varphi(p \cdot q) = (p-1) \cdot (q-1)$ nicht notwendigerweise gegeben und $\varphi(n)$ muss durch Faktorisierung von n berechnet werden. Dies wiederum verkürzt aufgrund der benötigten Rechenleistung die mögliche Schlüssellänge. Doch andererseits verdeutlicht gerade dieser Rechenaufwand die Sicherheit des RSA-Verfahrens bei ausreichend großer Schlüssellänge.

Der Sub-Workspace ist in fünf Bereiche gegliedert, die einem schrittweisen Ablauf entsprechen. Zu jedem Schritt gibt es eine kurze Erläuterung und auch Verweise innerhalb von CrypTool 2, die Grundlagenwissen oder Vertiefungen anbieten. So kann man beispielsweise die Bedeutung des Satzes von Euler-Fermat¹¹⁶ zur Bestimmung des inversen Elementes in einem Restklassenring auf einer neuen Registerkarte in Erfahrung bringen.

5.6. Schlusswort

CrypTool 2 stellt mit dem Workspace zur visuellen Programmierung ein ausgesprochen leistungsfähiges Werkzeug zur Verfügung, mit dem verschiedene Algorithmen angewendet und kombiniert werden können.

Auch wenn ich mehrere Detailverbesserungen der aktuellen Programmversion von CrypTool 2 anregen konnte¹¹⁷, hat sich gezeigt, dass das zugrunde liegende Konzept vor allem Personen anspricht, die mit den Bereichen Programmierung und Kryptographie vertraut sind. Da CrypTool 2 auch von Anwendern verwendet werden soll, die diese Voraussetzungen nicht erfüllen, ist es nötig, an das Vorwissen dieser Anwender anzuknüpfen und vielfältig vernetzte Lernangebote und Einstiegsmöglichkeiten zu integrieren. Hier sind insbesondere eine Einführung¹¹⁸, Vermittlung von Grundlagenwissen¹¹⁹ und der Bezug zu alltagsrelevanten

¹¹⁶ Der Satz von Euler-Fermat könnte beispielsweise in *Die Welt der Primzahlen* integriert und dort erläutert und mit Beispielen angereichert werden.

¹¹⁷ Vor allem in Bezug auf Usability und Intuitivität.

¹¹⁸ In das Thema Kryptographie und in die Bedienung und den Funktionsumfang von CrypTool 2.

¹¹⁹ Z.B.: Was ist Kryptographie? Was sind die Hauptziele der Kryptographie? Wie funktionieren die modernen *Public Key Verfahren* prinzipiell? Welche rechtlichen Aspekte gibt es?

Fragestellungen¹²⁰ sowie vertiefende Ausführungen zu den einzelnen Algorithmen¹²¹ erforderlich.

Gerade die Darstellung eines Algorithmus als visuelles Programm¹²² kann die Funktionsweise schematisch und interaktiv deutlich machen. Hier sind Sub-Workspaces ausgesprochen hilfreich, um jeweils nur die nötige Komplexität darstellen zu müssen und weiterführende Informationen¹²³ auszulagern. Bei rückgekoppelten Algorithmen¹²⁴ sollte jedoch neben dem *Play-Mode*, der die automatisierte Ausführung startet, auch ein Modus zur schrittweisen Ausführung¹²⁵ enthalten sein. So lässt sich der zunächst schlecht überschaubare Gesamtablauf in nachvollziehbare Einzelschritte zerlegen. So entwickelt sich ein vernetztes und umfassendes Lernangebot, das Wissen auf verschiedenen Ebenen verbindet und so das bestehende CrypTool 2 aus didaktischer Sicht bereichert.

Da CrypTool 2 immer wieder durch sehr unterschiedlich ausgestaltete Beiträge erweitert wird¹²⁶, besteht die Gefahr, dass Darstellung oder Bedienung inkonsistent werden. Dies ist einem erfolgreichen Lernen und Arbeiten äußerst abträglich, da so die Aufmerksamkeit des Anwenders immer wieder vom eigentlichen Lerninhalt auf Nebensächlichkeiten gelenkt wird. Dieses Problem kann nur dadurch gelöst werden, dass ein umfassender und konkreter didaktischer Rahmen vorgegeben wird¹²⁷, in den die verschiedenen Beiträge eingefügt werden.

120 Z.B.: Wie funktioniert Online-Banking oder ein *Virtual Private Network*? Warum werden Verbindungen im WLAN verschlüsselt? Können Hacker meine Daten ausspähen?

121 Um die Vielfalt der Informationen systematisch anbieten zu können, habe ich die Einführung von Lernebenen vorgeschlagen. Die Funktionsweise eines Algorithmus sollte auf verschiedenen Ebenen und unter Verwendung verschiedener Darstellungsarten verdeutlicht werden.

122 Mit erklärenden Hilfetexten.

123 Aber auch Unter-Algorithmen oder Erklärungen bzw. Grundlagenwissen.

124 Also solche, die ihre Ausgabe wieder als nächste Eingabe verwenden wie rundenbasierte Verschlüsselungsalgorithmen (z.B. AES) oder auch der Euklid'sche Algorithmus.

125 Wie in der Programmierung bei Debuggern üblich.

126 Die beispielsweise im Rahmen von Diplomarbeiten entstehen.

127 Wie beispielsweise die von mir genannten Lernebenen als Ausgangspunkt.

6. Abbildungs- und Literaturverzeichnis

Abbildungsverzeichnis

Abbildung 1: Ein Bildschirmfoto von CrypTool 1.4.xx [CT_48].....	13
Abbildung 2: Ein Bildschirmfoto von CrypTool 2.....	14
Abbildung 3: Der Splash Screen von CrypTool 2.....	35
Abbildung 4: Die Fortschrittsanzeige beim Programmstart von CrypTool 2.....	36
Abbildung 5: CrypTool 2 nach dem Programmstart.....	37
Abbildung 6: Dialog Box Launcher der Multifunktionsleiste.....	39
Abbildung 7: Symbol einer kollabierten Gruppe.....	39
Abbildung 8: Multifunktionsleiste, Registerkarte Home.....	39
Abbildung 9: Multifunktionsleiste, Registerkarte Settings.....	41
Abbildung 10: Multifunktionsleiste, Registerkarte Algorithms.....	42
Abbildung 11: Das Navigationsfenster.....	42
Abbildung 12: Das Konfigurationsfenster.....	43
Abbildung 13: Das Logbuch.....	45
Abbildung 14: Unklare Verbindungen in Factorisation-Sample.cte.....	48
Abbildung 15: Vorschlag für klarere Abzweigungen und Kreuzungen.....	48
Abbildung 16: Vorschlag für eine lokale Fehlermeldung im visuellen Programm....	49
Abbildung 17: Beispiele für Symbole von Algorithmen.....	50
Abbildung 18: Die QuickWatch Ansicht eines Algorithmus.....	53
Abbildung 19: Vorschlag zur Erweiterung der QuickWatch-Ansicht.....	54
Abbildung 20: Die Plugin-Beschreibung.....	55
Abbildung 21: Die Präsentation des Plugins Häufigkeitsanalyse.....	56
Abbildung 22: Präsentation des Plugins PRESENT in der QuickWatch-Ansicht.....	56

6. ABBILDUNGS- UND LITERATURVERZEICHNIS

Abbildung 23: Symbol des Stream Comparators.....	57
Abbildung 24: Bildschirmfoto von „Die Welt der Primzahlen“.....	59
Abbildung 25: Visualisierung zur Goldbach-Vermutung.....	61
Abbildung 26: Hilfetext zur Goldbach-Vermutung.....	62
Abbildung 27: Vorschlag zur Gestaltung eines Startcenters.....	66
Abbildung 28: Der Struktur verschiedener visueller Programme ähnelt sich.....	68
Abbildung 29: Vorschlag eines Lernebenen-Tabs für die Multifunktionsleiste.....	71
Abbildung 30: Symbol des Modulo-Rechners.....	73
Abbildung 31: Symbol der Euler'schen Phi-Funktion.....	73
Abbildung 32: Symbol des erweiterten Euklid'schen Algorithmus.....	74
Abbildung 33: Weitere verwendete Symbole von Algorithmen.....	74
Abbildung 34: Workspace zur visuellen Programmierung des RSA Kryptosystems.	75
Abbildung 35: Workspace zur visuellen Erzeugung eines RSA-Schlüssels.....	76
Abbildung 36: Aufgabe 1, Buchstabenhäufigkeit eines Caesar-Textes.....	98
Abbildung 37: Aufgabe 1, Entschlüsseln eines Caesar-Textes.....	91
Abbildung 38: Aufgabe 2, Buchstabenhäufigkeit eines Vigenère-Textes.....	92
Abbildung 39: Aufgabe 3, Kasiski- und Friedman-Test.....	93
Abbildung 40: Aufgabe 3, Entschlüsseln eines Vigenère-Textes.....	94
Abbildung 41: Aufgabe 4, Schema der Funktionsweise von AES.....	95
Abbildung 42: Aufgabe 5, Entschlüsseln eines Enigma-Textes.....	96
Abbildung 43: H. Witten: Geheime Kommunikation.....	125
Abbildung 44: Vorschlag zu einem Startcenter für CrypTool 2.....	126
Abbildung 45: Workspace: Das RSA Kryptosystem.....	127
Abbildung 46: Workspace: RSA-Schlüssel erzeugen.....	128

Literaturverzeichnis

- Bachfeld: BACHFELD, Daniel, Artikel "Großbritannien: Passwort oder fünf Jahre Gefängnis" in "heise Security", Heise Zeitschriften Verlag, 08.10.2007, abgerufen am 1. Oktober 2009,
<http://www.heise.de/security/Grossbritannien-Passwort-oder-fuenf-Jahre-Gefaengnis--/news/meldung/97050>
- Bauer: BAUER, Friedrich L., Entzifferte Geheimnisse, Springer-Verlag, 1995
- Beutelspacher: BEUTELSPACHER, Albrecht, Kryptologie, 8., aktualisierte Auflage, Vieweg Verlag, 2007
- Buchmann: BUCHMANN, Johannes, Einführung in die Kryptographie, 4., erweiterte Auflage, Springer-Verlag, 2008
- CT_42: CrypTool Projekt, CrypTool Seite: "Was ist CrypTool?", abgerufen am 1. Oktober 2009,
<http://www.cryptool.de/index.php/de/about-topmenu-42.html>
- CT_46: CrypTool Projekt, CrypTool Roadmap Seite, abgerufen am 1. Oktober 2009, <http://www.cryptool.de/index.php/de/roadmap-featuresmenu-46.html>
- CT_48: CrypTool Projekt, Screenshots von CrypTool 1.4.xx, abgerufen am 1. Oktober 2009, <http://www.cryptool.com/index.php/de/media-topmenu-48.html>
- CT_63: CrypTool Projekt, CrypTool Download Seite, abgerufen am 1. Oktober 2009, <http://www.cryptool.de/index.php/de/download-topmenu-63.html>
- Eckhardt: ECKHARDT, Timo, Zur Rolle von Primzahlen in der Kryptografie sowie Visualisierung ihrer Eigenschaften, Diplomarbeit an der Universität Siegen, 2008

6. ABBILDUNGS- UND LITERATURVERZEICHNIS

- Esslinger 1: ESSLINGER, Prof. Bernhard, Kryptologie mit CrypTool (Präsentation), Version 1.4.30 Beta04, abgerufen am 1. Oktober 2009, <http://www.cryptool.org/download/CrypToolPresentation-de.pdf>
- Esslinger 2: ESSLINGER, Prof. Bernhard, Das CrypTool-Skript: Kryptographie, Mathematik und mehr (9. Auflage – zu Version 1.4.20), 2008, abgerufen am 1. Oktober 2009, <http://www.cryptool.de/download/CrypToolScript-de.pdf>
- Gnome HIG: Das Gnome Usability Projekt, GNOME Human Interface Guidelines 2.2, abgerufen am 1.Okttober 2009, <http://library.gnome.org-devel/hig-book/stable/>
- Jank/Meyer: JANK, Werner und MEYER, Hilbert, Didaktische Modelle, Cornelsen Verlag Scriptor, 1994
- MBWJK 1: Ministerium für Bildung, Wissenschaft, Jugend und Kultur des Landes Rheinland-Pfalz, Lehrplanentwurf Informatik Grund- und Leistungsfach für die Einführungsphase und Qualifikationsphase der gymnasialen Oberstufe, abgerufen am 1. Oktober 2009, http://gymnasium.bildung-rp.de/fileadmin/user_upload/gymnasium.bildung-rp.de/rechtsgrundlagen/Lehrplan_GF_LF_1-08.pdf
- MBWJK 2: Ministerium für Bildung, Wissenschaft, Jugend und Kultur des Landes Rheinland-Pfalz, Einheitliche Prüfungsanforderungen in der Abiturprüfung Informatik, abgerufen am 1. Oktober 2009, http://www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/1989/1989_12_01-EPA-Informatik.pdf
- MS officeui: Microsoft Corp., 2007 Microsoft Office System User Interface Design Guidelines, 2006, abgerufen am 27 April 2009, <http://msdn.microsoft.com/officeui>
- Norman 1: NORMAN, Donald A., Dinge des Alltags, Campus-Verlag, 1989
- Norman 2: NORMAN, Donald A., Emotional Design, Basic Books, 2005

6. ABBILDUNGS- UND LITERATURVERZEICHNIS

- Schmeh: SCHMEH, Klaus, Codeknacker gegen Codemacher,
2. Auflage, W3L-Verlag, 2008
- Schmid: SCHMID, Thomas, Untersuchungen zur visuellen
Programmierung: Methodik und Umsetzung in moderner
Component Plugin-Architektur auf der .NET-Plattform,
Diplomarbeit an der Universität Siegen, 2008
- Schröder: SCHRÖDER, Dr. Max, Skript zur Kryptographievorlesung,
Universität Koblenz, Sommersemester 2008
- Schröm: SCHRÖM, Oliver, Artikel "Verrat unter Freunden" in "ZEIT
ONLINE", DIE ZEIT 1999, abgerufen am 1. Oktober 2009,
http://www.zeit.de/1999/40/199940.nsa_2_.xml
- Singh: SINGH, Simon und MEE, Nick, The Code Book on CD-ROM,
Version 1.6, abgerufen am 1. Oktober 2009,
http://www.simonsingh.net/The_CDROM.html
- Südmeyer: SÜDMEYER, Philipp, CrypTool 2 Roadmap, 2009-01-05,
abgerufen am 1. Oktober 2009,
http://cryptool2.vs.uni-due.de/downloads/ct2brochure_de.pdf
- Tagesschau: tagesschau.de - Die Nachrichten der ARD,
Artikel "Bankkunden-Daten versehentlich versteigert",
26.08.2008, abgerufen am 31. Oktober 2009,
<http://www.tagesschau.de/ausland/datenschutz126.html>
- Wilkens: WILKENS, Andreas, Artikel "Erste Passwort-Erzungungshaft in
Großbritannien" in "heise Online", Heise Zeitschriften Verlag,
13.08.2009, abgerufen am 1. Oktober 2009,
<http://www.heise.de/newsticker/Erste-Passwort-Erzwingungshaft-in-Grossbritannien--/meldung/143462>

6. ABBILDUNGS- UND LITERATURVERZEICHNIS

WP:AliceBob: Wikipedia, Die freie Enzyklopädie, verschiedene Autoren, Seite „Alice und Bob“, Bearbeitungsstand: 16. Juni 2009, abgerufen am 1. Oktober 2009,
[http://de.wikipedia.org/w/index.php?
title=Alice_und_Bob&oldid=61220742](http://de.wikipedia.org/w/index.php?title=Alice_und_Bob&oldid=61220742)

WP:Kr_graphie: Wikipedia, Die freie Enzyklopädie, verschiedene Autoren, Seite „Kryptographie“, Bearbeitungsstand: 26. September 2009, abgerufen am 1. Oktober 2009,
[http://de.wikipedia.org/w/index.php?
title=Kryptographie&oldid=64942490](http://de.wikipedia.org/w/index.php?title=Kryptographie&oldid=64942490)

WP:PGP: Wikipedia, Die freie Enzyklopädie, verschiedene Autoren, Seite „Pretty Good Privacy“, Bearbeitungsstand: 28. September 2009, abgerufen am 1. Oktober 2009,
[http://de.wikipedia.org/w/index.php?
title=Pretty_Good_Privacy&oldid=65021867](http://de.wikipedia.org/w/index.php?title=Pretty_Good_Privacy&oldid=65021867)

WP:WPK: Wikipedia, Die freie Enzyklopädie, verschiedene Autoren, Seite: "WikiProjekt Kryptologie", Bearbeitungsstand: 21. März 2009, abgerufen am 1. Oktober 2009,
[http://de.wikipedia.org/w/index.php?
title=Wikipedia:WikiProjekt_Kryptologie&oldid=58157116](http://de.wikipedia.org/w/index.php?title=Wikipedia:WikiProjekt_Kryptologie&oldid=58157116)

7. Anhang

7.1. *Danksagung*

Bei der Umsetzung dieser Examensarbeit haben mich viele Menschen unterstützt, denen ich von Herzen Danke sagen möchte:

- Zuerst möchte ich meiner Frau Susanne und meiner Tochter Marlene danken, dass sie mich so sehr unterstützt und manches mal auf mich verzichtet haben. Außerdem hat Susanne die Examensarbeit korrekturgelesen.
- Den Probanden danke ich für ihre Mühe und für so manche Stunde Arbeit. Zum Teil waren die Rückmeldungen sehr ausführlich und lieferten gute Anregungen.
- Professor Esslinger hat mich mit Hintergrundinformationen und bisherigen Arbeiten versorgt und beantwortete viele meiner Fragen. Er zeigte großes Interesse an meiner Arbeit und hat mich so angespornt, gute Ideen zu entwickeln. Dafür danke ich ihm recht herzlich.
- Herr Hug von der Universität Koblenz hat mir ermöglicht, an der HRPI-Fortbildung zur „Kryptographie im Unterricht“ teilzunehmen, Frau Professor Harbusch ebenfalls von der Universität Koblenz hat mir die Ausarbeitung zum „Projektpraktikum CrypTool“ zur Verfügung gestellt.
- Auch die beiden Gutachter dieser Arbeit, Professor Ullrich und Professor Grimm, haben mich in meinem Vorhaben bestärkt und letztlich den Kontakt zu Professor Esslinger und dem CrypTool-Team vermittelt.

Ihnen allen gebührt mein Dank für die vielfältige Hilfe und Unterstützung.

7.2. Befragung von Probanden (Fragebogen)

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 Kryptographievorlesungen 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 Schiebereglern 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 „strengeheim“ 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

7.3. Aufgaben zur Bearbeitung durch die Probanden (Bildschirmfotos)

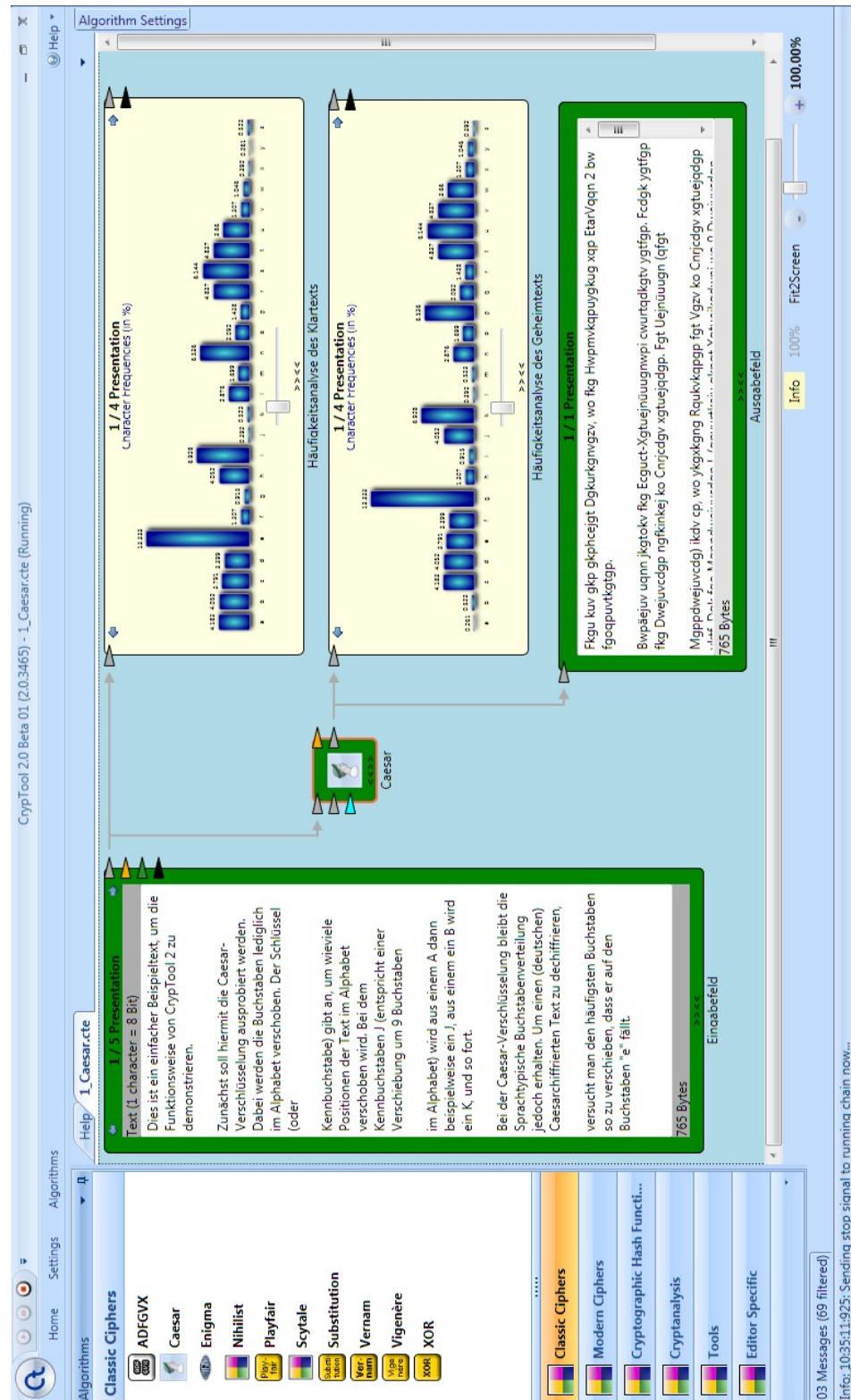


Abbildung 36: Aufgabe 1, Buchstabenhäufigkeit eines Caesar-Textes

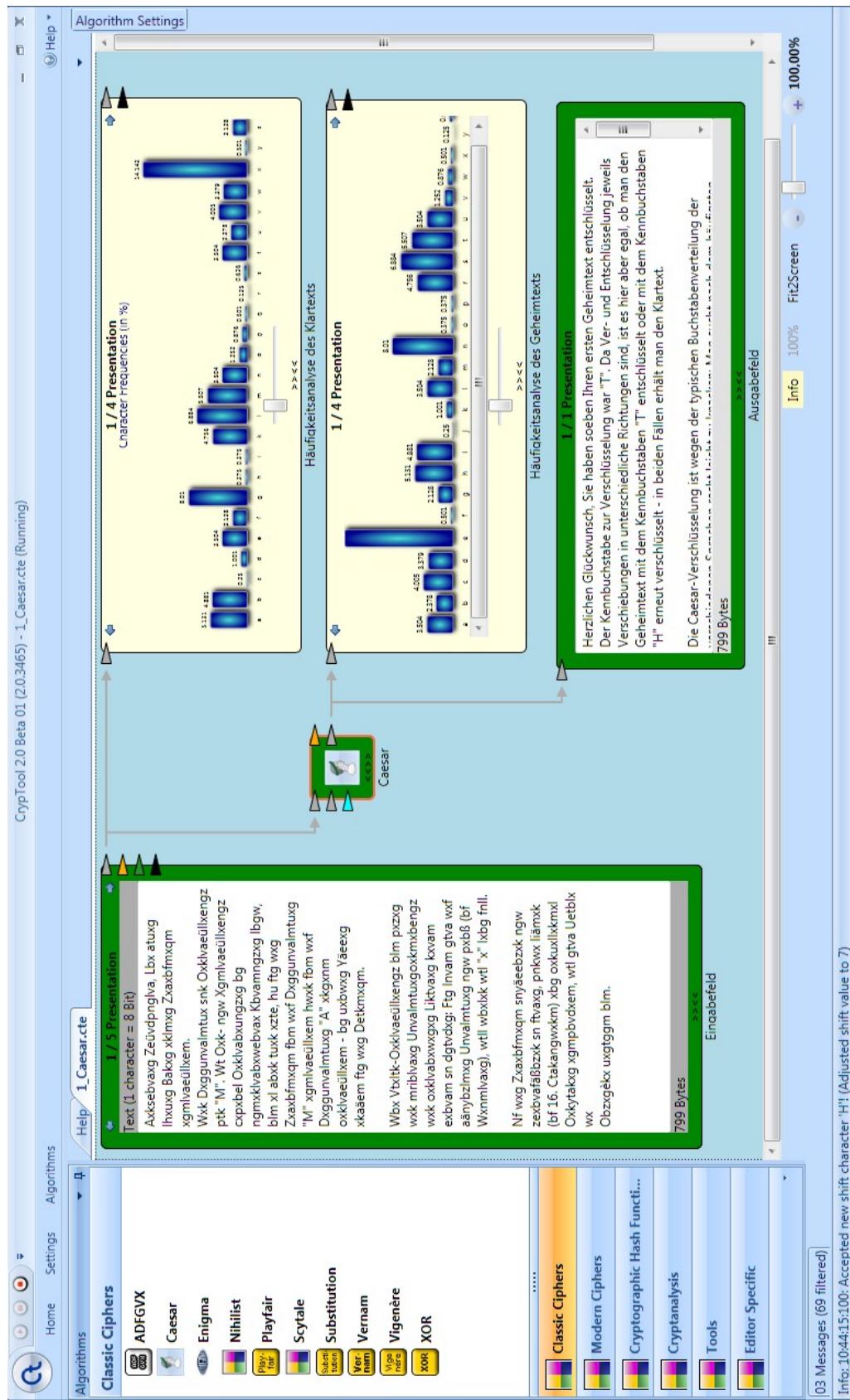


Abbildung 37: Aufgabe 1, Entschlüsseln eines Caesar-Textes

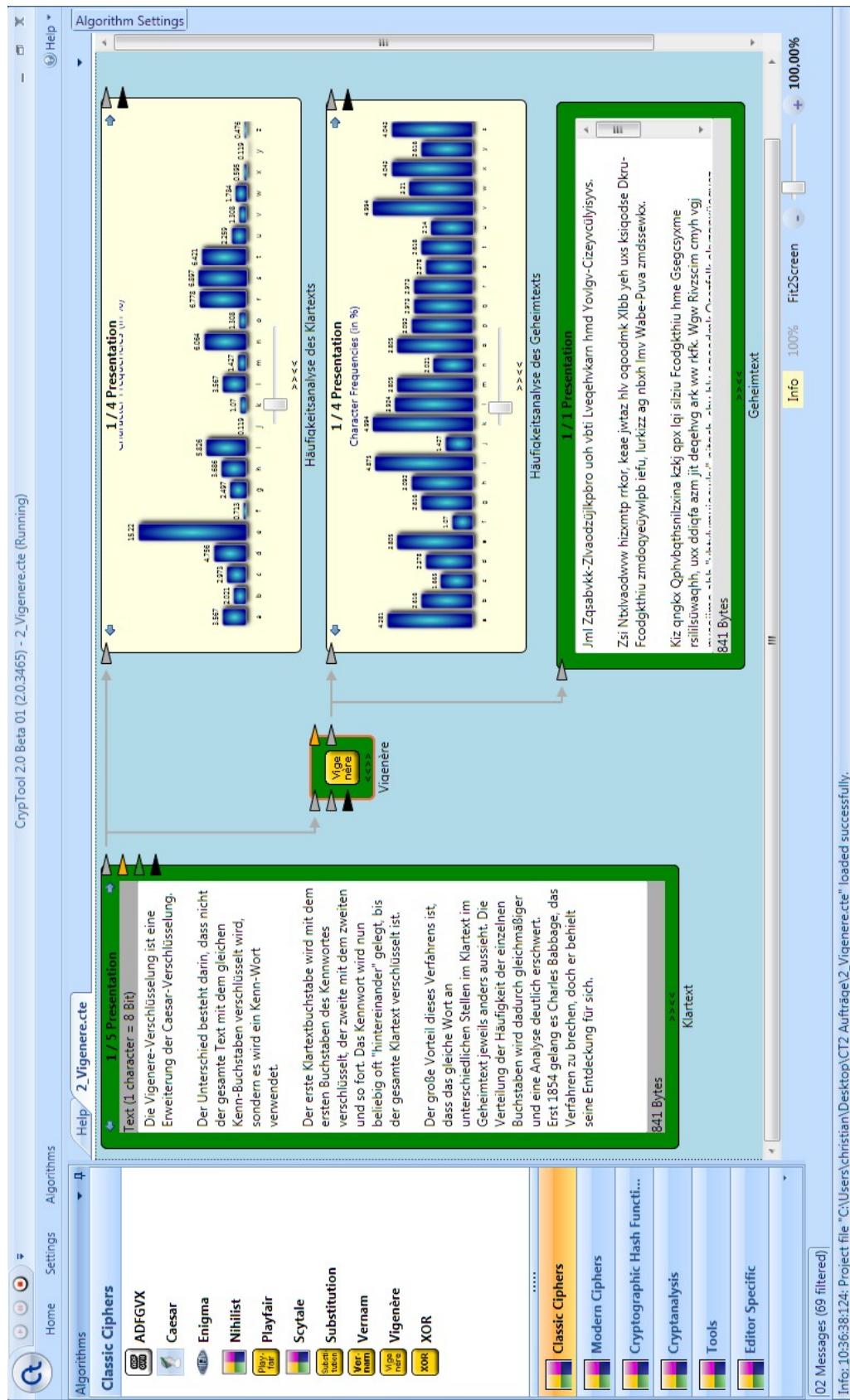


Abbildung 38: Aufgabe 2, Buchstabenhäufigkeit eines Vigenère-Textes

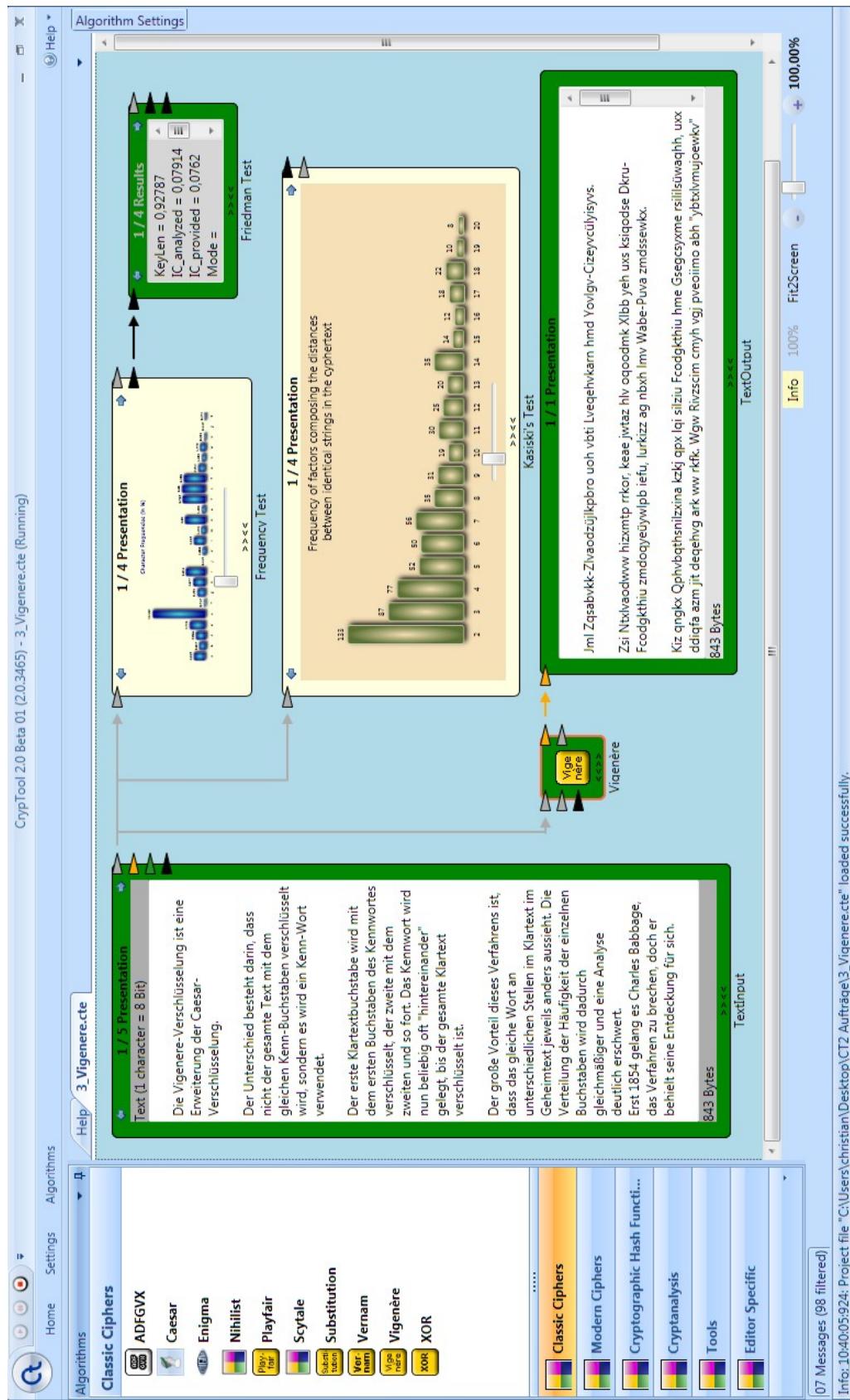


Abbildung 39: Aufgabe 3, Kasiski- und Friedman-Test

07 Messages (98 filtered)
Info: 1040/05/24: Project file "C:\Users\christian\Desktop\CT2 Aufträge\3_Vigenere.cte" loaded successfully.

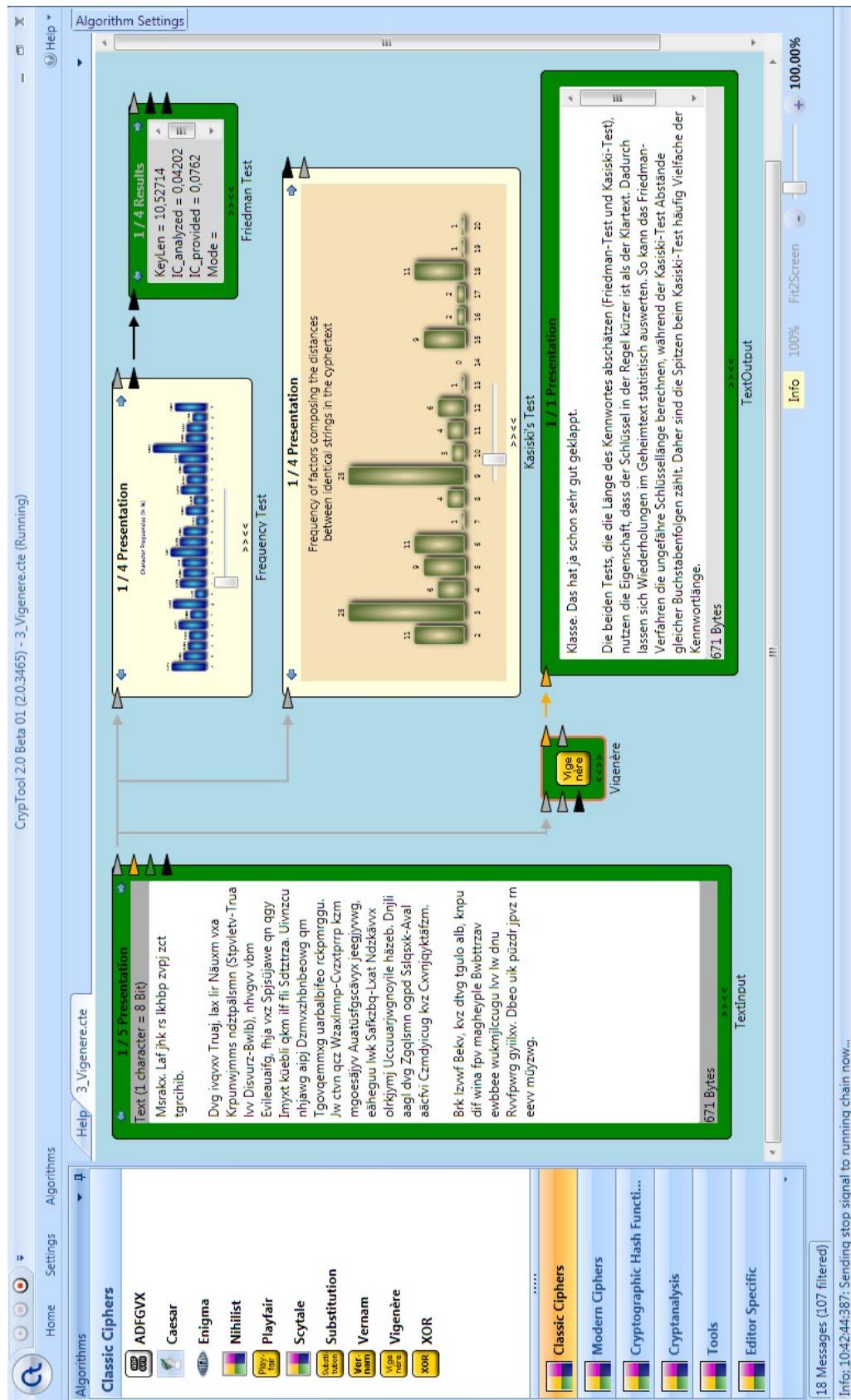


Abbildung 40: Aufgabe 3, Entschlüsseln eines Vigenère-Textes

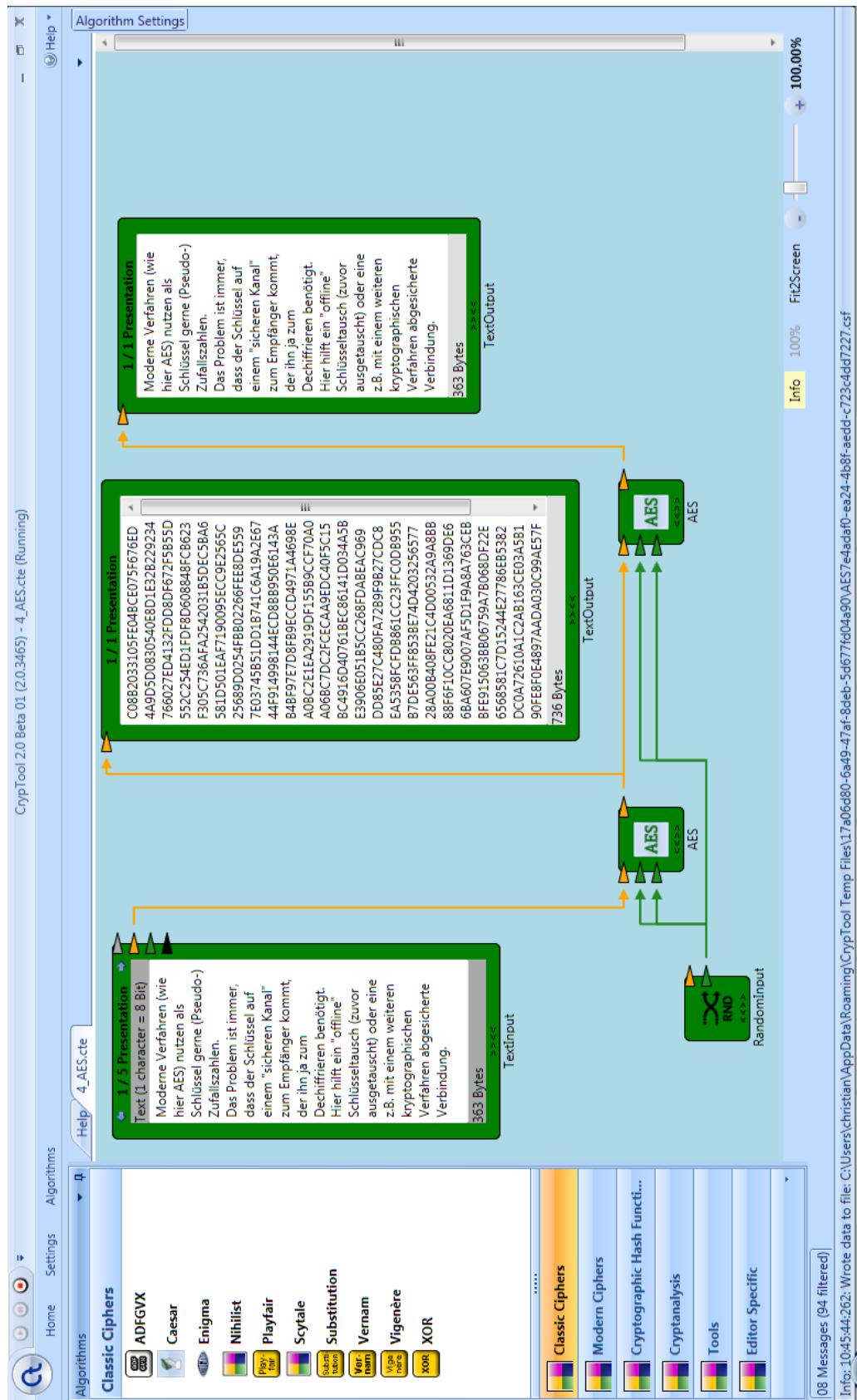


Abbildung 41: Aufgabe 4, Schema der Funktionsweise von AES

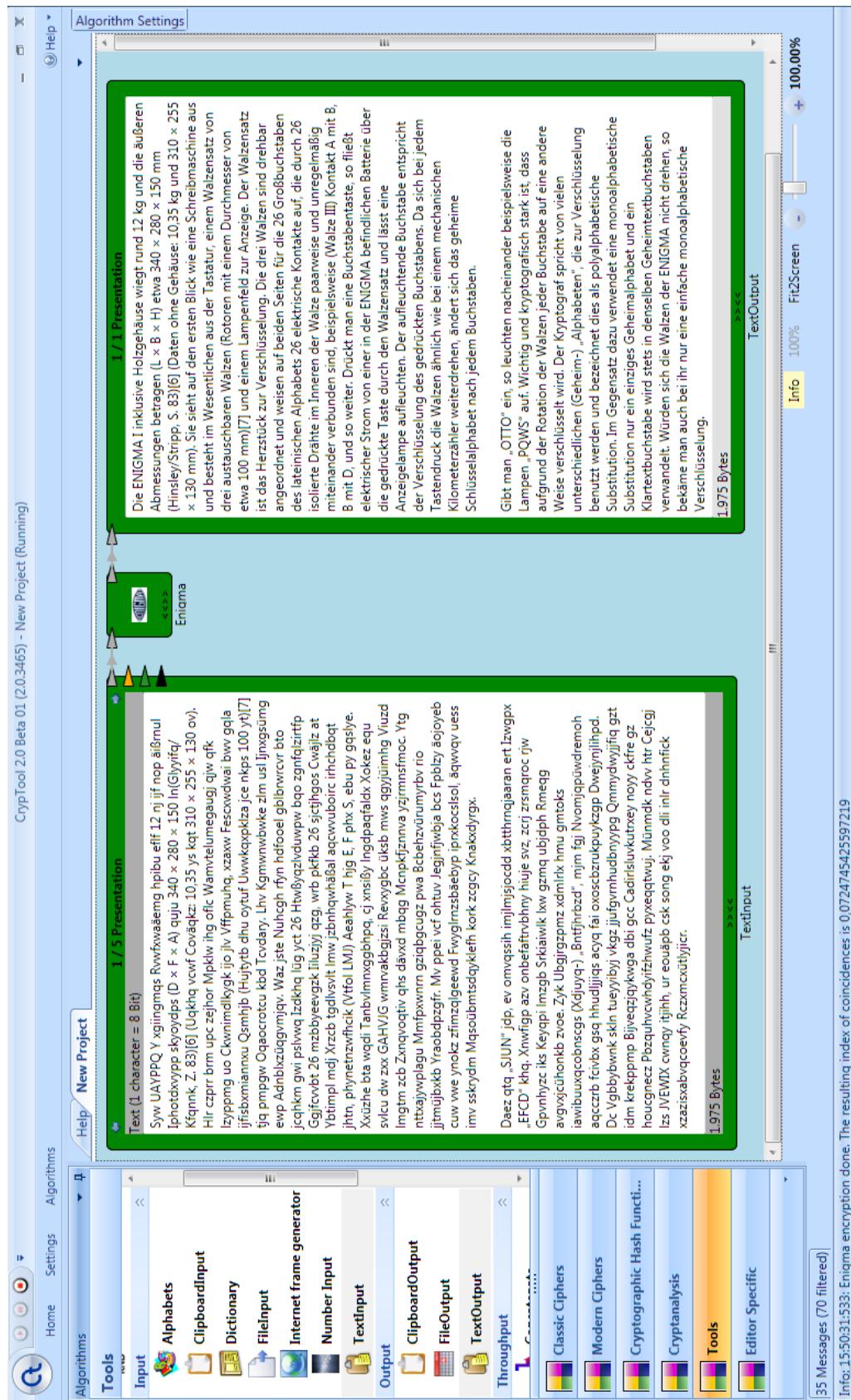


Abbildung 42: Aufgabe 5, Entschlüsseln eines Enigma-Textes

7.4. Antworten der Probanden

Antwort 1:

- A1 - Leistungskurs Mathematik; 3-4er-Kandidatin, nicht so viel Freude
 - Studium Mathematik im Rahmen des Lehramtsstudiums Grund- und Hauptschule, viel Freude, noch keine Ergebnisse (in Form von Studienabschluss)
 - Meine Kenntnisse sind nicht die besten, habe aber Spaß am Ausprobieren und Ausdauer beim Nachvollziehen (auch schwerer Aufgaben)
 - Lasse mich nicht mehr so sehr von Herausforderungen erschrecken oder einschüchtern!
- A2 - Täglich mindestens einmal (außer Urlaub oder ähnliches)
 - Korrespondenz per e-mail
 - Schreiben (für Universität)
 - Im Internet surfen
 - Gelegentlich Computer spielen
 - Gelegentlich DVD sehen
- A3 - Ich komme ganz gut damit zurecht.
 - Blende Funktionen, die ich noch nie angewendet habe vor meinem inneren Auge aus; nutze also nur eine begrenzte Anzahl der möglichen Funktionen
 - Ab und an bin ich am suchen. Leider bin ich noch nicht so gut darin, die Leisten für meinen Gebrauch umzustellen.
- A4 - Nicht direkt. Meist komme ich aber über google auf wikipedia.
 - Es hängt davon ab, wer den Beitrag geleistet hat. Kann je nach Suche sehr unterschiedlich ausfallen.
- A5 - Keine großen Erfahrungen, in der Mittelstufe Englisch-Software
 - Bei mir hält sich der Gedanke (eventuell ein Vorurteil): Zeitaufwand geringer, wenn ich so lerne und nicht mit Software
- A6 Zum Beispiel beim Online-Banking oder Einkaufen per Internet.
- A7 - Enigma
 - Vigenère
 - „Einfaches“ Austauchen von Buchstaben
 - Mehr ist leider nicht hängen geblieben aus der Vorlesung bei Hr. Schröder
- A8 Interessant. Aber mir fällt im Moment kein spezielles Interesse ein.
- E1 Ich bin gut mit den Aufgaben zu recht gekommen. Vielleicht etwas langsam

zu Beginn.

Probleme:

- Habe nicht auf ‚Stop‘ gedrückt, konnte deshalb nichts unter ‚Algorithm settings‘ ändern
- Habe eine Weile nach den Tools suchen müssen.
- Habe bei Aufgabe 3 nicht auf dechiffrieren umgestellt. War eine Weile irritiert und kam deshalb zu keiner Lösung.

E2 Scheint übersichtlich, die Funktionsmöglichkeiten gehen nicht ins Unendliche. Wer mit Microsoft Office schon gearbeitet hat, dem scheint die Oberfläche schnell vertraut.

Das Englisch als Nutzersprache hat mich davon abgehalten, die Hilfsfunktion zu nutzen.

E3 Ganz in Ordnung. Ich finde, die Idee der Textfelder mit den Pfeilen dazwischen gut.

E4 Irritierend bei Enigma Aufgabe: Warum gehen unterschiedlich bunte Pfeile aus den Feldern? Und nicht nur graue?

Neben „new Projekt“ hat sich „Text Input“ Fenster geöffnet, obwohl ich das eigentlich nicht wollte.

Ich fände es einfacher, wenn es nur eine Funktionsleiste geben würde und die Algorithms Anzeige nicht zweimal erscheint. Ich habe die obere leiste kaum benutzt.

E5 Ich hätte kein Problem, mehr mit dem Programm zu arbeiten. Schwierigkeiten könnten da entstehen, wo ich einfach deiner Anwendungserklärung gefolgt bin und eigentlich nicht wusste, was ich tue. Wie mir meine Erfahrung bei Word sagt, entstehen die Probleme erst, wenn ich selber etwas ganz Bestimmtes mit dem Programm erreichen will, und dies nicht klappt. Dazu kommt die Tatsache, dass, wenn man mit dem Programm wirklich arbeiten will, man mehr von den unterschiedlichen Verschlüsselungsverfahren wissen muss.

E6 Habe alles geschrieben, was mir eingefallen ist.

Antwort 2:

- A1 Grundkurs Mathe am Gymnasium mit befriedigendem Erfolg; nutze im Alltag lediglich einfache Rechenkenntnisse; rechne gerne, schalte aber bei komplexeren mathemat. Zusammenhängen schnell ab, wenn sie mich überfordern.
- A2 Nutzung des Internets
- zum Verfassen von E-Mails
 - zum Surfen als Freizeitbeschäftigung
 - Internetrecherche für berufliche Zwecke
 - Online Banking und online Einkäufe
- ansonsten Textverarbeitung (am liebsten mit älteren Windows-Versionen): private und berufl. Korrespondenz
- A3 Nein
- A4 Recht häufig zur Recherche für berufl. Zwecke (gesellschaftl. und politische Themen, Geschichte, Literaturwissenschaften, Allgemeinwissen). Meistens finde ich dabei schnell die Infos, die ich brauche; ich halte die Qualität vieler Beiträge inzwischen für recht gut. Jedoch kaum Erfahrungen im Bereich Mathematik/ Naturwissenschaften; daher kann ich zur Eignung der Beiträge in diesen Bereichen nicht viel sagen.
- A5 Habe lediglich einige Sprachlern-Programme für Kinder ausprobiert. Bin generell eher ein Fan von konventionellen Büchern, Papier und Schreibgeräten, was das Lernen angeht. Halte das Schreiben von Hand auf Papier für wichtig für den Lernprozess.
- A6 Bei allen finanziellen Transaktionen im Internet (Banking, Shopping); beim Versenden von E-Mails?
- A7 Nein
- A8 Als Kind schon: Wir haben selbst Geheimschriften und Codes entwickelt und uns zeitweise damit verständigt.
Heute: Auf populärwissenschaftlichem Niveau, ja. (Z.B. in Form von Beiträgen in einer Zeitung/ einem Magazin.)
Ich würde gerne mehr erfahren über verschiedene Verfahren der Verschlüsselung, Beispiele für Anwendungen aus der Geschichte (z.B. im 2. WK, bei Geheimdiensten); Anekdoten; Wie sicher sind Online-Aktivitäten?

- E1 Ohne zusätzliche persönl. Hilfe gar nicht. Habe die Aufgaben 3-5 gar nicht erst bearbeitet, da ich neben den Schwierigkeiten mit der Anwendung des Programmes die Verschlüsselungsverfahren ab Aufgabe 3 an sich zu schwierig finde, um diese „mal eben so“ zu dechiffrieren.
- E2 Erster Eindruck: Extrem unübersichtlich
 Nutzung für mich überhaupt nur bei sehr kleinschrittiger, extrem expliziter Anweisung möglich – sprich: intuitive Nutzung gar nicht möglich
 leicht zu verstehende Einführung in Kryptographie an sich und in das Programm (Zielsetzung???) fehlt
 Kenntnis vieler Fachtermini der Mathematik/ Informatik/ Kryptographie in engl. Sprache nötig, um die Leiste Algorithm Settings überhaupt nutzen zu können
- E3 Grundsätzlich gute Idee: Den Prozess des Chiffrierens/ Dechiffrierens auf „Knopfdruck“ sichtbar zu machen.
 Auch finde ich z.B. die Visualisierung der Buchstabenverteilungshäufigkeit im Balkendiagramm sinnvoll, da diese sehr eingängig ist.
 Jedoch: Aufteilung der Benutzeroberfläche generell zu unübersichtlich; vor allem stört das Protokollfeld in der unteren Hälfte (Welche Relevanz hat das für das Programm???).
 Generell überlagern sich die Felder störend, sodass man sich erst selbst durch Schließen von Feldern einen orientierenden Überblick ermöglichen muss.
 Durch die Vielzahl an Feldern wird man auf einen Schlag mit einer Fülle unbekannter Begriffe konfrontiert, was einen Einstieg erschwert: Viel zu hohe Informationsdichte! Viel zu viele Details! (Z.B. die unterschiedlich farbigen Pfeile an den Rändern der Textboxen bzw. des Symbols mit der Chiffre.) Reduktion wäre sinnvoll! (Z.B., indem das Protokollfeld und die Namen der einzelnen Verschlüsselungsverfahren nicht sofort erschienen.)

- E4 Überfordert hat mich bereits die Frage, welche Schritte nacheinander auszuführen sind, um die verschiedenen Codes auszuprobieren. (Siehe oben: Schrittweise Anleitung fehlt.)

Hinderlich: Das gleichzeitige Operieren mit der Play bzw. Stop-taste in der Ribbon-Leiste links oben und der Algorithm Setting-leiste rechts ist extrem benutzerunfreundlich! Warum kann man nicht mit Enter die Befehle/Einstellungsänderungen in der Algorithm Setting-Leiste aktivieren?

Generell: Warum müssen die Operationen in der A.S.-Leiste eingestellt werden? Könnte man die Befehle nicht über das Symbol mit der jeweiligen Chiffre (zwischen Klartext und Geheimtext) aktivieren?

Sprich: Mehr Benutzerfreundlichkeit wäre hilfreich. So sollten die Blicke und die Aufmerksamkeit des Nutzers nicht während eines einzelnen Arbeitsschrittes ständig von rechts nach links und zurück springen müssen.

- E5 Ich habe schnell die Lust an einer weitergehenden Beschäftigung mit CrypTool2 verloren, da ich dabei nicht weit gekommen bin: Immer wieder bin ich irgendwo an einer Verständnisklippe (Fachvokabular, Welcher Arbeitsschritt kommt als nächstes?) hängen geblieben bin.

Es lädt insgesamt nicht ein, Dinge auszuprobieren: Zu verwirrend, zu wenig motivierend! Es müsste mehr Anreize bieten, die Lust darauf machen, die verschiedenen Verfahren auszuprobieren!

- E6 s.o.

Zudem: generell eine ansprechenderes Layout – klarere und funktionale Wahl von Farben; für jedes Chiffrierverfahren ein eigenes Icon

Antwort 3:

- A1 Werde bald Lehramtsstudium im Fach Mathematik beenden, hatte Leistungskurs Mathematik im Gymnasium, großes Interesse in das Fach Mathematik, Einschätzung der eigenen Fähigkeit: gut bis sehr gut
- A2 Mehrfache tägliche Benutzung (beruflich wie auch privat), Zweck: Studium, Internet (studivz, Wkw usw.)
- A3 Kenne sie ein bisschen, habe sie aber selbst nicht, komme damit noch nicht so gut zu recht, weil ich selbst kaum ausprobiert habe
- A4 Ich benutze Wikipedia um ein gewisses Grundverständnis aufzubauen, stütze mich aber lieber auf andere Dinge (Buchrecherchen, Dozenten oder sonstiges) um mein Wissen aufzubauen
- A5 Ich habe Erfahrungen, allerdings mehr in Fremdsprachen (Englisch und Französisch) von der Schule aus. Ich arbeite gerne mit Lernprogrammen
- A6 Ich weiß nicht, wo im alltäglichen Leben mit Verfahren der Kryptographie gearbeitet wird. Könnte mir aber vorstellen, dass Computer damit etwas zu tun haben.
- A7 Gartenzaunverfahren? Bin mir nicht ganz sicher
- A8 Kenne mich in diesem Gebiet nicht aus, aber interessant ist es auf jeden Fall. Würde gerne mehr über das ganze Thema wissen. Nicht jedes Verfahren, aber ein paar als Beispiele wären schön.

- E1 Ich hatte keine Probleme, aber das ständige „Stop“ und „start“ war etwas nervig.
- E2 Mir gefällt das Programm sehr gut. Wenn das Thema in der Schule durchgenommen wird, würde ich es verwenden. Wenn auch wahrscheinlich nur mit Oberstufen-Schüler
- E3 Nicht schlecht gemacht. Vor allem modern. Das motiviert auch.
- E4 Überfordert hat mich nichts, ungewohnt war die Benutzung der Schaltfläche (hab ja kein Word 2007 z.b.), aber sonst war alles super
- E5 Ja, ich kann mir vorstellen weiterzuarbeiten, wenn es die Zeit zulässt. Hat viel Spaß gemacht.
- E6: Der Verbesserungsvorschlag wäre das ständige starten und stoppen des Programms. Müsste eine Tastenkombination oder so geben dafür. Wäre einfacher.

Aufgabe 5 wurde aus Zeitmangel nicht bearbeitet.

Antwort 4:

- A1 Leistungskurs Mathematik im Abi, 5. Semester Lehramtsstudium Mathematik in Koblenz.
- A2 Privat: Internet
Uni: Internet, Textverarbeitung.
- A3 Nein, kenne ich nicht.
- A4 Ich nutze Wikipedia zwar schon um mir Informationen zu verschaffen, aber nie als einzige Quelle, es ist ja auch nicht immer alles so richtig, wie es da steht. Im Allgemeinen ist es aber schon nützlich, übersichtlich und meist verständlich formuliert.
- A5 Nein, kann mich noch an ein Französischlernprogramm aus der 8. Klasse erinnern und das war einfach nur langweilig. Danach habe ich selbst nie wieder eins verwendet, habe allerdings für meinen Sohn etwas angeschafft (Grundschule) und er ist doch ziemlich zufrieden damit.
- A6 Wenn man beispielsweise seine Konto- oder Kreditkartenzahlen bei Onlinekäufen angibt, werden diese verschlüsselt übertragen, ebenso beim Einloggen in Emailaccounts oder Kundenkonten.
- A7 Morsealphabet, Blindenschrift, Zeichensprache
- A8 Anwendungsbereiche, Entwicklung

- E1 Ich konnte die Aufgaben nicht so gut lösen. Auch die Anleitung erschien mir oft etwas seltsam und unvollständig. Der Geheimtext lies sich erst nicht einfügen.
- E2 Mir gefällt es nicht besonders gut.
Was schön ist, ist eventuell dass es wohl kostenlos ist, aber das wäre für mich kein ausreichender Grund es zu benutzen.
- E3 Zu viel des Guten, man wird von den vielen Schaltflächen ja schlichtweg erschlagen, ich finde das sehr verwirrend und irritierend. Es ist einfach zu viel und dann ist alles auch noch sehr bunt.
- E4 Mir waren da einfach zu viele Schaltflächen, da hatte ich schon keine Lust mehr, es war mir zu überladen und verwirrend.
- E5 Wenn es sein müsste eventuell, aber ich glaube nicht, dass ich es freiwillig nutzen würde.
- E6 Weniger ist manchmal mehr. Ich finde es ist viel zu bunt und zu unübersichtlich.

Antwort 5:

- A1 Abitur – Mathe Leistungskurs – Mathe in Koblenz auf Lehramt – würde mich selber als begabt bezeichnen
- A2 Internet – E-mails(Kommunikation) – Spielen
- A3 Bekannt, wenn auch nur ganz selten benutzt, war vorher alte „oberfläche“ gewohnt, umgewöhnung nötig – altes wie neues nicht intuitiv, aber durch gewöhnung das alte eigentlich favorisiert (ein grund für OO)
- A4 nutze ich öfter, reicht aber nur in ganz seltenen fällen aus. oft nur als einstieg, weil nicht ausreichend tiefe vorhanden, die weiterführenden links oder google helfen da oft weiter...
- A5 keine erfahrung
- A6 ja!!!!!!!!!! Bankgeschäfte, e-mails, jegliche art von datenübertragung die nicht „rauskommen“ soll.
- A7 RSA
- A8 grundsätzlich interessant, wenn mein interesse in irgendeinem punkt zunimmt informiere ich mich bei wiki, google oder dir ;)

- E1 Benutzung zunächst nicht intuitiv:
1. Start – Stopp Taste vor Änderungen von z.B. Schlüssel
 2. Zuerst unübersichtlich, liegt aber wohl an den Präsentationen, ohne die man aber wieder gar nix verstehen würde
- E2 optisch erstma schöner als der vorgänger
bedienung durch module nicht leichter geworden =>
- E3 Möglichkeiten durch diese „Programmierung“ scheinbar größer (so genau kannte ich den vorgänger net...) aber nicht schnell oder intuitiv zu bedienen...
- E4 Zusammenbringen der nötigen module (aufgabe 5) hat zwar funktioniert, aber im prinzip durch rumprobieren, im anschluss an (korrekten) aufbau klappte die Übersetzung in realtext nur nach viel rumgeklickte, weil schlüsselwort cbm nur groß (CBM) akzeptiert wurde, sinnvoll?
- E5 selbstständig ist schwierig, habe mir die hilfen dokumentationen dazu net angesehen, aber wenn die halbwegs brauchbar sind und ich ganz dolle motiviert bin und rund 3h zeit habe mich einzuarbeiten, dann könnte das wohl klappen...
Ich denke es bietet den vorteil, wie du es gemacht hast, dass das „Programm“ vorgeschrrieben werden kann und der reine Nutzer nur noch texte eingeben braucht und dann die Parameter (schlüsselwort etc) ändern kann.
- E6 die „programmierung“ muss intuitiver sein (frag mich nicht wie, habsch keine ahnung von..)
änderungen in den parametern sollten ohne start-stopp-taste-gedöns möglich sein

Da der Proband Lehramtsstudent der Mathematik ist und Vorkenntnisse in Programmierung, Kryptographie und Didaktik hat, stellte ich ihm noch drei Zusatzfragen :

- F1: Bei der Enigma-Aufgabe (selbständiges Gestalten des "visuellen Programms"):
- wie intuitiv war die Auswahl der Plugins, die Anordnung auf dem Arbeitsplatz, das verbinden der einzelnen Icons mit Linien, etc.
 - sind Dir die verschiedenen Farben der Ein- und Ausgänge der Plugins aufgefallen? Hast Du eine Idee, was sie bedeuten sollen? (bzw. war klar, das die Farben die verschiedenen Datentypen darstellen?)
- A1: überhaupt nicht intuitiv, hat nur durch vorlage von deinen „Programmen“ überhaupt funktioniert
 schon bei eingabefeldern: was jetzt text oder datei oder was???(soll heißen: input alphabetical, file text, clipboard....)
 Pfeile hab ich zufällig bemerkt, wie man die macht...
 Versch farben bemerkt, aber keine ahnung wozu die gut sein sollen!!!
- F2: Was sind die Vor- und Nachteile beim Vergleich der ersten und zweite Version von CrypTool?
- A2: caesar: beim alten ein klick du siehst buchstabenverteilung – beim neuen musst du erst richtiges plugin-ding finden – probieren von buchstaben ist bei beiden mindestens gleichumständlich – neu start stopp, alt immer wieder menü aufrufen...
 vegenere: alt ermittelt nicht nur kennwortlänge, sondern gibt auch ermitteltes kennwort an!!! keine ahnung ob neu das auch kann, aber auf jeden fall nich so schnell
 enigma – keine ob alt das auch kann, auf jeden nicht sofort, aber die einstellungen für neu hätte ich auch nie gewusst(was aber an meiner ahnung über dieses verfahren liegt, das musst du mir sagen!!!!!!)
- F3: Wie ist die Eignung des Programms für Laien? Wo kann es Probleme geben, was fehlt?
- A3: Für Laien völlig ungeeignet: da muss es zur benutzung vorgefertigte programme geben, die evtl durch versch plugins(erweiterungen ~ erklärunigen) manuell ergänzt können werden sollten. (ist der satz klar?!)

Antwort 6:

- A1 Abschluss Gymnasium, Mathe allerdings nicht als Leistungsfach. Im Alltag macht das meiste ja der PC, ich kann aber auch noch so rechnen :-)
Interesse ist auf jeden Fall vorhanden, insbesondere an versch. Einzelthemen (gödel, hatten wir ja schon mal, Unendlichkeit und ihre Erklärung)
Diverse Literatur dazu habe ich, und hab sie auch gelesen.
- A2 beruflich jeden Tag, privat eher nur Internet. Immer aber auf vorgefertigten Programmen.
- A3 Nein.
- A4 Ja, aber nie ausschließlich, außer für Kurzinfos. Erfahrungen bis jetzt waren eigentlich ok.
- A5 Ja, beruflich öfter. Ich persönlich mag sie nicht. Sie sind zu steif, sprechen nicht alle möglichen Kanäle des "lernens" an. Rückfragen, Hintergründe, tiefergehenden Fragen kann man vergessen. Für durchschnittlich schwierige Sachen aber dennoch sinnvoll.
- A6 Ich denke der komplette Datenverkehr im Internet oder Mailwesen ist, wenn er halbwegs wichtig ist (Adressdaten, pers. Daten, Bankdaten) verschlüsselt.
Das ist schon eine ganze Menge !!! Hinzu kommt noch Funkverkehr, Satelitendaten....
- A7 Ich kannte nur die Sache mit Enigma, aber nicht hundertprozentig. Wußte, daß das mit Walzen und Buchstabenverschiebung zu tun hatte.
- A8 Grundsätzlich ja. Interessant wären wohl schwierigere Verschlüsselungen und deren Lösung.

- E1 Die Aufgaben waren durchweg relativ gut beschrieben und somit gut zu lösen. Ein Problem hatte ich mal, da ich vergessen hatte oben links auf Stop zu gehen um eine neue Eingabe zu machen. Irgendwann hab ich es dann aber wieder gefunden. Fehler macht man meistens ja nur ein mal.
- E2 Gefallen.. naja, es ist ein zweckmäßiges Prorgamm, aber recht ansprechend aufgemacht. Je mehr man damit arbeitet, desto besser klappt es. Es macht diesbezüglich keinen besonders positiven oder negativen Eindruck auf mich. Man benutzt es halt.
- E3 Wie oben schon beschrieben, ansprechend aufgemacht, nicht zu bunt (ist aber Geschmackssache). Was mir persönlich gefällt sind die abgerundeten Ecken. Sieht dadurch modern aus.
- E4 Ob es grobe hinderliche oder irritierende Merkmale gibt, dafür muß man vielleicht länger mit dem Programm arbeiten. Für die Anwendungen, die Du beschrieben hast, war das Programm einfach zu handeln. Die Start/ Stop Geschichte hätte ich vielleicht etwas größer oder zentraler gestaltet. Aber wie schon beschrieben, wenn man es einmal weiß, dann kommt man sogar mit einem komplizierten Programm zurecht. Ein kompl. Programm kostet dann nur mehr Zeit, auch wenn man weiß wie es geht. Das kann man hier nicht sagen.
- E5 Ich denke schon.
- E6 Verbesserung..... So direkt jetzt nicht. Als Anwender gewöhnt man sich halt an das, was man vorgesetzt bekommt. Da ich ja jetzt nur kurz mit dem Programm gearbeitet habe, fallen mir zumindest keine groben Dinge auf, die direkt den Arbeitsfluss negativ beeinflussen.

Da der Proband nur eine mathematische und computertechnische Grundbildung hat und, für mich unerwartet, problemlos die Aufgaben bewältigen konnte, stellte ich ihm noch folgende Zusatzfrage:

F: Bei der Enigma-Aufgabe (selbständiges Gestalten des "visuellen Programms"):

- wie intuitiv war die Auswahl der Plugins, die Anordnung auf dem Arbeitsplatz, das verbinden der einzelnen Icons mit Linien, etc.
- sind Dir die verschiedenen Farben der Ein- und Ausgänge der Plugins aufgefallen? Hast Du eine Idee, was sie bedeuten sollen? (bzw. war klar, dass die Farben die verschiedenen Datentypen darstellen?)

A: Bei der Schwierigkeit von Aufgaben kommt es natürlich immer auf die eigene "Schmerzgrenze" an.

Wann empfinde ich etwas als schwierig, wann nervt es, wie groß ist mein "Lösungsergeiz".

Ich war natürlich nicht in 5 Minuten fertig beim ersten mal mit der Enigma Aufgabe, ich empfand es aber als lösbar. Wenn man mit cem 64'er aufgewachsen ist dann hat man ja manchmal diese "Try and Error" Mentalität. Ich habe mir gesagt, ich löse das und es ging auch. Insgesamt denke ich so 15 Minuten bis 20 Minuten beim ersten mal, empfand ich persönlich nicht als nervend.

Beim zweiten mal habe ich es aus dem Kopf gemacht in ca. 1 Minute. Parameter gab es ja nicht so viele bei der Enigma Einstellung, konnte man also beim zweiten mal auswendig.

Wo liegen jetzt die Unterschiede. Ich versuche mich mal an der Aufgabenstellung und an Deinen Fragen entlang zuhangeln.

Erst mal habe ich überlegt, was bedeutet es ein neues Arbeitsblatt zu erstellen. Ich dachte zunächst tatsächlich an ein DIN A4 da Du mit der Post ein leeres DIN A4 mitgeschickt hattest, wahrscheinlich Zufall.

Ich entschied dann die Aufgabe weiterzulesen, obwohl man ja denkt, wenn ich Punkt 1 nicht habe, was soll ich mit Punkt 2. Ok, war dann klar nach dem Befehl "new".

Also leeres Blatt, links Enigma anklicken war auch klar. Jetzt war mir auch klar was mit visuellem Programm gemeint war.

Aus den Aufgaben vorher war mir noch im Gedächtnis dass ich ja ein Eingabefenster brauche, das war dann die Sache mit den Tools, stand ja auch in Aufgabenstellung. Also Text markieren, kopieren einfügen. Ausgabe habe ich etwas länger gesucht, obwohl die Dinge ja gebündelt waren unter inputs und outputs, ich glaube ich hatte auch mal den falschen output gewählt, später habe ich dann gesehen dass ich einen "Textoutput" brauche.

So, dass waren die Symbole. Das verbinden war nirgends erwähnt, die Striche aus den vorherigen Aufgaben hatte ich schon verdrängt.

Erst mal auf "go" nix passiert ! 10 mal auf Enigma gedrückt um die Parameter einzugeben, nix passiert. Dan fiel mir ein, dass man das am rechten rand macht. Ok, war dann einfach. Go, nix passiert. Allein vom Anblick her könnte man die Kästchen mal verbinden, die Farben führen einen ja... Enigma mit Ausgang geht nicht, trotzdem "go"... Ah, da war noch was mit Ausgabeparameter, ok geändert , Enigma mit Ausgäbe verbunden, dann kam die Geschichte und Funktionsweise der Enigma : FREUDE.

Die Handhabung ist wirklich einfach, input, rechnen, output. Wir haben ja früher noch Ablaufdiagramme in der Schule gemalt. Hat mir geholfen.

Die Anordnung links ist ok, sehr viele Auswahlmöglichkeiten, dehalb bin ich drübergehuscht und habe beim ersten mal gepatzt. Aber wenn es so viele Unterpunkte gibt, ist das halt so. Verbinden der Element ist super einfach, man muss nur wissen, dass man es machen soll.

Die verschiedenen Farben sind mir aufgefallen, daß die verschiedenen Datentypen darstellen ist mir zunächst nicht bewusst gewesen. Erst als ich den Output mit der falschen Farbe hatte, hatte ich eine Vorstellung davon, daß hier noch irgendwas falsch sein muss.

Später habe ich dann gesehen, dass die Pfeilspitzen beim überfahren mit dem Mauszieger mit den Datentypen hinterlegt sind.

Wenn man es dann geschafft hat, ist es wohl immer einfach, locker leicht wäre aber übertrieben. Man muss schon lesen und sich darauf konzentrieren was man da macht, aber ok. Eigentlich war ja alles vorgegeben in der Aufgabenstellung.

Antwort 7:

A1: Sekundarabschluß I, Noten: gut bis befriedigend, vor 22 Jahren.

Mein mathematisches Verständnis beschränkt zur Zeit auf die einfachen Rechenarten. Im Alltag nutze ich es hauptsächlich für Kalkulationen und Betriebswirtschaftliche Auswertungen.

Ich habe eigentlich ein gutes Zahlenverständnis, ist aber seit der Schule nicht weitergebildet worden.

A2: Ich nutze den MAC (kein PC), hauptsächlich beruflich für Erstellung von Dokumenen Präsentationen und Vorträgen, unter starker Einbeziehung von Email und Internet.

Privat für Dokumente, Bilder, Email und Internet.

A3: Ich habe damit in meinem letzten Unternehmen gearbeit und kam damit zurecht, wir hatten es erst kürzlich umgestellt, bevor ich ging. Ich arbeite ansonsten mit einer älteren Version Office for Mac, hauptsächlich aber mit Powerpoint, Excel, CS Indesign.

A4: Ja oft und habe gute erfahrungen damit.

Allerdings nutze ich es als einstieg, um dann über Literatur mich einzulesen.

A5: Wenig Erfahrung, arbeite aber ganz gerne mit Ihnen.

A6: Ja, z.B. im Bereich von Übertragung von Passwörtern, Homebanking

A7: Nein, keine aktuellen.

A8: Ja, da es in der heutigen Zeit immer wichtiger wird.

Antwort 8:

Ich gestehe gleich zu Anfang: Ich bin bei CrypTool an meine Grenzen gestossen. Natürlich habe ich die Darstellungen verstanden und auch die Bildaufbereitung war sehr ansprechend, aber ich habe eben nicht nachvollziehen können, was da passiert. Ich habe die Programme und deren Funktionsweisen nicht verstanden. Vielleicht liegt es einfach daran, dass ich die Umsetzung im Alltag nicht benötige und daher relativ schnell bei Unverständnis die innere Bereitschaft zur Auseinandersetzung mit der Materie schweindet (wie früher in der Schule - muss ich das wissen?).

Hier meine Antworten:

- A1 Ich verfüge über Fähigkeiten der Alltagsmathematik.
- A2 Ich arbeite täglich mehrere Stunden am PC. Hierbei verwende ich neben der Internetsuche vorwiegend ein Schreibprogramm.
- A3 Nein, da ich mit einem anderen Programm arbeite.
- A4 Ja, sehr oft. Allerdings nutze ich die Erklärungen nur zur ersten Information. Besonders hilfreich sind mir darüber hinaus die Links und Quellenangaben bei Wikipedia.
- A5 Ich verfüge über keine neueren und aktuellen Erfahrungen mit Lernsoftware. Die letzten Begegnungen mit Lernsoftware hatte ich vor wenigen Jahren mit meinen Söhnen. Hier fand ich die Angebote für Kinder sehr interessant.
- A6 Banken und andere Stellen, die sensible Daten weitergeben, arbeiten mit der Verschlüsselung von Daten. Auch beim eMail-Verkehr ist die Verschlüsselung von Daten ein Thema.
- A7 Nein.
- A8 Hier habe ich noch nicht darüber nachgedacht. Vielleicht ist mein Vertrauen in das Funktionieren der Datenverschlüsselung auch einfach zu groß. Möglicherweise wäre es besser, manchen Vorgang selbst überprüfen zu können.

- E1 Hier bin ich regelrecht gescheitert. Ich habe zwar die Anleitungen und auch den Bildschirm verstanden, aber mit der Umsetzung kam ich nicht zu Recht.
- E2 Das Programm ist optisch gut aufbereitet. Die einzelnen Schritte sind nachvollziehbar dargestellt. Die Erläuterungen sind hilfreich.
- E3 Gut.
- E4 Ich habe zunächst längere Zeit für die Installation des Programms benötigt (was allerdings auch an meinem PC liegen kann). Das hat mich genervt und zugleich meine Bereitschaft zur tieferen Auseinandersetzung getrübt.
Die Darstellung der Gesamtheit des Vorganges auf einen Blick war ebenfalls irritierend bzw. gewöhnungsbedürftig. Zugleich aber sehr spannend.
- E5 Nein!
- E6 Ich bin Alltagsmathematiker, was könnte ich an Vorschlägen unterbreiten, die sinnvoll und logisch wären? Nein, ich habe keine Vorschläge.
- Da der Proband schreibt, bei CrypTool 2 an seine Grenzen gestossen zu sein, es aber als ansprechend und optisch nett aufgemacht empfindest und auch keine Verbesserungsvorschläge hat, formulierte ich eine weitere Frage:
- F: Was müsste das Programm können (bzw. was fehlt an dem Programm), um DIR ein Erkenntnis-reiches Arbeiten damit zu ermöglichen?
- A: Allerdings stellt sich für mich immer wieder die Frage, muss ich das Programm kennen und beherrschen?
Mir fehlen aber vor allem kurze und knappe Erläuterungen und Hilfestellungen, wenn ich "hänge". Und, der Einstieg in die Lernphase des Programms müsste spielerischer gestaltet werden. Vielleicht auch am Beispiel einer typischen Bankverschlüsselung.
Letztendlich denke ich natürlich zu viel und frage mich, ob Hacker etc. bei intensiver Kenntnis dieser Dinge nicht in der Lage sind, meine verschlüsselten Daten zu entschlüsseln. Hier müsste vielleicht auch eine Info erfolgen.

Antwort 9:

- A1 Schulabschluss: Abitur, Leistungskurs Mathematik, BWL, Deutsch
 Studienabschluss: LA RS Uni Koblenz Mathematik,
 Wirtschaftswissenschaften
 Anwendung: Täglicher Einsatz in der SEK I, sowohl Realschule als
 auch Hauptschule
 Interessen: hauptsächlich die geschichtliche Entwicklung der
 Mathematik in den asiatischen Ländern
 Einschätzung: im Bereich der SEK I kompetent
 Durch fehlende Impulse und Diskussionspartnern außerhalb der Schule wenig
 Streben nach „höherer“ wissenschaftlicher Mathematik
 Weiterbildung hauptsächlich im didaktischen Bereichen, sowie Verknüpfung
 des Faches Mathematik mit anderen Fächern.
- A2 Den PC nutze ich um Emails zu schreiben und zur Recherche von aktuellen
 Themen, Materialien, etc. für das Fach Sozialkunde. Des Weiteren nutze ich
 ihn um Arbeiten zu konzipieren sowie sonstige Materialien für diverse
 Unterrichtszwecken zu erstellen.
- A3 Diese Abbildung der Leiste kenne ich so nicht. MacOffice benutzt eine sehr,
 sehr ähnliche Schaltleiste. Die PCs in der Schule verwenden Office XP.
- A4 Für die Schüler ist es sehr hilfreich, da Einleitung meistens sehr einfach und
 übersichtlich strukturiert ist.
- A5 Nein, durch diverse technische Defekte und mangelnde Einrichtungen ist eine
 Aussage zum Einsatz nicht möglich.
- A6 Ja, vgl. die Inhalte der Vorlesung Schröder
- A7 RSA, Viginere, Caesar, WEP, Block-Chiffre,....
- A8 Das Gebiet ist sicher interessant jedoch nicht so interessant um sich weiter
 damit zu beschäftigen. Mich interessieren Weiterbildungen, Einzelheiten im
 Bereich der Schulanwendungen diverser Methoden im Mathematikunterricht.

- E1 Problemlos, die Schritte konnten gut durchgeführt werden, da selbsterklärend. Durch learning by doing und etwas „herumspielen“ um einige Funktionen im Voraus zu testen, konnten die Aufgaben gut gelöst werden.
- E2 positiv: sehr gute Übersicht, verbesserte Bedienbarkeit durch Anlehnung an MS Office. Graphische Aufbereitung durch Datenflussdiagramme, weniger Fenster – bei Eingabe und Auswertung haben sich bei älteren Versionen viele Fenster geöffnet, ging zulasten der Übersichtlichkeit
Negativ: viele Funktionen, die im Normalbetrieb gar nicht alle angewendet werden können (Schulbetrieb: Programm nur auf englisch – Entwicklungsstand von Schülern kann vielleicht nicht ausreichen?!)
- E3 Nach kurzer Eingewöhnungszeit ist das Programm gut strukturiert. Durch die Anlehnung an MS Office ist ein Transfer der Basics / Funktionen in CrypTool sehr leicht.
- E4 Man muss sich mit dem Programm auseinandersetzen, dann kann man die gestellten Aufgaben lösen.
- E5 Für eine Weiterentwicklung fehlen mir die notwendigen technischen Ressourcen und auch das Know-how.
Das Weiterarbeiten mit diesem Programm ist durchaus gewährleistet. Ich sehe keine großen Probleme, aber vgl. E6
- E6 Da Das Programm nicht auf meinem MAC läuft, ist der Anwendungsbereich sehr eingeschränkt und ich werde das Programm insofern es keine AG in der Schule zu diesem Thema gibt nicht weiter verwenden.

Antwort 10:

- A1 Ich denke ich verfüge über recht gute Kenntnisse im Fach Mathematik. Ich studiere seit mittlerweilen 5 Semestern Mathematik an der Universität Koblenz. Angestrebter Studienabschluss ist das Lehramt an Realschulen.
- A2 Am meisten verwende ich den Computer zu privaten Zwecken: Ich höre viel Musik, mache aber auch selbst Amateuraufnahmen mit halbwegs professioneller Software, außerdem schaue ich viele Filme mit dem Rechner und surfe ständig im Netz und nutze regelmäßig Instant Messenger (Skype, ICQ).
- Im Rahmen meine Studiums verwende ich den PC zur Anfertigung von Porwer-Point Präsentation und zum Verfassen schriftlicher Ausarbeitungen.
- A3 Ich ahne schlimmes, ist das die Leiste von dem neuen Office??
Nunja, ich bin was so was angeht etwas konservativ. Ich benutze auch noch das klassische Windows Design und habe noch Office XP im Betrieb. Wenn ich denn mal auf einem neuen Vista Rechner dazu gezwungen bin dieses Office zu nutzen, dann bekomm ich die Krise. Finde das etwas verwirrend, weil ich das „alte“ Design gewöhnt bin. Ich glaub aber schon das ich damit klar kommen könnte. Ich kenne die Leiste aber kaum.
- A4 Um schnell mal was in Erfahrung zu bringen schau ich oft in Wikipedia. Wenn ich aber wirklich wissenschaftlich korrekt arbeite verlasse ich mich nur sehr ungern auf Wikipedia, da ich mir nie sicher bin, ob das was da steht so stimmt. Aber grundsätzlich halte ich Wikipedia für eine gute Informationsquelle, die durchaus geeignet ist, um sich einen Überblick über bestimmte Sachverhalte zu verschaffen.
- A5 Fast noch keine. Ich lasse mich am PC schnell durch Dinge ablenken, deswegen fällt es mir grundsätzlich schwerer mich für eine längere Zeit auf etwas zu konzentrieren. Deswegen glaub ich das Lernsoftware für mich nicht das optimale Mittel wäre. Aber ich denke man kann mit Hilfe solcher Software viele Dinge schön grafisch veranschaulichen.
- A6 Heute morgen habe ich im Saturn mit ner EC Karte bezahlt. Die Übertragung meine PIN an die Bank Zentrale und die gesamte Kommunikation zwischen Kasse und Bank läuft, so hoffe ich zumindest, verschlüsselt ab. Im Internet kommuniziert mein eMailprogramm mit dem eMail Server verschlüsselt. Mit manchen Portalen im Internet (z.B. eBanking) baut man eine verschlüsselte Verbindung auf.
Im Prinzip komme ich mit Kryptographie jeden Tag in Berührung.
- A7 Hmm, nicht wirklich. Ich glaub es wird viel in verschiedenen b-adischen Systemen gearbeitet (Hexadezimalsystem, etc.)
- A8 Ja! Ich würde gerne ein Verfahren kennen lernen. Mehr darüber erfahren wie sicher das ist. Interessant finde ich auch immer wieder Erzählung wie während das 2. Weltkrieges Daten verschlüsselt wurden und wie Codes geknackt wurden, bzw. Deschiffrierer in fremde Hände geraten sind ☺
Auch Hacking im Internet find ich interessant.

- E1 Die Anleitungen waren recht ausführlich, die Bedienung des Programms nachvollziehbar, am Anfang hatte ich das Problem, dass ich den „Algorith Settings“ Button nicht gefunden hab, da der doch recht unscheinbar am Rande platziert ist. Aber hab den dann auch schnell gefunden.

Aufgabe 1 fand ich sehr einfach und das Verschlüsselungsprinzip habe ich schnell verstanden. Zuerst wusste ich nicht, wie ich das dechiffriere, da mir nicht sofort klar war, welches der häufigste Buchstabe in der deutschen Sprache ist, habe dann aber einfach in der Vorlage in der Analyse des Klartextes nachgeschaut und dann bin ich schnell auf das E gekommen und hab dann zurück gerechnet um wie viel Buchstaben das ganze verschoben wurde.

Bei der Vigenere Verschlüsselung habe ich noch nicht ganz verstanden wie das funktioniert. Zuerst dachte ich, es werden nur Buchstaben aus dem Kennwort verwendet, aber das stimmt ja auch irgendwie nicht. Mir ist auch nicht klar, wie die Buchstaben dann einzeln genau verschoben werden. Wenn ich also das Wort „efgh“ habe und das Kennwort „abcd“, dann wird daraus: egik ? Also wird der Buchstabe bei 1 um nix verschoben, bei b um 1, bei c um 2 und bei d um 3 und das ganze wird dann analog gemäß der Stellung des Buchstabens im Kennwort auf das zu verschlüsselnde Wort übertragen? Wie ist es mit einem kürzeren Schlüssel, wenn ich zum Beispiel „efgh“ verschlüssle mit ab, e bleibt, f wird um eine Stelle verschoben, verwende ich dann bei g wieder dass a zum verschlüsseln, also fange ich beim Kennwort von vorne an? Ich schau grad mal, vielleicht wird es mir klar wenn ich noch mal in den Text schau, ok, ich glaub ich hab grad beim erklären so halb verstanden. Aber das ist mir auch erst nachdem ich das Kennwort wusste klar geworden. Ohne deinen Tip und ohne das Kennwort wäre ich nicht dahinter gekommen, wobei ich habe auch grad in der Vorlage gescheut mit dem Kennwort (GEHEIMWORT). Nunja, es geht, aber es ist etwas knifflig. Fand ich erstmal schwierig nachzuvollziehen mit deinen Angaben. Aber dies zwingt einen wiederum auch selber mal seinene Kopf anzuschalten. Jetzt ist mir auch klar, warum pssst ein schlechtes Kennwort ist, weil bei 3 Buchstaben hintereinander die Verschiebung gleich bleibt, das ist natürlich nicht so gut, wie wenn sich die Verschiebung unterscheiden würde.

Die letzte Aufgabe E4 erschien mir nachvollziehbar, da gings ja nur darum, dass Schaubild zu verstehen und zu kapieren wie das Prinzip funktioniert. Das war mir schon einleuchtend.

- E2 Das Programm ist auf den ersten Blick irgendwie ein wenig, nunja trocken! Also keine aufwendigen Designs, bunte Buttons, Schnick-Schnack. Es wirkt nicht so einladend für denke ich viele User, die jetzt grade auf so was stehen, also Schönheit von Programmen. Für mich persönlich ist das aber OK, da ich wie schon bereits erwähnt eh kein Fan davon bin, mir geht's eher um den Nutzen eines Programms, und da ich die Bediehnungseleme, die in den Aufgaben gebraucht wurden, schnell verstanden habe, denke ich, ist das Programm darin gut. Ich finde aber, dass die Play/Stop Leiste da oben etwas unglücklich ist. Man ist das eben so gewohnt, dass so eine wichtige Taste unten in der Mitte, groß ist.
- E3 Vieles habe ich dazu ja schon in E2 geschrieben. Die Diagramme und Schaubilder, die in der Mitte entstehen finde ich gelungen und dass der codierer, bzw. Decodierer als Box in der Mitte dargestellt wird halte ich für sehr sinnvoll. Die Wege, die ein Text durch den Codierer bis zum Codierten Text geht, werden durch die Verbindungslien sehr gut deutlich. Auch machen die Verbindungslien deutlich wo die verschiedenen Analysen greifen, also ob sie am codierte oder uncodierten Text druchgeführt werden. Wie schon gesagt ist das Programm nichts für animationsverliebte, designliebene Menschen/Schüler. Vielleicht werden diese Nutzer ein wenig abgeschreckt, aber ich glaube dass zuviel Schnick Schnack bei einer Lernsoftware auch nicht gut ist.
- E4 Überfordert eigentlich nichts, gewundert: das mit dem Play Butten, Platzierung mancher Buttons. Hinderlich: Ich habe einen kleinen Bildschirm und musste die Analysen stets anpassen, sodass ich alles lesen konnte. Manche Sachen wurden dann recht klein, aber man kann nicht alles haben, im Prinzip hat es gut funktioniert.
- E5 Ja, ich denke ich könnte damit arbeiten, wenn ich noch ein wenig mehr darüber erfahren würde, wie man ein solches Arbeitsblatt gestaltet. Aber ich denke, da lässt es sich reindenken.
- E6 Keine gravierenden, kommt auf die Zielgruppe an. Jenachdem könnte man was am Design machen, sodass das Programm insgesamt etwas attraktiver wirkt. Über die Platzierung mancher Buttons lässt sich streiten. Ich persönlich halte dies nicht für unbedingt notwendig. Aber wenn Schüler damit arbeiten, oder Menschen die nicht so viel mit PC'S am Hut haben könnte das sinnvoll sein.

Antwort 11:

- A1 Ich habe die Realschule mit Mathe 2 abgeschlossen. Meine Kenntnisse sind nach meiner Einschätzung durchschnittlich. Nicht zuletzt dadurch, dass mir Taschenrechner und Computer das bisschen Mathe, das ich benötige, noch abnehmen. Ich arbeite in einem Steuerbüro. Mathematische Fähigkeiten sind hier nicht wichtig. Mathematische Grundoperationen und Prozentrechnung reichen meistens aus. Wichtig sind aber logisches Denken und logische Operationen in der Tabellenkalkulation.
- A2 Beruflich: PCs sind mein tägliches Brot. Ohne Computer geht gar nichts. Genutzte Software sind Steuer- und Finanzwirtschafts-Programme, Office-Programme, Rechtsdatenbanken, email und Internet.
 Privat: In meiner Freizeit nutze ich den PC überwiegend für email-Korrespondenz und Internet-Informationsbeschaffung, Onlinebanking, Online-Einkäufe, Bildbearbeitung und –archivierung aber auch für Software und Betriebssystemtests, also des PCs selbst wegen. Ist ein großes Hobby von mir. Ich nutze den PC also auch täglich zu privaten Zwecken (aber kein Wort ans Finanzamt..). Bis zu mehreren Stunden, wenn ich die Zeit dazu habe, meist aber eher eine Stunde pro Tag.
- A3 Sie sind mir vom privaten PC bekannt. Einige Arbeiten gehen mir dadurch leichter von der Hand. Manche andere Funktionen, die ich aus älteren Office-Versionen kenne, muss ich erst umständlich suchen. Manche Funktionen habe ich gar nicht mehr wieder gefunden. Sehr negativ finde ich, dass man nicht einfach eigene Ribbons für die häufigsten Funktionen erstellen kann. Hier steht leider manchmal Optik vor Funktion. Das Add-On von Ubit bringt wenigstens teilweise Abhilfe: <http://www.ubit.ch/software/ubitmenu-office2007/>
- A4 Ich finde Wikipedia hervorragend. Die Qualität der Artikel, die ich mir bisher angesehen habe, war weitaus überwiegend sehr gut. Die Informationsbeschaffung gestaltet sich damit sehr schnell und flexibel. Es gab ein paar wenige Themen, die ich nicht optimal erläutert fand. Die waren aber Themen, die ohnehin kontrovers diskutiert werden.
- A5 Ja. Ich arbeite nicht gerne damit. Meistens ist der Ablauf fix vorgegeben. Das Lernen ist unflexibel und nervt mehr als es hilft. Es entspricht einfach nicht meiner Lernmethodik. Allerdings habe ich nur Lernprogramme bezüglich rechtlicher Themen und zu EDV-Themen kennen gelernt.
- A6 Onlinebanking, SSL-Websites, Smartcards, Bankkarte. Wenn ich mit Doro rede und Jolanda es nicht mitbekommen soll, reden wir manchmal englisch...
- A7 Nicht im Detail.
- A8 Interessant ist übertrieben. Ich interessiere mich mehr für die Anwendung – weniger für den technischen Hintergrund. Ich finde das Thema aber allgemein sehr wichtig. Mich würde die einfache Umsetzung im PC-Alltag interessieren: z.B. email und Datenverkehr verschlüsseln.

- E1 Nach einer gewissen Eingewöhnungsphase klappte der Umgang mit dem Programm an sich ganz gut. Mit jeder neuen Aufgabe brauchte ich aber mehr Anläufe, um zu einem Ergebnis zu kommen. Schließlich habe ich dann ganz abgebrochen. Ich vermute aber, dass das weniger am Programm, sondern mehr an der Thematik liegt.
- E2 Das Programm ist nicht ganz so starr, wie die Lernprogramme, die ich kenne. Das finde ich sehr positiv.
- Nicht gefallen hat mir, dass die Daten in den Fenster erst „zurecht rücken“ muss, um einen Überblick zu haben, obwohl eigentlich genug Platz auf dem Bildschirm wäre, so z.B. das Fenster bei der Caesar-Datei. Die Algorithm-Settings klappen sich standardmäßig wieder zu nach jeder Einstellung. Ich habe eine Weile gebraucht um zu sehen, dass man diese Optionen „festpinnen“ kann. Vielleicht liegt auch an der Bildschirmauflösung meines Laptop (1680 x 1050).
- Ich bin auch nicht wirklich zufrieden mit dem Programmablauf. Ich bin jemand, der gern erst mal ein bisschen spielt und probiert, ohne vorher ein Handbuch zu wälzen. Ich konnte auf diesem Wege nichts mit dem Programm anfangen. Glücklicherweise hatte ich über den beiliegenden Fragebogen aber auch eine klare Anleitung zur Hand, wie die Dateien zu bearbeiten sind. Damit ging es dann. Ohne die hätte ich das Programm nicht nutzen können. Für einen Kryptografie-Einsteiger zum Selbststudium ist das Programm nicht (gut) geeignet. Ich kann mir jedoch vorstellen, dass es im Rahmen von Vorträgen und Workshops gute Dienste leistet.
- Fazit: Wow. Tolles Fahrzeug mit eindrucksvollem Design. Die Karosserie, der glänzende Lack und die breiten Reifen machen was her. Und der hat ganz bestimmt einiges unter der Haube. Leider kann ich nicht Schwertransporter fahren und brauche einen Fahrlehrer mit Spezialausbildung, der sich mit dieser Art Fahrzeug auskennt und jede Menge Fahrstunden.. Ich überlass das lieber anderen ;-)
- Kurz gesagt: Die meisten Normalbürger verstehen von Kryptografie soviel wie von Quantenphysik und möchten das auch nicht ändern. Es stellt sich die Frage nach der Zielgruppe. Wenn es das sehr ambitionierte Ziel des Programmes war, einem Jedermann Kryptografie per Selbststudium nahe zu bringen, dann erreicht es das Ziel leider nicht. Für Menschen, die beruflich mit der Thematik zu tun haben (sollen), vermittelt es allerdings wichtige Hintergründe.
- E3 Die Farben sind angenehm gewählt und dem MS Office 2007 nachempfunden. Optisch gefällt mir das Programm grundsätzlich gut. Aber: Die Elemente auf der Arbeitsoberfläche nutzen den vorhandenen Raum nicht aus, sodass man sich die in den Fenstern vorhandenen Daten erst zurecht rücken muss. Danach sind sie sehr klein. Im Aufgabenblatt Nr.1 :“schieben Sie die Schiebereglung so, dass Sie die Auswertung komplettsehen..“. Das könnte man besser regeln.

- E4 Überfordert und ermüdet hat mich die Thematik. Wie eingangs erwähnt: Ich finde die Anwendung der Kryptografie wichtig, das Handling für den Alltag zu üben über ein Programm. Erfrischend ungewohnt war die Art und Weise, wie man mit dem Programm arbeitet. Hinderlich ist, dass es für Newbies keinen roten Faden im Programm gibt (oder dass ihn ein Newbie nicht findet). Das Programm animiert den Anwender nicht, Dinge auszuprobieren oder anzuwenden. Verwirrend ist für den ein oder anderen sicher auch, dass das Programm (Textfelder und Schaltflächen) teilweise in Englisch, teilweise in Deutsch beschriftet sind.
- E5 Nein. Ohne vorgegebenen roten Faden wüsste ich nicht, wie ich mit diesem Programm weiter machen sollte. Es ist mir auch zu anstrengend. Ein Stück weit liegt das aber vielleicht auch an der Thematik.
- E6 Es sollte einen Modus geben für absolute Neulinge, mit rotem Faden, der die möglichen nächsten Schritte anzeigt. Dieser Modus sollte kontextbezogene Hilfe und Anregungen anbieten. Bei Steuerprogrammen nervt mich das immer, weil ich weiß, was ich will und wie ich will und es in einigen Fällen bewusst nicht so machen will, wie die Maschine. Bei Kryptografie fänd ich das sehr angenehm, weil mir das Thema völlig fremd ist. Ein Präsentationsmodus für die verschiedenen Verschlüsselungstechniken und Programmfunctionen wäre für mich auch hilfreich gewesen. Einfach dran setzen und loslegen geht bei diesem Programm nicht. Gerade das wäre aber nötig, um solch ein (für den Laien) schwieriges Thema nahe zu bringen.

Antwort 12:

- A1 mündliche Abiturprüfung in Mathe, studiere Mathe
- A2 beruflich keine Nutzung, Nutzung des Computers regelmäßig für Hausarbeiten, Mails, Internet etc.
- A3 Habe kein Microsoft Office 2007, sondern Vista, komme mit der Funktionskeiste aber gut klar
- A4 Nutze die Erklärungen aus Wikipedia ab und zu, habe sowohl gute als auch schlechte Erfahrungen damit
- A5 Habe Erfahrungen mit Derive und verschiedenen Vokabeltrainern und erachte diese sowohl als hilfreich als auch als sinnvoll
- A6 Ja, kenne aber sicher nicht alle Bereiche
- A7 Daten können z.B. mit Hilfe von Zahlen verschlüsselt werden
- A8 Finde das Gebiet interessant und würde gerne mal ein paar Verschlüsselungsverfahren näher kennen lernen und ggf selbst etwas verschlüsseln

Die Aufgaben des Fragebogens wurden wegen nicht näher genannter Probleme mit der Bedienung von CrypTool 2 nicht bearbeitet.

7.5. Graphiken zur „Krypto-Entwicklung“ von H. Witten

Veröffentlicht als Präsentation von Helmut Witten unter dem Titel *Die wichtigsten Verfahren der Kryptologie* auf <https://www.cryptoportal.org/>

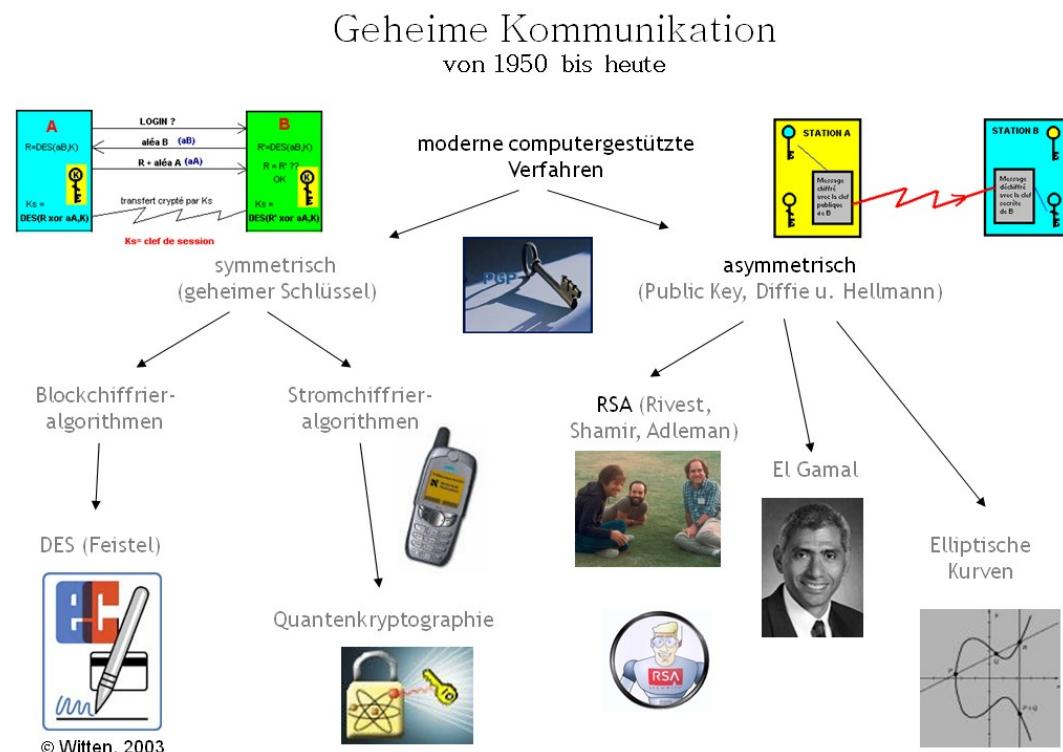
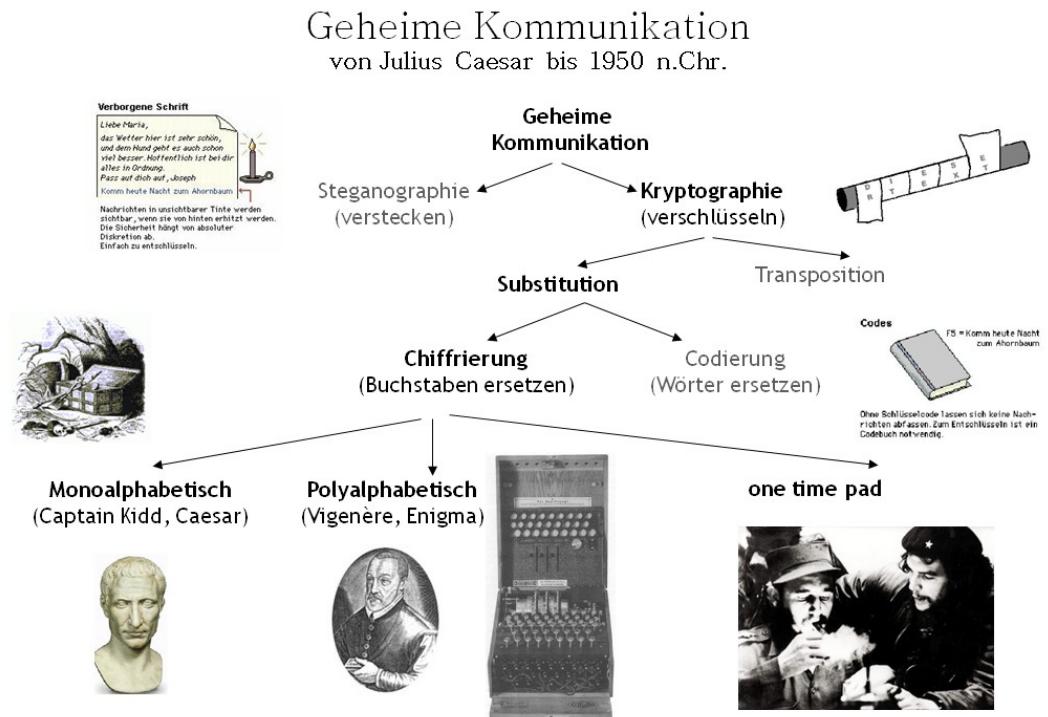


Abbildung 43: H. Witten: Geheime Kommunikation

7.6. Entwurf zu Startcenter und visueller Programmierung

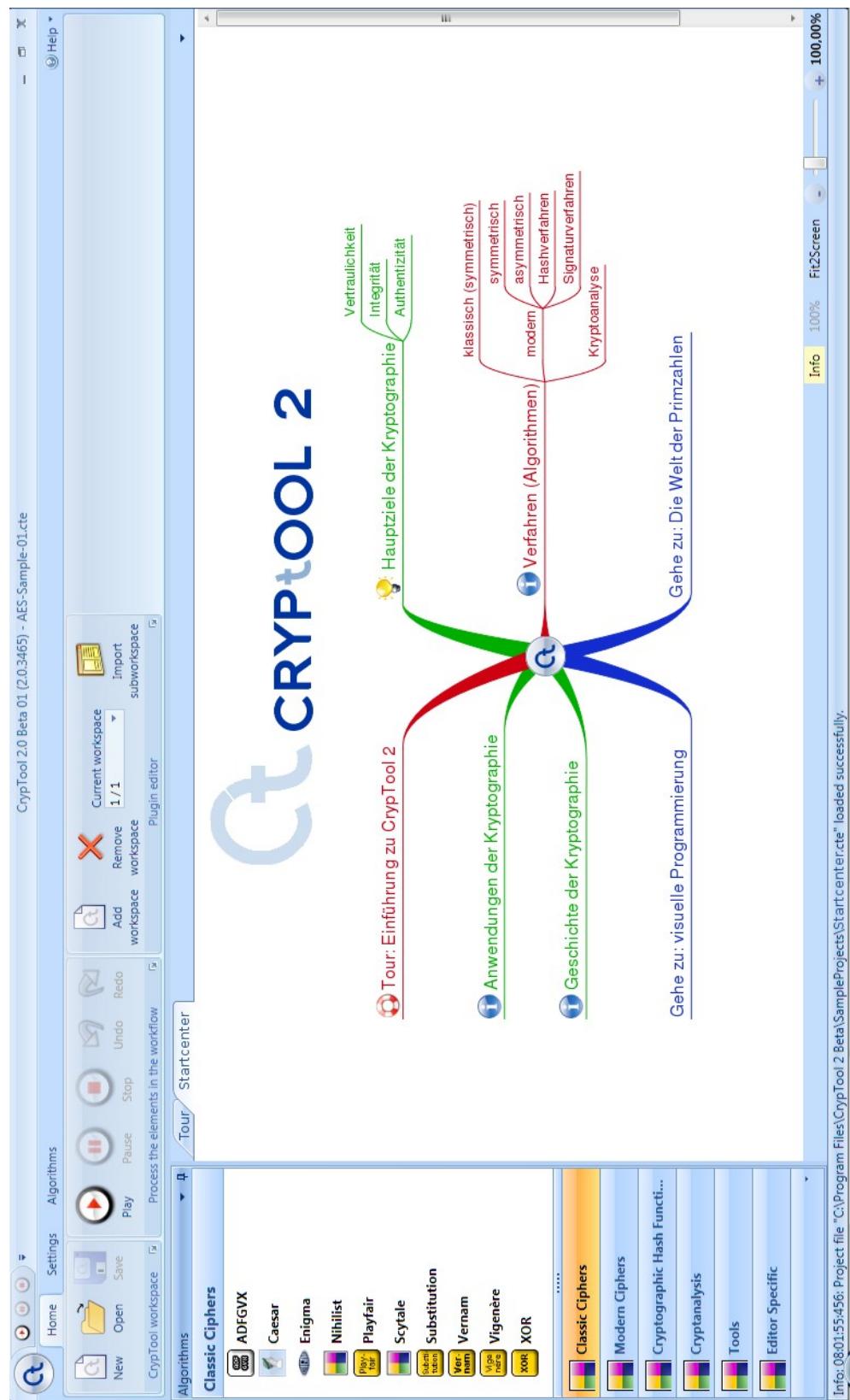


Abbildung 44: Vorschlag zu einem Startcenter für CrypTool 2

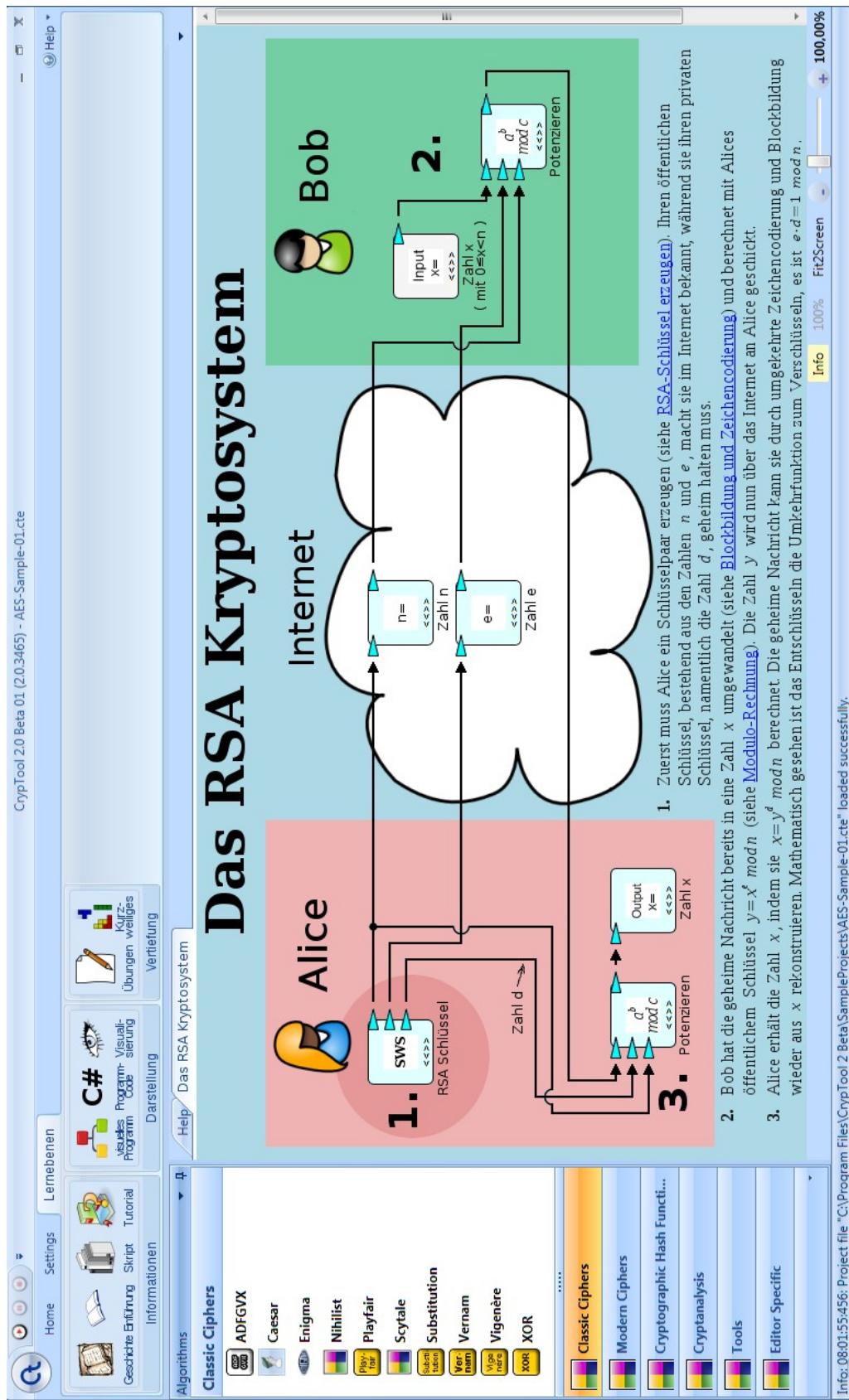


Abbildung 45: Workspace: Das RSA Kryptosystem

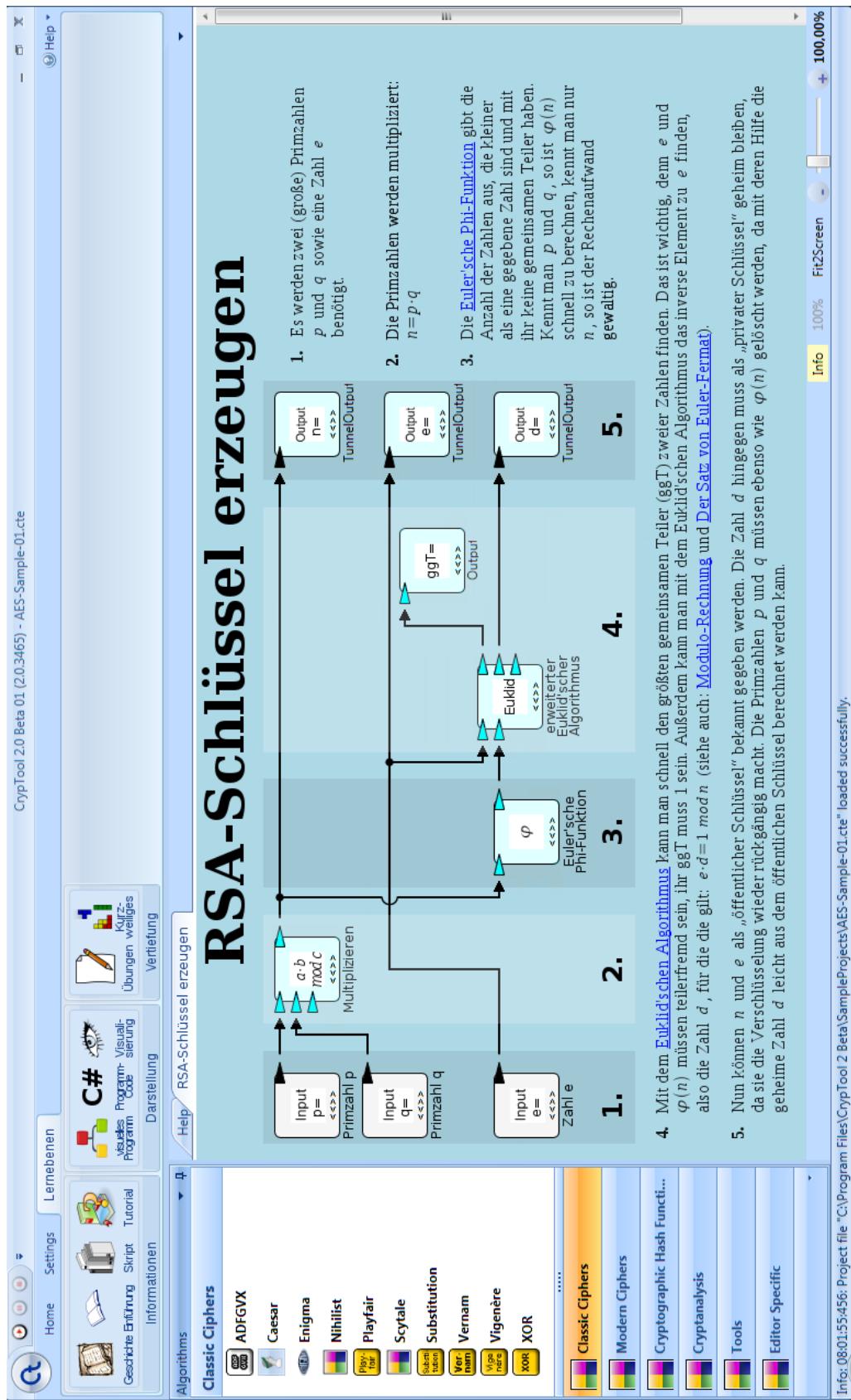


Abbildung 46: Workspace: RSA-Schlüssel erzeugen

7.7. Teilnahmebestätigung HRPI-Fortbildung



7.8. Versicherung

Ich versichere, dass ich die Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Welschneudorf, den 5. November 2007

A handwritten signature in blue ink, appearing to read "Christian Geyer", is written over a horizontal line.