

Bachelorarbeit

CrypTool 2/Learn-CrypTool

Erstellung eines HTML 5-basierten elektronischen
Lerntagebuches zur Unterstützung und Motivation von
AnfängerInnen für das Softwareprogramm
CrypTool 2

FB4 Informatik an der Universität Koblenz-Landau
Institut für Computervisualistik
(AG Computervisualistik)

Gutachter: Prof. Dr. Karin Harbusch

vorgelegt von Alyona Byelaya/Mtr. Nr. 207200030/belaya@uni-koblenz.de

11.Juni.2014

Eigenständigkeitserklärung

Hiermit bestätige ich, Alyona Byelaya (207200030), dass die vorliegende Bachelorarbeit mit dem Thema "CrypTool 2 / Learn-CrypTool – Erstellung eines HTML 5-basierten elektronischen Lerntagebuches zur Unterstützung und Motivation der AnfängerInnen-Modus für das Softwareprogramm CrypTool 2,,

- von mir selbständig verfasst wurde und ich keine anderen als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internet-Quellen benutzt habe.
- bisher weder vollständig noch in Teilen von mir oder Anderen in einem Prüfungsverfahren eingereicht wurde.
- alle in ihr vorkommenden wörtlich oder sinngemäß übernommenen Textteile aus Schriften anderer Autoren als *Zitate* gekennzeichnet und die jeweiligen Quellen im Literaturverzeichnis am Ende der Bachelorarbeit aufgelistet sind.
- nur Grafiken, Illustrationen, Skizzen, Zeichnungen und sonstige bildliche Darstellungen anderer Urheber enthält, welche als Übernahmen gekennzeichnet sind und die jeweiligen Quellen im Literaturverzeichnis am Ende der Studienarbeit aufgelistet wurden.
- gebunden und auf elektronischem Speichermedium (CD-Rom) gespeichert eingereicht wird. Die gedruckten Fassungen und die elektronischen Fassungen sind vollständig überein.

Ich bin mit der Auslage meiner Studienarbeit in der Bibliothek einverstanden.

Koblenz, den 11.Juni.2014

(Eigenhändige Unterschrift der Verfasserin)

Inhaltsverzeichnis

| | | |
|----|--|----|
| 1 | Zusammenfassung | 3 |
| 2 | Einleitung | 5 |
| 3 | Literaturstudie im Bereich Serious Games und Lerntagebuch | 7 |
| | 3.1 Spielbasiertes Lernen durch serious games | 7 |
| | 3.2 Serious Games und Artverwandtes | 10 |
| | 3.3 Lerntagebuch | 13 |
| | 3.4 Grundlegende Einflussfaktoren des Lernens nach Manfred Spitzer | 16 |
| 4 | Erstellung einer Lernsoftware | 19 |
| | 4.1 Erstellung einer Lernsoftware | 19 |
| | 4.2 Spielerstellung | 24 |
| | 4.3 Grundaufbau des Spiels | 26 |
| 5 | CrypTool 2 | 28 |
| | 5.1 CrypTool 2 Wizard | 28 |
| | 5.2 CrypTool 2 Workspace Manager | 30 |
| 6 | Homepage | 39 |
| | 6.1 Aufbau der Homepage | 39 |
| | 6.2 Pädagogisch sinnvoller Aufbau von der Homepage | 51 |
| 7 | Technischer Hintergrund | 56 |
| | 7.1 MySQL | 56 |
| | 7.2 jQuery | 58 |
| 8 | Fazit | 60 |
| 9 | Quellenverzeichnis | 61 |
| | 9.1 Literatur | 61 |
| | 9.2 Internet-Quellen | 63 |
| | 9.3 Abbildungsverzeichnis | 65 |
| 10 | Anhang | 66 |
| | 10.1 „Strategien interaktiven Lernens zur Realisierung kognitiver, affektiver und psychomotorischer Lernziele“ | 66 |
| | 10.2 Anhänge auf DVD | 73 |

Kapitel 1

Zusammenfassung

Meine Bachelorarbeit ist als Fortsetzung und Weiterentwicklung der Studienarbeit „Erstellung einer HTML 5-basierten Lernoberfläche zur Unterstützung der Zielgruppe der AnfängerInnen für das Softwareprogramm CrypTool 2“ von Liane Syré, eingereicht am 13.08.2013 an der Universität Koblenz-Landau, konzipiert. Die Inhalte ihrer Studienarbeit dienen somit als Grundlage für die hier vorliegende Bachelorarbeit.

Ich habe im Rahmen meiner Bachelorarbeit einen Prototyp eines teilweise automatisierten Lerntagebuchs entwickelt, welchen ich im Folgenden Vorstellen möchte. Außerdem stelle ich meine ebenfalls eigenständig konzipierte LearnCrypTo-Homepage in dieser Arbeit vor.

Nach einer Einleitung in die Thematik (Kapitel 2) folgt eine Literaturstudie zu Serious Games als Teilbereich des Media-based Learning (Kapitel 3), in welchem auch explizit auf die Führung eines Lerntagebuchs und didaktische Konzepte eingegangen wird.

Es folgt eine Beschreibung wichtiger Aspekte bei der Erstellung einer Lernsoftware und gehe im Kontext der Serious Games noch mal auf die Spielerstellung ein (Kapitel 4).

Da meine Bachelorarbeit vor allem darauf ausgerichtet ist, CrypTool 2 AnfängerInnen nahe zu bringen, erläutere ich sodann die für benannte Zielgruppe wichtigsten Funktionen von CrypTool 2 (Kapitel 5).

Dann gehe ich näher auf Inhalt und Aufbau meiner eigens erstellten LearnCrypTo-Homepage ein (Kapitel 6).

Ich erläutere gegen Schluss meiner Arbeit ausgewählte technische Aspekte (Kapitel 7).

In einem abschließenden Fazit versuche ich, die Ergebnisse meiner Arbeit zu bewerten und wage einen kleinen Ausblick (Kapitel 8).

Im Verlaufe der Arbeit wird vermehrt mit einer hauptsächlich englischen Terminologie gearbeitet. Um Missverständnissen vorzubeugen werde ich die englischen Begriffe bei ihrer ersten Verwendung in meiner Arbeit ins Deutsche übersetzen und im Folgenden dann weiter mit der englischen Bezeichnung arbeiten.

Um Lesbarkeit zu fördern benutze ich in meiner Arbeit das generische Maskulinum.

Kapitel 2

Einleitung

“Erinnerung, du Wächter des Gehirns”
William Shakespeare

Welche Vorteile gab Wissen unseren Vorfahren?

Erstens ließ es die Menschen in der wilden Natur überleben und letztere bändigen. Dann lernten die Menschen, immer vollkommene Werkzeuge anzufertigen, fingen an sich mit dem Handwerk zu beschäftigen und unerforschte Länder zu erschließen.

So in einer beliebigen Sphäre der menschlichen Tätigkeit das Wissen zu ergreifen gaben die offensichtlichen Vorteile. Die Möglichkeit zu Lernen wurde immer schon als eine Belohnung angenommen.

Ob die Einstellung zum Lernen sich heutzutage geändert hat?

Ja, sie hat sich geändert. “Für das Lernen Interesse zu wecken oder zu lehren?” ist die Frage die heutzutage viele Pädagogen und Didaktiker beschäftigt.

Damals konnten die Menschen also durch ihr Wissen in der wilden Natur überleben.

Heutzutage sieht es etwas anders aus. Unsere Umwelt hat sich gewandelt. Wir leben urbanisiert und zivilisiert. Unsere alltägliche Natur und Umwelt stellt mehr und mehr das Internet dar.

Auch die Raubtiere, vor denen sich Menschen durch Wissen schützten, sehen heute anders aus. 16 Millionen geknackte E-Mailkonten geben Aufschluss darüber, worauf moderne Raubtiere aus sind – und darüber, was dem Menschen an Wissen fehlt, um sich in der modernen Umwelt zu schützen.

Kryptografie ist eine Wissenschaft, welche sich mit Codierung und Verschlüsselung von Informationen beschäftigt. Mittels Verschlüsselung kann sich der Mensch in einer modernen Umwelt schützen.

Es gibt ein sinnvolles Kryptografie-Programm namens CrypTool 2. Dieses ist ein Lernsystem, welches vielfältige technische Möglichkeiten zum Verschlüsseln zur Verfügung stellt und frei zugänglich ist.

Aufgrund der vielfältigen Funktionalität von CrypTool 2 verlieren Anfänger leicht die Übersicht und können überfordert werden. Im Rahmen meiner Bachelorarbeit versuche ich, einen Anfänger-Modus zu entwerfen.

Das erste Kernstück des Modus soll ein Serious Game darstellen, welches grundlegende Inhalte von Kryptografie bzw. Funktionen von Cryptool 2 vermittelt.

Was das Wissen angeht, so wurde es als so wichtig zum Überleben in damaliger wie heutiger Umwelt empfunden, dass auf der ganzen Welt Kulturtechniken entwickelt wurden, welche zum Speichern des Wissens in Schriftform dienen. Eine persönliche Form des regelmäßigen Datenspeichers ist das Tagebuch.

Das zweite und wichtigere Kernstück meiner Arbeit ist daher ein an das eben erwähnte Serious Game gekoppelte, teilweise automatisiertes Feedback in Form eines elektronischen Lerntagebuches.

Kapitel 3

Literaturstudie im Bereich Serious Games und Lerntagebuch

Den entscheidenden Reiz von Digitalspielen machen die spezifische Weise der Interaktivität und die Mensch-Computer-Interaktion, die sie anbieten, aus.

3.1 Spielbasiertes Lernen durch Serious Games

*“As children we learn to play,
and as we grow up, we play to
learn.”* [Michael & Chen 2006]

[Als Kinder lernen wir zu spielen,
und wenn wir erwachsen werden,
spielen wir um zu lernen.]

Serious Games (ernsthafte Spiele), sind, wie aus dem Begriff deutlich wird, in erster Linie Spiele. Serious Games treten in Form von Computer- oder Onlinespielen auf. Sie implizieren ausführliche Lernziele statt reiner Unterhaltung, so rechtfertigen sie ihre Zusatz “Serious” im Namen.

Im Folgenden werden einige Definitionen von Serious Games aufgelistet. Weiterhin wird eine Abgrenzung von artverwandten Begriffen versucht:

“A serious game is a game in which education (in its various forms) is the primary goal, rather than entertainment.” [Michael & Chen 2006, S. 17]

[Ein Serious Game ist ein Spiel in dem Ausbildung/Erziehung (in seinen verschiedenen Formen) primäre Absicht ist, eher als die Unterhaltung.] Michael Zyda führt eine andere Definition von Serious Games an: *“Serious games have more than just story, art, and software, however. (...) They involve pedagogy: activities that educate or instruct, thereby imparting knowledge or skill. This addition makes games serious.”* [Zyda 2005, S. 26]

[Serious Games beinhalten/bedeuten mehr als nur Story, Kunst und Software. (...) Sie involvieren Pädagogik: Aktivitäten, welche erziehen oder anweisen und dadurch Kenntnisse oder Fertigkeiten fördern. Diese Beigabe macht Spiele zu ernstern Spielen].

Michael Zyda beschreibt Serious Games als Spiele, die Unterrichtsmethoden nicht explizit ansprechen und realisieren, sondern eher als Spiele, die als Nebeneffekt erziehen und bilden. Im Gegensatz dazu kennzeichnen Michael und Chen Serious Games als Spiele, in denen es hauptsächlich auf Bildung/Erziehung ankommt.

Also sind Serious Games Computerspiele, welche unter dem Aspekt Spielen Wissen vermitteln. Die Idee, Computerspiele nicht nur zu Spaßzwecken zu verwenden, wurde zuerst im Buch von Clark C. Abt [1975] „Serious Games“ formuliert. Laut Abt muss der Bildungszweck der Serious Games nicht im Design des Spiels selbst liegen, sondern kann auch einem fertigen einfachen Spiel durch einen sinnreichen Zusammenhang bzw. Kontext zugeteilt werden. So kann zum Bsp. ein ursprünglich zum Spaß entworfenes Brettspiel in einem militärischen Lehrzusammenhang verwendet werden, um strategisches Denken und Grundsätze der taktischen Kriegsführung zu schulen.

Serious Games sind dem Bereich der Lernspiele zuzuordnen. Sie haben eine deutliche Struktur, Ziele, und ihre Ergebnisse finden praktische Anwendung im Leben. Als Hauptzweck von Serious Games wird Ausbildung und Training gesehen.¹

“Serious Games offer a new mechanism for teaching and training by combining video games with education. Serious Games can extend the value of training films and books by allowing the player to not only learn, but also to demonstrate and apply what he or she has learned.” [Abt 1975]

(Ernsthafte Spiele bieten durch die Kombination von Videospielen und Bildung einen neuen Mechanismus zum Lernen und Üben. „Ernsthafte Spiele“ können den Wert von Übungsfilmen und Büchern erweitern, indem sie dem Spieler erlauben, nicht nur etwas zu lernen sondern auch zu demonstrieren und anzuwenden was er oder sie gelernt hat.)

Der Prozess des Lernens wird dank der Serious Games interessanter – der Lernende kann entsprechende Fertigkeiten leicht entwickeln und perfektionieren. Während des Spielens lernt man aus eigenen Fehlern zu lernen.

¹ Vgl.: http://edutechwiki.unige.ch/en/Serious_game (letzter Zugriff: 24.05.2014)

Serious Games ist ein Teilgebiet der Lernspiele, das Simulationen ausdrücklich einschließt. Dies wird in folgendem Diagramm von Clark Aldrich [2009] veranschaulicht.

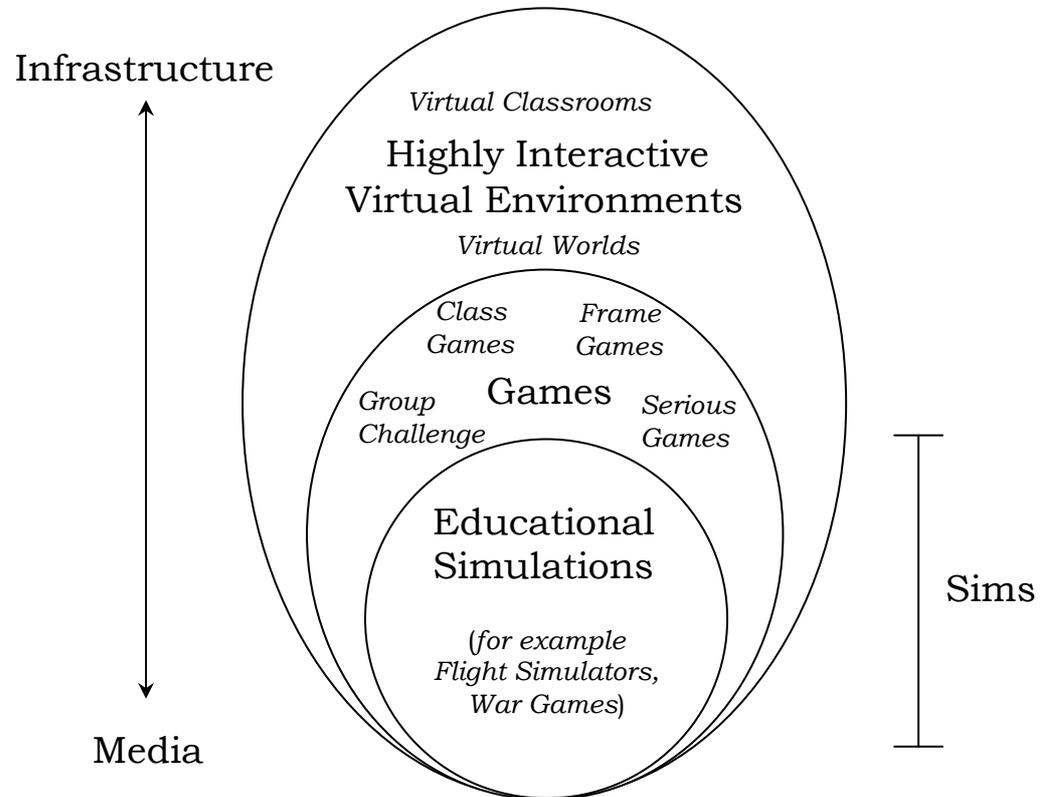


Abbildung 1: Media-based Learning

Da die Drehbücher der Serious Games ausreichend vielfältig und verzweigt sind, lassen sie dem Spieler Zeit sich an die Spielstruktur und die spieltypischen Prozesse zu gewöhnen. Sie fördern die Kompetenzentwicklung des Spielenden.

Dank der Serious Games erlebt ein Lernender ein und dieselbe Situation im Spiel mehrmals und kann Fehler begehen, bis die nötigen Ergebnisse zum Erreichen eines Lernerfolges erreicht werden. Serious Games simulieren nicht nur reelle Arbeitsprozesse sondern helfen sachkundiges Wissen zu ermitteln und auf Situationen zu reagieren, die im realen Arbeitsprozess entstehen.

Simulationen ermöglichen demnach auch das experimentelle Lernen, Sie können Prozesse simulieren, die zu teuer, zeitaufwendig oder unsicher gewesen wären, wenn sie in der echten Welt als Übungssimulation durchgeführt werden.

Eine gewisse Vereinfachung der Wirklichkeit im Rahmen einer didaktischen Reduktion ist für ein Simulationsprogramm dennoch unvermeidlich.

Argumente für Serious Games

- Motivierung des Spielenden für den Lernprozess (Schaffung von intrinsischer Motivation)
- Möglichkeit für den Spielenden, Fehler zu begehen und zu riskieren, ohne dass reeller Schaden für Gesellschaft und/oder Karriere entsteht
- Ermöglichung interaktiver und dynamischer Lernprozesse, Entwicklung von Kompetenzen
- regelmäßiges Einschätzen und Hinterfragen gesetzter Ziele wird angeregt und geschult
- Das Lernen mit mehreren Sinnen (Sehen, Hören, Fühlen) fördert die Gedächtnisleistung und damit die Lerneffizienz
- Spaßfaktor am Spiel führt zum Lernen
- Anpassungsmöglichkeit bzgl. Alter und/oder Erfahrung mit dem Lerninhalt
- Eine Menge an kostenfreien Produkten ist bereits im Internet verfügbar.

3.2 Serious Games und Artverwandtes

“A game is a system in which players engage in an artificial conflict, defined by rules, that results in a quantifiable outcome.” [Salen et al. 2004]

Ein Spiel ist ein System in dem Spieler sich an einem durch Regeln definierten, künstlichen Konflikt beteiligen, welcher zu einem quantitativ bestimmbaren Ergebnis führt.

Es existiert eine Menge an weiteren computer- und technikbasierten Lernkonzepten, wie z. Bsp.: Edutainment (unterhaltsames Lernen), Game-Based Learning (Spiel-basiertes Lernen) oder E-Learning (elektronisch-unterstütztes Lernen).

All diese Lernkonzepte benutzen Multimedia-Soft- und Hardwaresysteme als Grundlage. Aus diesem Grund haben diese Lernkonzepte viele Gemeinsamkeiten/Überschneidungen.

Abbildung 2 veranschaulicht das Ergebnis des Vergleichs und der Kombination nahezu aller oben erwähnten Definitionen und Klassifikationen aus dem Bereich des Media-Based-Learning (medienbasiertes Lernen). Es fasst die Beziehungen von Edutainment, DGBL Technology-enhanced learning, Game-Based-Learning, Entertainment education und den Serious Games zusammen. Durch ein Venn-Diagramm von Johannes Breuer, Gary Bente² sollen die begrifflichen Zusammenhänge veranschaulicht werden.

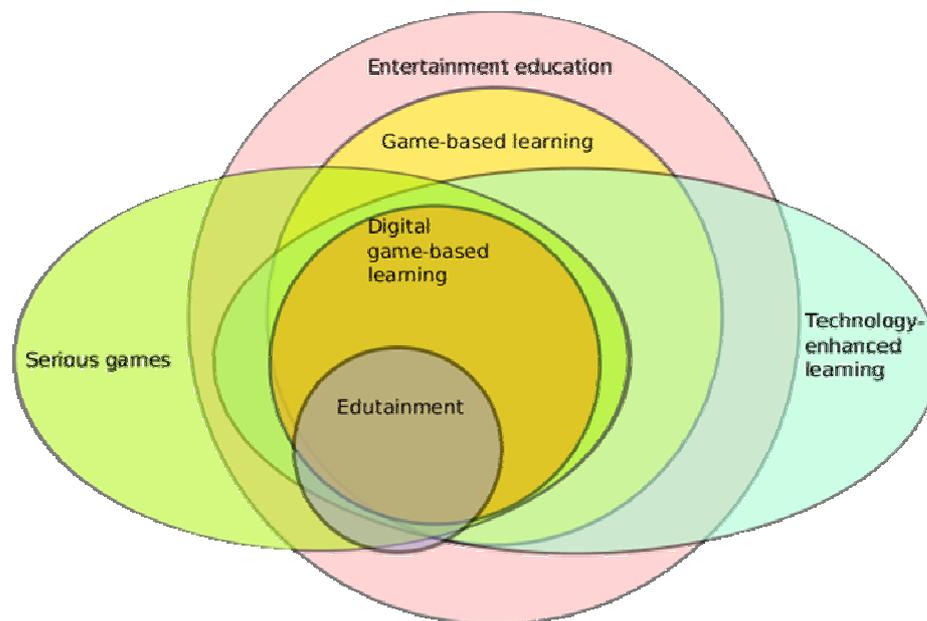


Abbildung 2: Beziehungen von Lerntechniken aus dem Media-Based-Learning (modifiziert durch Schneider, D. K.)

Das Diagramm stellt Edutainment als die kleinste Teilmenge von DGBL dar. Meist sind Edutainments Lernspiele für Kinder und/oder Jugendliche. Lernspiele greifen auf kognitive Sachkenntnisse zurück. Edutainmentprogramme präsentieren in der Regel mehr themenübergreifendes Wissen als Serious Games. Das Konzept des Edutainments verbindet Education (Bildung/ Erziehung) und Entertainment (Unterhaltung).

Digital Game-Based Learning (DGBL – Spielbasierte Digitallernen) schließt Spiele ein, in welchen das Lernen der wichtigste

²

<http://www.eludamos.org/index.php/eludamos/article/viewArticle/vol4no1-2/146> (letzter Zugriff: 24.05.2014)

oder alleinige Zweck ist. Marc Prensky [2007, S. 146] definiert DGBL als "any learning on a computer or online!". Darunter fallen z. Bsp. die typischen Lernspiele der 80-er Jahre (z. Bsp. Tetris, PONG), sowie die große Teilmenge der modernen Serious Games.

Game-Based Learning (spielbasiertes Lernen) bezieht sich auf alle Sorten von Spielen mit Bildungszielen (z. Bsp.: Brettspiele, Kartenspiele oder Digitalspiele). Game-Based Learning basiert auf dem Gleichgewicht zwischen den Lerninhalten und Spielaspekten. Eine besondere Rolle beim Game-Based Learning nimmt der Spielspaß ein. Dieser soll ebenso groß sein wie bei einem gewöhnlichen Computerspiel. Somit ersetzt Spielspaß die Motivation bei dem Game-Based Learning („Flow-Erlebnis“ nach Mihály Csikszentmihályi [2013]).

Entertainment Education (Unterhaltungsausbildung/-erziehung) ist an kein spezifisches Medium gebunden, wohingegen E-Learning mit dem Gebrauch von Computern assoziiert wird. Entertainment education bezieht sich einfach auf die Idee das Lernen angenehmer zu machen, z.B. durch das Hinzufügen von Spieldesignelementen.

E-Learning ist ein allgemeiner Begriff, der sich auf jeden Typ des computergestützten Lernens bezieht. Es impliziert weder Unterhaltung noch Spaß beim Lernprozess.

Laut Marc Prensky [2007] besteht der Hauptvorteil des E-Learnings darin, dass es Lernen in Gruppen ermöglicht. Und dies auch, wenn die Lernenden Räumlich voneinander getrennt sind. Es ermöglicht zeitlich und geografisch synchrones wie asynchrones, flexibles Lernen.

Mit E-Learning verbindet man im Wesentlichen Flexibilität beim Lernen und Lernen im virtuellen Klassenzimmer. E-Learning wird auch sehr mittels folgender Facetten beschrieben:

→ Interaktivität: Steuerungs- und Eingriffsmöglichkeiten für den Benutzer (z. Bsp.: Manipulation eines Objekts im Spiel, grafische, auditive oder optische Rückmeldung über die Folgen von Spieleraktionen);

→ Multimedialität: gleiche Informationen in den verschiedenen Medien können verschieden codiert werden (z. Bsp.: e-Books können animierten Bilder zeigen, was bei Papier Bücher nicht sein kann);

→ Multimedialität: Möglichkeit verschiedene Medien zu benutzen (z. Bsp.: Audiovisuelle Darstellung eines historischen Szenarios mit Textquellen und Hintergrundinformationen als Objekte im Spiel);

→ Multimodalität: verschiedene Möglichkeiten, Informationen über die Sinnesmodalitäten aufzunehmen (z. Bsp.: visuelle und auditive Reize).³

Abbildung 2 zeigt an, dass Serious Games andere Zwecke einschließen können als Bildung, z. Bsp. Kunst, Therapie oder Werbung. Daher unterscheiden sich Serious Games von klassischen Lernspielen, die eine Mischung aus Bildung und Unterhaltung darstellen.

Das Spielen von Serious Games kann gegebenenfalls das Sammeln von reellen Erfahrungen in echten Situationen ersetzen, aber sie verlangen simulierte Handlungen und emotionale Teilnahme von einem oder mehr Entscheidungsträgern, die Spielabsichten verfolgen.⁴

Das zentrale Konzept von Serious Games fokussiert die Integration eines Lerninhaltes in einen Spielablauf und das Erlangen wie Ausbauen von Kompetenzen und Kenntnissen, welche im (Arbeits-) Alltag Anwendung finden sollen.⁵

Serious Games simulieren meistens komplexe Arbeitsabläufe in einer nicht fiktiven Welt, daher richten die sich eher an die Zielgruppe der Erwachsenen. Im Vergleich dazu richten sich Edu-tainments eher an die Zielgruppe Kinder.

3.3 Lerntagebuch

Beschäftigt sich eine Person über längere Zeit mit einem Lernspiel ernsthaft, entwickeln sich im Laufe der Lerntätigkeit Fähigkeiten und Fertigkeiten. Um diese oder jene Fertigkeit zu erlernen, muss man Wiederholungen bestimmter Handlungen (Übungen oder Training) durchführen.

Der Fokus interaktiver Lernmethoden ist auf die Bildung von Fähigkeiten und Fertigkeiten gerichtet und besteht darin, die Ausführung solcher Aufgaben durch den Lernenden zu gewähr-

³ <http://de.wikipedia.org/wiki/E-Learning> (letzter Zugriff: 23.01.2014)

⁴ <http://www.eludamos.org/index.php/eludamos/article/viewArticle/vol4no1-2/146> (letzter Zugriff: 23.01.2014)

⁵ http://edutechwiki.unige.ch/en/Serious_game (letzter Zugriff: 23.01.2014)

leisten und zu fördern. Um dem Lernenden den eigenen Fortschritt und Entwicklungsprozess durch wiederholte Anwendung des Lernprogramms anzuzeigen und damit seinen Reflexionsprozess zu unterstützen wird sehr oft ein Lerntagebuch benutzt.

Ein Lerntagebuch ist ein pädagogisches Lernhilfsmittel, das Lernende weitgehend beim Lernprozess unterstützt durch deren Auseinandersetzungen mit dem Lerninhalt und persönlichen Lernzielen. Es hilft über erworbenes Wissen zu reflektieren, dieses teilweise zu dokumentieren und im Nachhinein einen Rückblick über das Erlernte zu erhalten.

Lerntagebücher haben keine bestimmte Form oder Norm, an welche man sich halten müsste, also lassen sie einem Lernenden einen großen Freiraum was Form und Inhalt anbelangt.

Es kann als ein Heft, Ordner oder als Buch gestaltet werden. Der Tagebuchschreiber kann die gelehrteten Inhalte als formlose Einträge schreiben oder in eine bestimmte, vorstrukturierte Form führen.

Da ein Lerntagebuch persönliche Eindrücke über die Lerninhalte enthält, sollte das Tagebuch auf jeden Fall eine Seite enthalten, welche die Besitzverhältnisse festlegt. Außerdem sollte nur dem Autor und ggf. vom Autor autorisierten Lesern Zugang zu den Inhalten des Tagebuches gewährt werden. Bei dem elektronischen Lerntagebuch wird dies durch den Log-In und den entsprechenden Passwortschutz ersetzt.

Mittels eines Lerntagebuchs kann ein Lernender seinen Lernprozess festhalten. Anhand einzelner Einträge im Lerntagebuch lässt sich ein Lernstoffzuwachs leicht visualisieren. Somit wird Lernerfolg (erreichte Ziele und Kompetenzen) einem Lernenden möglicherweise bewusst gemacht. Jeder Lernfortschritt baut auf Vorwissen. Dadurch, dass man ein Tagebuch über seinen Lernprozess führt, erklärt man sich Lernstoff möglicherweise noch einmal in seinen eigenen Worten. Somit unterstützt das Tagebuch wichtige Elaborationsstrategien. Des Weiteren schweift man beim Tagebuchschreiben immer wieder ab und denkt weniger in vordefinierten Klassifikationen wie z. Bsp. Schulfächern. Dadurch werden assoziative Lernstrategien gefördert.

Vorteile der Führung eines Lerntagebuches:

- Personalisierungsmöglichkeiten durch eigene Gestaltung
- reflektierende Auseinandersetzung mit Lerninhalten
- persönliche Erlebnisse kommen zum Ausdruck
- persönliche Erlebnisse werden verarbeitet
- unterstützt Einzelarbeit
- unterstützt mentale Verarbeitung der Lerninhalte
- Lernender entwickelt eigene Struktur der Lerninhalte
- Problemverbalisierungsmöglichkeiten
- möglicher Denkanstoss durch eigene Assoziationen und E-selsbrücken
- Lösungsvorschläge durch persönliche Stellung zum Problem
- Dokumentierte Inhalte können geschützt, privat und vertraulich gegenüber anderen Lernenden bleiben (gilt eher für das Online-Lerntagebuch, z. Bsp. durch Einloggen im Account und Sichtbarkeitseinstellungen)
- Freiheit der Entscheidung welche Inhalte weiter mitgeteilt werden (gilt eher für Online-Lerntagebuch, z. Bsp. durch Sichtbarkeitseinstellungen)

Mögliche Nachteile der Führung eines Lerntagebuches:

Die Ergebnisse einer Studie durch die britischen Forscher Elaine Duncan (Glasgow Caledonian University) und David Sheffield (Staffordshire University) zeigte, dass das Schreiben der Tagebücher negative Auswirkung auf die Gesundheit haben. Bei einer Umfrage (135 Studenten, davon 94 Tagebuchschreiber) haben Freiwillige Standardfragebogen zu ihrer Gesundheit ausgefüllt.

“We expected diary-keepers to have some benefit, or be the same, but they were the worst off.”⁶

„Wir haben angenommen, dass Tagebuchbewahrer [durch die Tagebuchführung] einen Vorteil hatten, oder genauso gut waren, aber sie waren am schlechtesten dran“.

Die Ergebnisse der Studie sind nicht eindeutig, da von den Forschern meiner Meinung nach nicht entgültig geklärt werden konnte, ob eine rein zufällige Verbindung oder ein klarer Kausal-Zusammenhang zwischen dem Führen eines Tagebuches und dem aktuellen Gesundheitszustand der Befragten bestand. Es wäre verkehrt, dies als Gesetzmäßigkeit zu behandeln. Allerdings erscheint mir das Führen eines Tagebuches als zeitaufwändig. Ich kann mir durchaus vorstellen, dass eine solche Tätigkeit neben dem eigentlichen Lernen als belastend empfunden

⁶ <http://www.newscientist.com/article/mg18324642.300-depressing-news-for-diarists.html> (letzter Zugriff: 16.01.2014)

werden und sich über längere Zeit auch gesundheitlich auswirken kann.

Dennoch: Um die oben benannten Nachteile zu vermeiden und gleichzeitig die Vorteile einer Tagebuchführung zu nutzen, bietet sich zur Unterstützung meiner Lernsoftware ein automatisiertes bzw. teilweise automatisiertes Lerntagebuch als Feedbackmöglichkeit und Leitfaden beim Lernen an.

Durch Nutzung des Lerntagebuch soll erreicht werden, dass die Motivation beim Lernenden auch über längere Zeit nicht nachlässt – und dies ohne Druck auf den Lernenden aufzubauen.

Was soll beim Lerntagebuch automatisch eingetragen werden?

Um Struktur bei Lerninhalten zu verschaffen ist es wichtig zu erwähnen WAS man NEUES gelernt hat und WAS man vom Lerninhalt WIEDERHOLT hat. So behält der Lernende einen Überblick über seinen Fortschritt.

Der inhaltliche Fortschritt kann automatisch eingetragen werden.

Was nicht automatisch eingetragen werden kann, ist der emotionaler Zustand des Lernenden, welcher aber deutlichen Einfluss auf die Lernleistung hat: *„Akute emotionale Erregung kann dazu führen, dass wir bestimmte Dinge besser behalten. Was den Menschen umtreibt, sind nicht Fakten, sondern Gefühle!“* [Spitzer 2007, S. 160]. Insofern erscheint es mir wichtig, dass der Lernende durch das Tagebuch die Möglichkeit erhält, über seine Laune nach jedem einzelnen Lernabschnitt nachzudenken und diese festzuhalten.

3.4 Grundlegende Einflussfaktoren des Lernens nach Manfred Spitzer

Einer der derzeit am meisten im Bereich Hirnforschung und Lernen zitierten Autoren ist der Psychologe und Psychiater Manfred Spitzer. Er beschreibt in seinem Buch „Lernen. Gehirnforschung und die Schule des Lebens“ vier grundlegende Faktoren, welche Einfluss auf das Lernen haben. Es handelt sich um Emotionen, Aufmerksamkeit, Motivation und Vorwissen. Von jedem dieser Einflussfaktoren leitet Spitzer Forderungen für das Lernen ab. Auch wenn Spitzer seine Forderungen konkret an Lehrer und Schulen richtet, so lassen sich aus seinen Aussagen durchaus Forderungen für E-Learning ableiten. Durch eine Anwendung der abgeleiteten spitzerschen Forderungen werde ich die

LearnCrypTo-Homepage an aktuellen Maßstäben der Pädagogik/Hirnforschung messen.

Laut Spitzer sind Emotionen: „*nicht beschreibbar und nicht zählbar. Sie haben eine Stärke (viel-wenig) und eine Valenz (gut-schlecht), haben kognitiven, qualitativ-gefühlsmäßigen, körperlichen Aspekt: (Ausdrucks -)Bewegungen, Effekte des unwillkürlichen Nervensystems (Zucken).*“ Beim Lernen verknüpft man Lerninhalte mit der entsprechenden Lernsituation, und besonders mit damit verbundenen Emotionen. Positive Emotionen führen dazu, dass Lernender den Lernstoff besser behält. Angst oder negative Emotionen dagegen blockieren kreatives wie problemlösendes Denken. Das liegt daran, dass vor allem das Herstellen von Zusammenhängen zwischen dem Gelernten und dem Vorwissen verhindert wird.

Folgende Forderungen kommen vom Einflussfaktor Emotionen zu Stande:

- lernförderliches Klima
- angstfreie Lernatmosphäre
- wertschätzender und respektvoller Umgang
- Positive Grundstimmung herstellen
- Fehler als Chance sehen
- Trennung von Lern- und Leistungsüberprüfungen
- kein Notendruck
- Lernorientierung/Unterstützung
- Stärkung des Selbstvertrauens
- positive Einstellung zum Lernen fördern

Ein weiterer Einflussfaktor ist Aufmerksamkeit. Aufmerksamkeit hat 2 Ebenen: Daueraufmerksamkeit (Vigilanz) und selektive Aufmerksamkeit. „*wir nehmen die Welt um uns herum wahr und filtern das für uns Wesentliche aus den vielen Stimuli heraus.*“

Jeder Lernende hat eine bestimmte Aufmerksamkeitsspanne, also eine Zeitspanne über welche der Lernende konzentriert aufmerksam sein (zum Beispiel einem Vortrag folgen) kann. Beim Überfordern dieser Spanne wird ein Lernender unaufmerksam. So kommen folgende Forderungen bzgl. des Einflussfaktors Aufmerksamkeit zu Stande:

- Lernen durch eigenes Tun (durch eigene aktive Handlungen misst ein Lernender einem Lerninhalt mehr Bedeutung bei, dadurch steigt seine/ihre Aufmerksamkeit dem Inhalt gegenüber)
- eigene Regeln beim Lernen aufstellen (z. Bsp. bzgl. Pausenzeiten)

→ Lernen mit allen Sinnen (je mehr Sinne bei einem Lernprozess beteiligt werden, desto mehr Gehirnareale werden beim Lernen beansprucht, desto stärker werden Lerninhalte vernetzt)

Motivation ist ein dritter Einflussfaktor auf das Lernen laut Spitzer. Als Motivation wird das Streben nach bestimmten Zielen oder Zielobjekten beschrieben. *„Unser Gehirn berechnet, was als Nächstes passieren könnte. Tritt etwas ein, das besser als erwartet ist, kommt es zu einem körpereigenen Belohnungseffekt (Dopamin-Ausschüttung). Das ausschlaggebende Ereignis wird weiterverarbeitet und mit höherer Wahrscheinlichkeit gespeichert.“* Also lernt ein Lernender immer dann etwas, wenn er eine positive Erfahrung gemacht hat. Dabei ist positive Erfahrung von Gemeinschaft und somit von Sozialkontakten (Lob oder Belohnung) des Lernenden abhängig.

Folgende Forderungen lassen sich laut Spitzer vom Einflussfaktor Motivation zu ableiten:

- Lernen mit Überraschungen
- Bezug zur Lebenswelt aufbauen
- Sinn und Bedeutung des Lerninhalts erkennen lassen
- Erhöhen der Lernfreude:
 - durch Ermöglichen von Erfolgen
 - durch Lob
 - durch Begeisterung des Lehrenden für den Lernstoff
 - durch Fehlerfreundlichkeit

Der letzte von Spitzer beschriebene Einflussfaktor ist Vorwissen. Vorwissen beschreibt alles, was ein Lernender schon an Vorerfahrungen, -kenntnissen und auch -urteilen über einen Lerngegenstand mitbringt.⁷ Vorwissen bietet daher eine gute Lernbasis für weitere Lernerfolge. So kommen folgende Forderungen vom Einflussfaktor Vorwissen zu Stande:

- Klarheit des Lerninhaltes
- Anknüpfen an bereits Gelerntes, um Wissen zu vernetzen und zu erweitern
- Lerninhalte strukturiert darbieten, damit Lernender altes mit neuem Wissen vernetzen können (Transparenz)
- Skelett vor Detail
- Verknüpfung mit der Realität (Ankerpunkte)
- Lernen im eigenen Tempo
- Umgang mit Heterogenität

⁷ vgl. „Vorverständnis“ auf http://epub.uni-regensburg.de/7005/1/ubr04036_ocr.pdf

Kapitel 4

Erstellung einer Lernsoftware

4.1 Erstellung einer Lernsoftware

Als Lernsoftware bezeichnet man *„jede Art von Computer-Software, die speziell für Lernzwecke entwickelt und programmiert wurde.“*⁸ Heutzutage ist Lernsoftware in vielen Arten (z.B. Blended Learning, Serious Games, Onlinekurse oder Podcasts) und Formen (z. Bsp. Simulationen, Tutorials, Lernspiele oder Drill and Practice) im Umlauf. Bei dieser breiten Palette an Lernsoftware geht es nicht speziell um einen konkreten Lerncharakter, sondern um die Unterstützung des Lernverhaltens z.Bsp. durch spielerische Aspekte. Peter Baumgartner formuliert in seinem Buch *„Didaktische Anforderungen an (multimediale) Lernsoftware“* [1997] folgende Aussage: *„Lernsoftware hat einen klar umrissenen Lerninhalt, folgt einem bestimmten didaktischen Konzept und ist auf eine mehr oder weniger klar definierte Zielgruppe ausgerichtet.“*

Die gleichen Aspekte der Lernsoftware greift auch Franz Shanda in seinem Buch *„Computer-Lernprogramme“* [1995] auf.

→ Zielgruppe

Ob der Einsatz der Lernsoftware sinnvoll ist, ist von der Zielgruppe abhängig. Die Lernsoftware soll aber nicht nur Fortgeschrittenen gerecht werden, sondern auch für Anfänger geeignet sein.

Eine Zielgruppe lässt sich präzisieren durch z. Bsp. Alter, Geschlecht, schon vorhandene Kenntnisse oder Interessen.

Die Zielgruppe der LearnCrypTo-Homepage ist groß, aber beschränkt auf Anfänger im Bereich Kryptografie, welche Interessen an Kryptografie haben, aber minimales Vorwissen besitzen. Es gibt keine anderen Beschränkungen wie Alter, Geschlecht oder individuelle Merkmale. Es gibt jedoch Faktoren, die indirekten Einfluss auf die Zielgruppe haben, wie bisherige Lernerfahrungen und bevorzugte Lernstile, Notwendigkeit, Gruppenzwang oder andere soziale Einflussfaktoren. Der Faktor bisherige Ler-

⁸ <http://de.wikipedia.org/wiki/Lernsoftware>

nerfahrungen beispielsweise beschränkt die Zielgruppe indirekt auf Personen, welche bereits gewisse Erfahrungen mit (im vorliegenden Fall) Computern, Datenschutz und Symbolik haben. In Betracht dessen würde ich die Seite für Benutzer ab einem Alter von 12 Jahren empfehlen.

→ Lerninhalte

Ob Lerninhalte richtig vermittelt werden liegt lt. Franz Schanda [1995] an der Lernstofftiefe. Der Lernende soll durch den Lernstoff nicht unter- oder überfordert werden. Die richtige Lernstofftiefe soll zwischen 25 und 50% des Gesamtlernstoffes liegen, was durch Abbildung 3 verdeutlicht wird. Laut Schanda [1995]: *“Mit 25% des möglichen Lehrstoffes deckt man oft schon den Wissensbedarf von 50% der Adressaten ab.”* Für mein Anagramm-Lernspiel mit dem CrypToPhant (Siehe Kapitel 6) erscheint es daher angebracht, nicht die Erlangung Kenntnis über alle Funktionen von CrypTool 2 als verbindliches Spielziel zu bestimmen, sondern lediglich von ein Viertel bis zur Hälfte aller Funktionen. Die LearnCrypTo-Homepage vermittelt Lerninhalte zu Kryptografieverfahren und CrypTool. Sie regt zur Erlangung praktische Erfahrung in Kryptografie und Entwicklung von Handlungskompetenzen an.

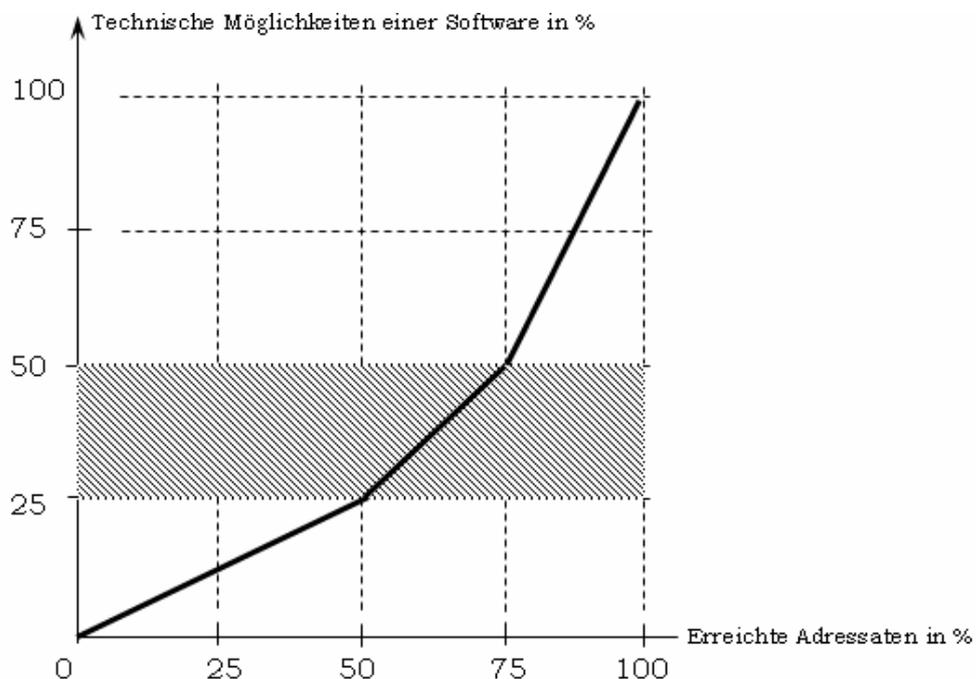


Abbildung 3: Wahl der Lernstofftiefe [Schanda 1995]

→ Lernziele

Benjamin Samuel Bloom kategorisierte 1956 in seinem Buch „*Taxonomie of educational objectives*“ („Taxonomie der Lernziele“) drei Bereiche: kognitive, affektive und psychomotorische Bereiche.

- Der kognitive Bereich unterscheidet zwei wichtige Lern-techniken: Auswendiglernen und Einsichtiges Lernen.
- Der affektive Bereich unterscheidet ebenfalls zwei Lern-techniken: Soziales Lernen und Einstellungslernen.
- Der psychomotorische Bereich unterstützt das Lernen von Bewegungsabläufen.

Bloom ordnet eine Reihe hierarchisch gegliederter Lernziele (nach Grad der Komplexität) diesen drei Bereichen zu. So ordnet Bloom folgende sechs Lernziele dem kognitiven Bereich zu:

1. Kenntnisse/Wissen (*Knowledge*): Bekannte Informationen können im Gedächtnis abgerufen werden.
2. Verständnis (*Comprehension*): Neue Informationen können verarbeitet und in einem größeren Kontext eingeordnet werden.
3. Anwendung (*Application*): Erlerntes soll in entsprechenden Situationen verwendet werden.
4. Analyse (*Analysis*): Ein Sachverhalt kann in seine Bestandteile zerlegt werden.
5. Synthese (*Synthesis*): Teile und Elemente können zu einem neuen Ganzen zusammengefügt werden.
6. Beurteilung/Evaluation (*Evaluation*): Einschätzung ob bestimmte Kriterien bestimmte Zwecke erfüllen.

Weitere fünf Lernziele werden dem affektiven Bereich nach Grad der Komplexität zugeordnet:

1. Aufmerksamkeit: Bereitschaft zur aktiven Aufnahme, passive Wahrnehmung.
2. Reaktion: Bereitschaft zur aktiven Reaktion, emotionale Betroffenheit erleben.
3. Werten: Präferenz für einen Wert, persönliche Verpflichtung für einen Wert eingehen.
4. Organisieren: Selbstständige Formulierung des Inhaltes, Einordnen von Inhalten und Werten in ein Wertesystem, Vergleich von Werten und Inhalten. Strukturierter Aufbau eines Wertesystems.
5. Erfülltsein durch einen Wert oder eine Wertstruktur: Werte- bzw. Inhaltsdarstellung in Kontexten.

Und die letzten fünf Lernziele werden dem psychomotorischen Bereich nach Grad der Komplexität zugeordnet:

1. Imitation: Bei der Konfrontation des Lernenden mit einer beobachtbaren Handlung beginnt der Lernende diese Handlung nachzuahmen.
2. Manipulation: „Entwicklung von Fertigkeiten beim Befolgen von Anweisungen, Ausführen selektiver Handlungen und Festigung des Handlungsablaufs mit fortschreitender Übung.“⁹
3. Präzision: Diese Stufe ist für das Reproduzieren von Lerninhalten bedeutsam, dabei sind Genauigkeit und Maßverhältnisse zu beachten.
4. Handlungsgliederung: Koordination von einer Folge von Handlungen durch Herstellung einer geeigneten Abfolge und ein harmonisches Zusammenwirken verschiedener Aktionen.
5. Naturalisierung: höchster Grad der Beherrschung der Handlungsfertigkeit, Ausführung mit geringstmöglichem Aufwand psychischer Energie.

Auf der Basis dieser verschiedenen Lerntechniken haben F. Schanda, J.U. Martens und G. Seng ein Papier [Schanda et al. 1990] entwickelt, der ein Katalog von Aspekten auflistet, welche notwendig für die verschiedenen Lerntechniken sind. Aus diesem Katalog lässt sich ableiten welche Lerntechniken für das Lernen mit dem PC bzw. Lernsoftware geeignet ist.

Das Fazit, zu den F. Schanda, J.U. Martens und G. Seng kamen (Lernsoftware ist rein kognitiver Lernprozess, der nach Bedarf differenziert werden kann.), trifft heutzutage leider nicht zu. Man darf nicht den Aspekt des Sozialen Lernens beim Erstellen einer Lernsoftware ausblenden, ebenso wenig das Lernen von verschiedenen Bewegungsabläufen. Die meisten weiter oben genannten Einflussfaktoren auf das Lernen nach Manfred Spitzer werden ebenfalls ignoriert.

Die Lernziele legen fest bei welchen Lernzielbereichen oder Lerntechniken eine Lernsoftware erfolgreich einsetzbar ist.

Heutzutage ist gute Lernsoftware eine Kombination von allen drei Lernzielbereichen, was ich auch bei der LearnCrypto-Homepage (siehe Kapitel 6) umgesetzt habe. Die Lernziele, die bei der Homepage gesetzt werden, sind erreichbare Lernziele:

- Wissen zu Kryptografie erwerben
- Handlungskompetenz erwerben
- Praktische Erfahrung in Kryptografie (Chiffrierverfahren anwenden können) erwerben.

⁹ <http://paedpsych.jk.uni-linz.ac.at/internet/arbeitsblaetterord/LERNZIELORD/m2.html>

→ Lernsituation

Lernsoftware ist heutzutage so vielfältig, dass sie eine Reihe von verschiedenen Einsatzmöglichkeiten bietet:

- Einzellernplatz – ist individuelles Lernen. Die Vorteile des Einzellernplatzes liegen darin, dass der Lernende selbst über Lernzeiten, Lernumfeld und Menge des Lernstoffes bestimmen kann.

Ein Nachteil eines Einzellernplatzes ist die automatische Voraussetzung von Motivation und Konzentration, die der Lernende zum erfolgreichen Lernen braucht.

- Lernpartnerschaft – Lernen mit einem Partner. Der Lernstoff wird zusammen mit einem Lernpartner bewältigt. Verständnisprobleme können im Gespräch geklärt werden. Das fördert entsprechende Konzentration und Ausdauer, setzt aber trotzdem ein gewisses Maß an Motivation voraus. Lt. Franz Schanda wichtig zu beachten: *„Mehr als zwei Personen an einem Gerät können nicht mehr individuell lernen“* [Schanda 1995].

Vorteile einer Lernpartnerschaft: gemeinsames Aufarbeiten und Lernerlebnis hat positive Auswirkung auf den Lernfortschritt. Nachteile einer Lernpartnerschaft: es geht ganz oder teilweise der eigene Lernweg sowie das individuelle Lerntempo verloren. Die LearnCrypTo-Homepage wird als Einzellernplatz eingesetzt, schliesst aber die Lernpartnerschaft nicht aus.

Die Didaktik einer Lernsoftware folgt in der Regel einem theoretischen Lernmodell (Konstruktivismus, Kognitivismus oder Behaviorismus).

Die Didaktik der von mir im Rahmen dieser Arbeit erstellten LearnCrypTo-Homepage folgt dem Lernmodell des Kognitivismus. *„Im Mittelpunkt des Kognitivismus stehen die individuelle Informationsverarbeitung sowie die dazu gehörigen Denk- und Verarbeitungsprozesse der Lernenden.“*¹⁰ Durch Präsentation des Lerninhalts als Lebensraum bzw. Landschaft (Cryptoplanet) wird der Benutzer zum explorativen, unterhaltenden und entdeckenden Lernen aufgefordert.

¹⁰ Vgl. Holzinger, Andreas (2000). Basiswissen Multimedia. Band 2: Lernen. Würzburg, S. 110 f.

4.2 Spielerstellung

Was muss man wissen oder können um ein Spiel zu erstellen?

1. Man braucht Erfahrung mit PC-Spielen.

Das ist notwendig um

- die allgemeine Struktur eines Spiels zu verstehen.
- den Aufbau von Spielprozess und Spiellogik zu verstehen.
- aus fremden Fehlern (bei der Erstellung des Spiels) zu lernen.
- eventuell fremde Ideen bzw. schon existierende Spiele weiter zu entwickeln.

2. Das logische Denken soll vorhanden sein.

Das ist notwendig um einen Programmcode zu schreiben und/oder die logische Reihenfolge eines Spiels aufzubauen.

3. Die Auswahl des Spiel-Motors

Der Spiel-Motor ist eine Zusammensetzung der Systeme, die die am öftesten verwendeten Funktionen des Spiels vereinfachen. Der Spiel-Motor besteht aus den Subsystemen, die bestimmte Teile des Spieles kontrollieren.

Mehrheit der Spiele haben die folgenden Subsysteme:

→ Grafiksystem

Der grafische Motor, dessen Hauptaufgabe die Visualisierung (Rendering) der zweidimensionalen oder dreidimensionalen Computergraphik ist. Er kann als selbstständiges Produkt oder als Teil eines Spielmotors existieren.

Er kann für die Visualisierung von abgesonderten Darstellungen oder Computervideos verwendet werden.

→ Physiksystem

Dies erzeugt die Computermodellierung der physischen Gesetze der realen Welt in der virtuellen Welt, mit dieser oder jener Stufe der Approximation. Meistens werden die physischen Motoren nicht wie abgesonderte selbstständige Softwareprodukte, sondern wie Bestandkomponenten (die Unterprogramme) anderer Programme verwendet.

→ Soundsystem

Die Soundkomponente des Spielmotors, die für die Wiedergabe der Geräusche im Computerspiel oder anderer Anlage verantwortlich ist. Der Sound-Motor ist auch für die Imitation bestimmter akustischer Bedingungen, die Wiedergabe der Geräusche laut der Lage, das Echo usw. verantwortlich [Gregory et al. 2009].

In der Regel besteht der Spiel-Motor nur aus einer grafischen Ausgabe (das Übrige wird von externen Bibliotheken importiert) oder aus allen drei Gruppen der Bibliotheken. Ebenso können zu dem Spiel-Motor verschiedene Arten des Spielinhaltseditors beigefügt werden.

Mir sind die folgenden drei Vorgehensweisen in der Spielentwicklung bekannt:

→ Einen fertigen Spiel-Motor (der englische Begriff ist im Bereich Informatik gängiger: Game Engine) bei der Entwicklung zu benutzen.

Die Nutzung des Spiel-Motors vereinfacht die Entwicklung des Computerspiels um Einiges. Ein Spiel-Motor ist eigentlich das Programm, in welchem man Spielobjekte optisch aufstellen und Parameter festlegen kann. Nur falls notwendig muss man diese mit wenigen selbstgeschriebenen Quellcodes erweitern. Nachteile von Spiel-Motoren sind die beschränkten Möglichkeiten durch standardisierte Abläufe. Mit der Hilfe von einem solchen Spiel-Motor lässt sich nur das machen, was der Motor zur Verfügung stellt.

→ Verschiedenen Arten der Spiel-Motoren zu benutzen (die Komplexität bei der Verwendung: mittel schwer)

Bei dieser Variante muss man auf jeden Fall programmieren. Der Spiel-Motor ist hier eine Bibliothek mit im Voraus erschaffenen Funktionen und Objekten, die in dem erschaffenen Spiel verwendet werden.

→ Das Spiel komplett, also einschließlich der Entwicklung eines eigenen Spiel-Motors zu programmieren (Komplexität: hoch bis sehr hoch)

Diese Variante ist die komplizierteste von allen drei und setzt Handlungskompetenz bzgl. API (OpenGL, DirecX) voraus.

Für die Erstellung eines eigenen Anagrammspiels zur Schulung Kompetenzen im Bereich Verschlüsselung/Codierung habe ich Tululoo Game Maker benutzt. Tululoo Game Maker ist eine komplexe Spielerstellungsumgebung, die zum Erstellen von Browser-basierten Spielen benutzt wird. Tululoo ermöglicht die Erstellung von Spielen für mobile Geräte, wie die Unterstützung der HTML5-Standards. Tululoo beinhaltet einen Ressourcenmanager und Skript-Editor. Tululoo erlaubt eigene Bilder, Hintergründe, animierte Sprites und Sounds zu importieren. So kann man einfach Objekte (wie z.B. Spieler, Gegner, sammelbare Gegenstände, etc.) und eigene Funktionen oder Skripte zu den Objekten im Spiel erstellen.

Alle zur Verfügung gestellten Funktionen des Spiel-Motors Tululoo habe ich durch JavaScript-Codeteile erweitert um benötigte für Anagrammspiel Funktionalität zu vervollständigen.

4.3 Grundaufbau des Spiels

Der Algorithmus fast jedes Spiels besteht aus einer Standardreihenfolge von Handlungen. Zunächst geschieht eine Vorbereitung, im Folgenden eine Abstimmung der Parameter des Spiels bzw. des Levels, dann wird der wiederholende Spielzyklus gestartet und nach dem Ausgang aus dem Spielzyklus (durch game over oder Übergang auf den nächsten Level) werden ausgewählte Ressourcen frei gegeben.

Die meisten und interessantesten Prozesse geschehen im Spielzyklus:

- Die Tastatur-/Mausabfrage – die Input-Verwaltung.
- Die globalen Ereignisse (z. Bsp. die Umstellung der Kamera).
- Die Aktualisierung des Zustandes der Spielobjekte (Koordinaten, Geschwindigkeit, Verhalten: Zusammenstoß, Sterben, Erscheinen, Umwandlung u. Ä.).
- Die Abbildung der Spielobjekte (Elemente des Spieles, welche über Verhalten verfügen; der Spieler oder andere Objekte können mit diesem Element zusammenwirken) und übrige Objekte (der Hintergrund, der Spielstand usw.).

Das im Rahmen dieser Arbeit entstandene Lerntagebuch kreiert teilweise automatisierte Einträge basierend auf den Lernerfahrungen und -Ergebnissen eines registrierten Benutzers. Dazu muss Letzterer aber zunächst entsprechend messbare Daten produzieren. Zu diesem Zweck habe ich mich entschlossen, ein Anagrammspiel zu programmieren, welches auf der LearnCrypto-Homepage angesiedelt ist und dessen Nutzung zu automatischen Einträgen im Lerntagebuch führt.

Ein Anagramm ist eine der einfachsten Chiffriermethoden, welche als Spielform mittlerweile durch u. A. zahlreiche Apps Einzug in den Alltag gefunden hat. Dadurch wird einem Benutzer der Einstieg in den Bereich Kryptografie erleichtert.

Das von mir programmierte Anagrammspiel ist ein mit Hilfe eines Spiel-Motors (Tululoo Game Maker) erstelltes Spiel. Die zusätzlichen, nicht im Tululoo vorhandenen, Funktionen werden durch mittels JavaScript erstellte Quellcodeteile realisiert. Das Spiel ist so aufgebaut, dass ein Wort ausgegeben wird, bei wel-

chem durch ein Permutationsverfahren die Buchstaben vertauscht werden. Das gesuchte Wort wird per Zufall aus einem Array, welches 100 Wörter speichert, ausgesucht. Um im Anagrammspiel weiter zu kommen, muss der Benutzer das gesuchte Wort (Buchstaben in richtiger Reihenfolge) eintippen. Das Ergebnis (Anzahl der abgefragten Wörter, Anzahl der richtig eingetippten Wörter, sowie das Verhältnis der beiden Angaben zueinander) des Anagrammspiels wird im Reisetagebuch eingetragen.

Kapitel 5

CrypTool 2

Da ich im Rahmen meiner Bachelorarbeit eine Lernwebseite inklusive eines Lerntagebuches zur Unterstützung und Motivation von Anfängern beim Aneignen von Kompetenzen bzgl. der CrypTool 2-Software erstelle, möchte ich im Folgenden zumindest die beiden für Neulinge relevantesten Funktionen von CrypTool vorstellen: CrypTool 2 Wizard und CrypTool 2 Workspace Manager.

5.1 CrypTool 2 Wizard

Wizard ist ein vielfältiges Werkzeug von CrypTool 2, welches für Anfänger zum Einstieg in CrypTool 2 gut geeignet ist.

Beim Starten von CrypTool 2 wird Wizard als erstes Werkzeug beim „Main Functions“ abgebildet, was seine Wichtigkeit deutlich zum Ausdruck bringt.

Durch Doppelklick gelangt man zu einer Liste möglicher Aufgaben/Verfahren/Vorlagen, welche mit Wizard einfach zu erlernen bzw. bearbeiten sind. Sobald man eine Aufgabe/Vorlage bzw. ein Verfahren auswählt, erscheint eine Beschreibung der Aufgabe/dem Verfahren/der Vorlage in der Mitte des Bildschirms.

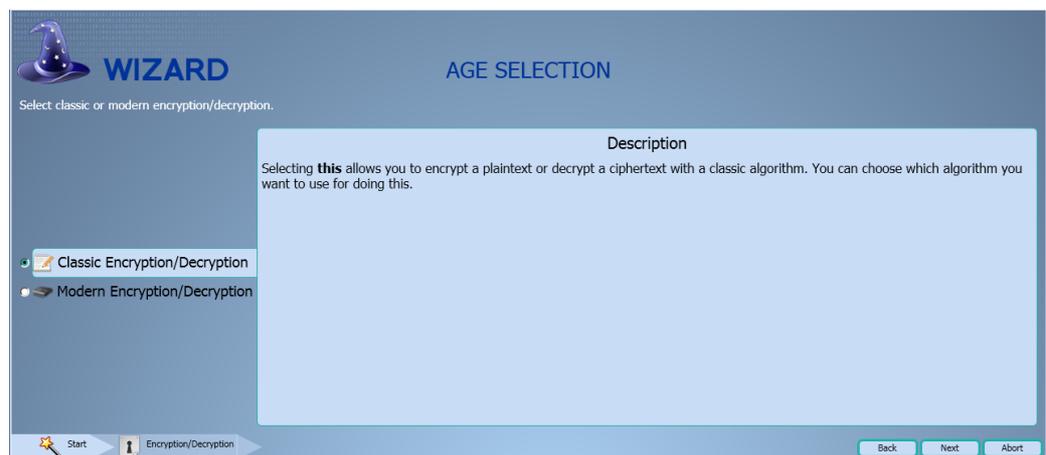


Abbildung 4: CrypTool 2 Wizard

Durch das Doppelklick auf die Aufgaben/Verfahren/Vorlagen kommt man im Wizard einen Schritt weiter. Diese intuitive Be-

wegungsmöglichkeit durch den Wizard wird, neben der Möglichkeit eines Doppelklicks auf die entsprechenden Inhalte, auch durch die Tasten unten Rechts „Back“ [Zurück], „Next“ [Weiter] und „Abort“ [Abbrechen] unterstützt. Die drei Tasten erlauben nicht nur Bewegung durch das Wizard Vorwärts, sondern auch Rückwärts oder auch den Abbruch jeglicher ausgeführter Benutzerhandlungen.

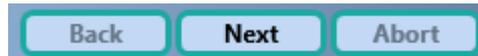


Abbildung 5: Tasten

Unten Links im Bild sieht der Benutzer ebenfalls einen Binärbaum der Aufgaben/Verfahren/Vorlagen, durch welche er sich momentan mit Hilfe des Wizard bewegt. So behält der Benutzer immer den Überblick über die Inhalte, mit welchen er sich momentan auseinandersetzt, sowie über die Bereiche, welchen der Inhalt zugeordnet ist. Jeder einzelne angezeigte Bereich ist über einen Klick auswählbar. Dies bietet einem Benutzer eine weitere Möglichkeit, einfach und bequem einen vorherigen Schritt seines Lernprozesses noch einmal zu betrachten und/oder zu bearbeiten.



Abbildung 6: Binärbaum der Aufgaben/der Verfahren

Wizard erlaubt nicht nur das schrittweise Erlernen von theoretischen Inhalten, sondern praktische Anwendung und Aneignung von Inhalten bzgl. des Crypto-Verfahrens. Es bleibt dem Benutzer überlassen den Schlüssel, das Passwort oder/und andere vorhandene Komponenten der Chiffre zu verändern.

 A screenshot of a web application interface for a substitution cipher. The interface has a light blue background. At the top, there is a dropdown menu labeled 'Encrypt or Decrypt:' with 'Encrypt' selected. Below it is another dropdown menu labeled 'Unknown symbols handling:' with 'Leave as is' selected. In the center, there is a text area labeled 'Message to encrypt/decrypt:' containing a paragraph of text about substitution ciphers. To the right of this text area is a text input field labeled 'Password:' with the word 'Crypto' entered. At the bottom left, there is a 'Password-Position:' label with a dropdown menu set to '1' and an 'Order:' label with a dropdown menu set to 'Descending'.

Abbildung 7: Substitution Chiffre zum Ausprobieren

Der Wizard zeigt am Ende der Chiffrierung den Klartext oben und den Geheimtext unten drunter an (siehe folgende Abbildung). Diese Textvisualisierung unterstützt das Lernen auf zwei Ebenen: Die erlernten theoretischen Inhalte und angewandten praktischen Inhalte werden zu einem Ganzen zusammengefügt. Der im oberen Fenster eingegebene Klartext wird in Echtzeit verschlüsselt angezeigt, so dass (vor allem bei einfachen Verschlüsselungsverfahren) kleine Schritte wie die Verschlüsselung von einzelnen Zeichen transparent gemacht werden. Dies regt Reflexionsprozesse an und fördert experimentelles Lernen.

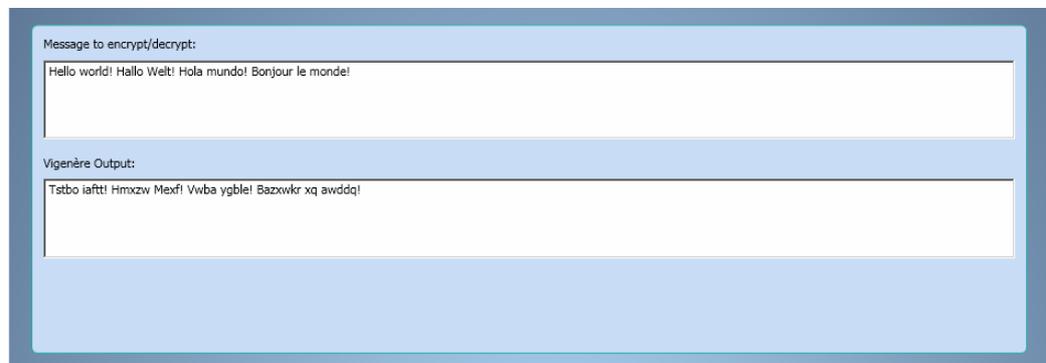


Abbildung 8: Vigenère Chiffre: Klar- und Geheimtext

5.2 CrypTool 2 Workspace Manager

Direkt bei dem letzten Ereignis der Verschlüsselung gibt es die Möglichkeit der Visualisierung durch den Workspace Manager (im Folgenden CWM abgekürzt), gekennzeichnet durch den roten dünnen Rahmen. Der Button für den CWM befindet sich oben rechts über dem Feld mit dem Klartext.

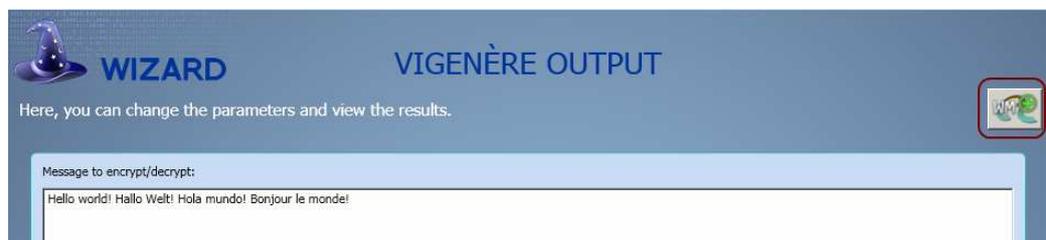


Abbildung 9: Übergang vom Wizard zu dem CWM

Der CWM ist weiteres wichtiges Werkzeug von CrypTool 2. Mit der Hilfe des CWM kann der Benutzer „Arbeitsblöcke“ erstellen, die Inhalte und Einstellungen von Blöcken bearbeiten und diese später abspielen. Aus drei Arten von Blöcken (Klartext-Block, Chiffre-Block und Geheimtext-Block) kann ein Diagramm erstellt werden. Je nach dem ob der Text ver- oder entschlüsselt wird, kommen die drei Blöcke in unterschiedlicher Reihenfolge zum tragen.

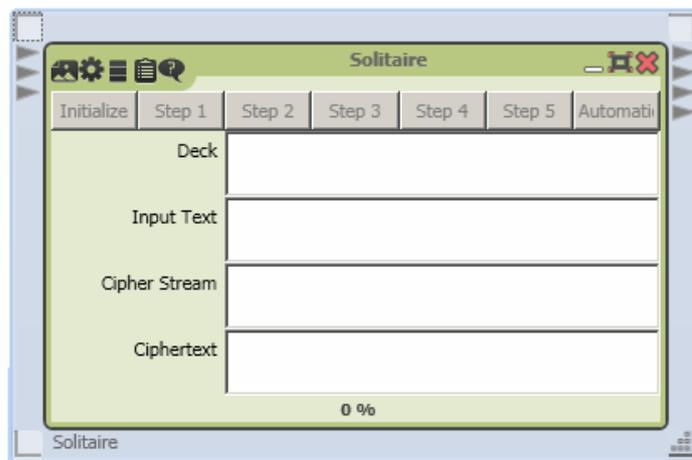


Abbildung 10: Klartext-Block bei der Solitaire Chiffre

Jeder Block weist fünf Menü-Icons auf: „*Presentation*“ [Präsentation] „*Settings*“ [Einstellungen], „*Log*“ [ich habe es für mich als Konsole übersetzt wegen der Ähnlichkeit], „*Data*“ [Daten] und „*Help*“ [Hilfe].

Durch das Anklicken der Icons gelangt der Benutzer in entsprechende Menüs.

Im Menü *Presentation* kann der Benutzer selber den Inhalt festlegen. *Presentation* ist das einzige Menü, das einzigartig für jeden Block ist. Dieses Menü wird nicht statisch (per default) von CWM erstellt.

Im Menü *Settings* hat der Benutzer die Möglichkeit verschiedene Einstellungen einer ausgesuchten Chiffre einzugeben bzw. diese zu verändern. Auch dieses Menü wird nicht statisch von CWM erstellt.

Im Menü *Log* findet der Benutzer unterschiedliche Informationen über den Kompilierungsstatus, die Fehlermeldungen und Warnungen. Diese Inhalte sind somit schon festgelegt durch das CWM.

Im Menü *Data* kann der Benutzer, je nach dem ob er den Text ent- oder verschlüsselt, entsprechende Texteingaben machen

(Text Output – beim Entschlüsseln, Text Input – beim Verschlüsseln). Je nach Verschlüsselungsverfahren ändern sich die zur Verfügung stehenden Optionen. Die Funktionalität ist von CWM festgelegt/begrenzt (der Benutzer kann nur die Texteingabe machen). Im Menü *Help* gelangt der Benutzer zur großen CrypTool 2 Online-Dokumentation.

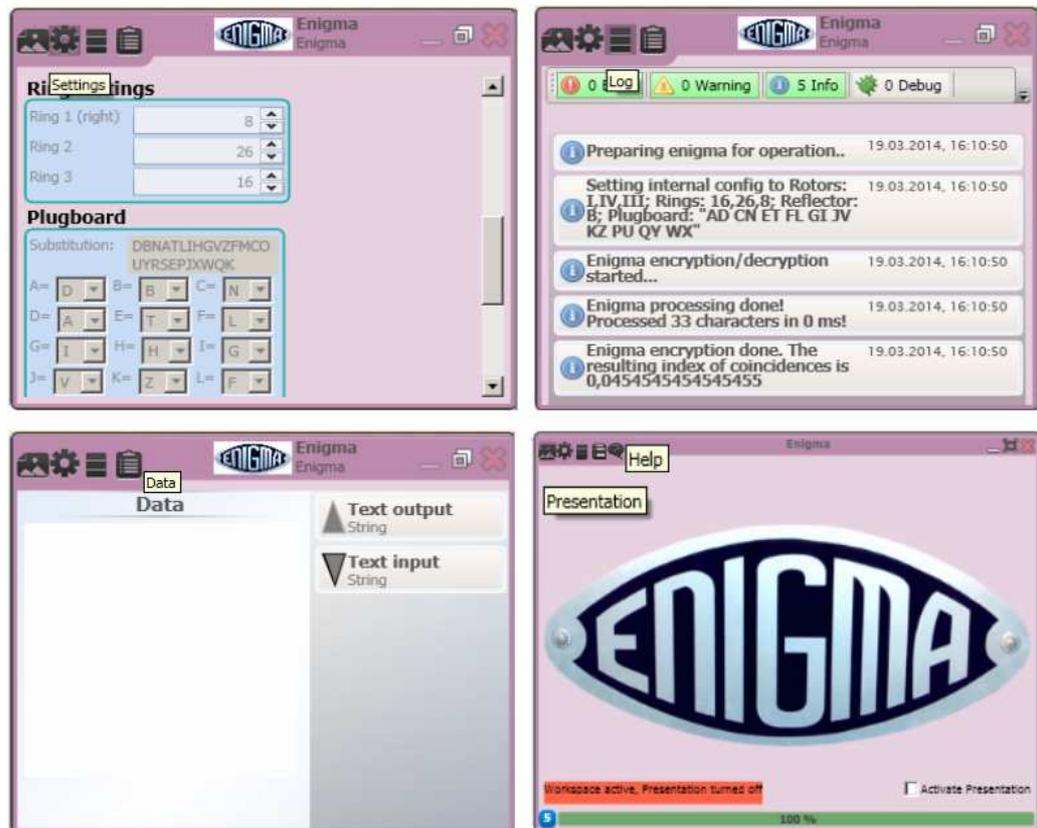


Abbildung 11: Menüs im Überblick

Über einen Rechtsklick an den Blockecken (links oben, rechts oben oder links unten) gelangt man in ein Kontextmenü (Abbildung 12), welches die fünf oben genannten Menüs noch mal zur Verfügung stellt. Außerdem erhält man im Kontextmenü Zugriff auf vier weitere Optionen, welche die räumliche Organisation verschiedener Blöcke untereinander unterstützen. Anmerkung: Sollte nur ein Block geöffnet sein, bewirkt das Anklicken einer solchen Option nichts.

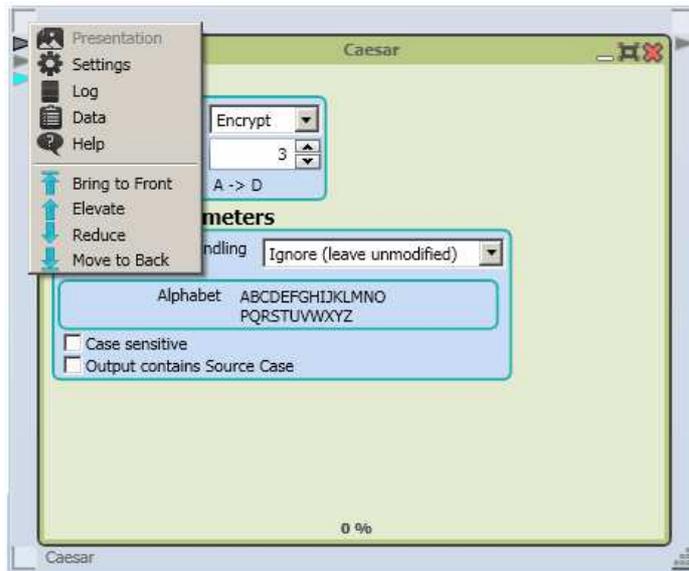


Abbildung 12: Kontextmenü

Bei der Arbeit mit dem CWM erscheinen die neuen Blöcke oft unten rechts im Bild und ganz klein, so das die Lage und Größe nicht gerade optimal für die Arbeit mit dem Block ist.

Der Block lässt sich durch Ziehen der unteren rechten Ecke (gekennzeichnet mit dem grünen Rahmen) per Maus vergrößern und verkleinern.

Der Block lässt sich auch bewegen: durch das Ziehen an den übrigen drei Ecken (gekennzeichnet mit dem blauen Rahmen).



Abbildung 13: Verschiebung und Vergrößerung

Die Blöcke lassen sich auch anders vergrößern und minimieren. Vergrößerung kann man auf andere zwei Weisen durchführen:
 → maximieren (Block wird nur ca. 20-25% größer)

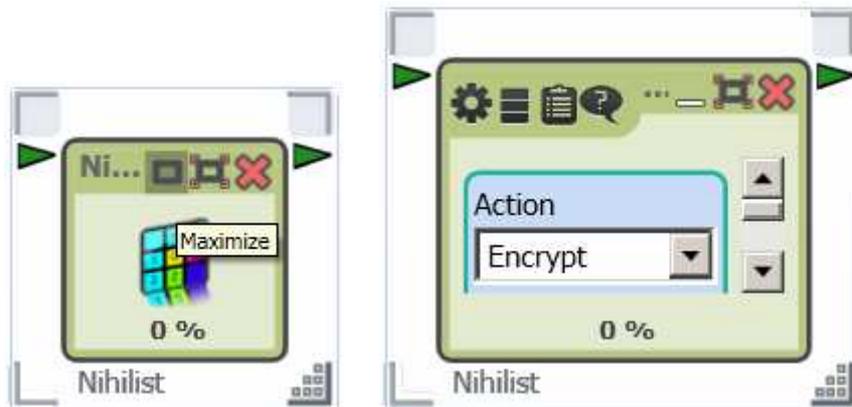


Abbildung 14: Maximierung eines Blocks

→ maximieren auf Vollbild (die ganze Arbeitsfläche wird ausgenutzt)

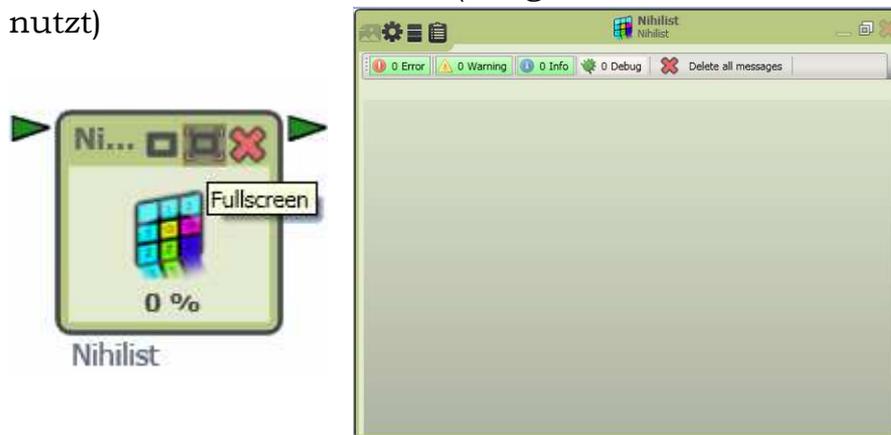


Abbildung 15: Maximierung auf Vollbild

Die Option zur Minimierung eines Blocks ist mit einem Standardzeichen für „Minimierung“ gekennzeichnet.

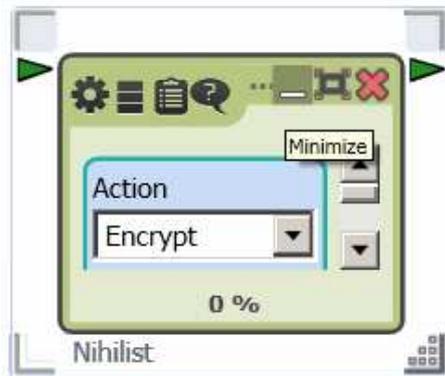


Abbildung 16: Minimierung eines Blocks

Um die Blöcke miteinander zu verbinden muss der Benutzer den Verbindungspfeil anklicken und ziehen (gekennzeichnet mit dem blauen Rahmen).

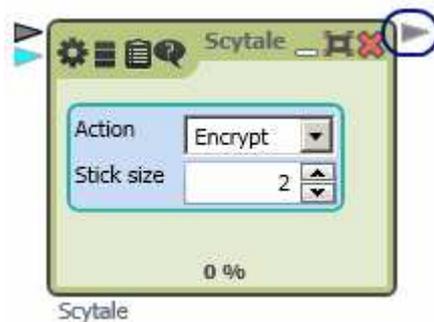


Abbildung 17: Verbindung der Blöcke

Sobald man den Verbindungspfeil in eine beliebige Richtung zieht, kriegt man alle Möglichkeiten die sich mit dem aktuellen Block verbinden lassen angezeigt. So kann der Benutzer selber eigene Ver- oder Entschlüsselungsalgorithmen entwickeln und ausprobieren.

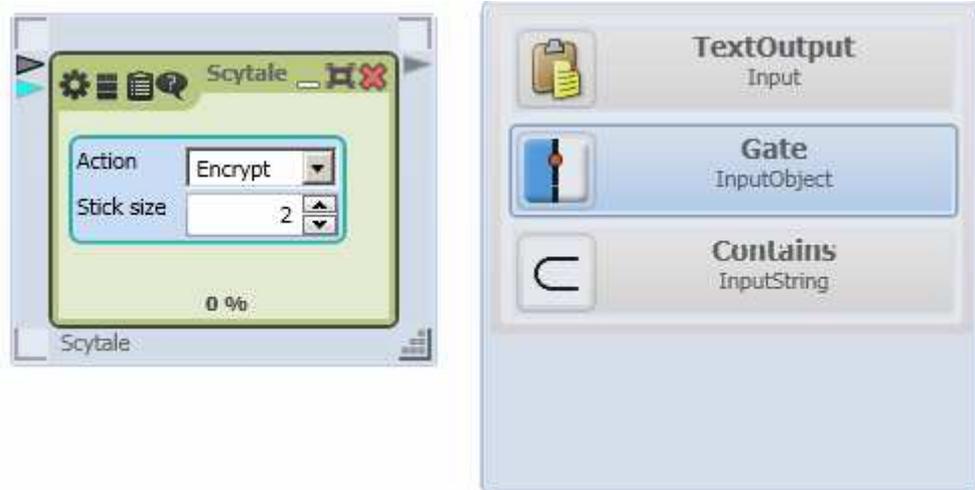


Abbildung 18: Verbindungsmöglichkeiten von Scytale

In der Mitte des Bildschirms entsteht ein Diagramm – die Visualisierung des Verfahrens, mit welchem der Benutzer die Nachricht verschlüsselt hat. Das Diagramm kann man in drei wichtige Blöcke unterteilen: Klartext-Block, Chiffre-Block und Geheimtext-Block.

In allen drei Blöcken kann der Benutzer Änderungen vornehmen, welche direkt übernommen werden.

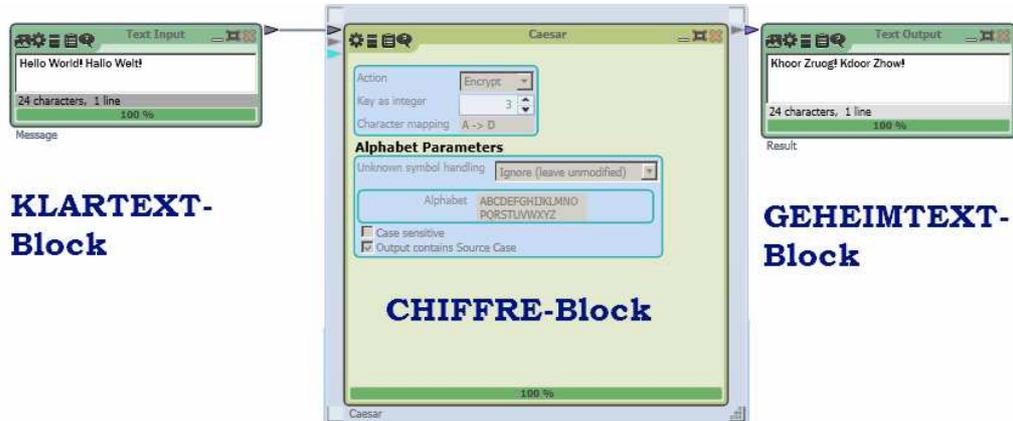


Abbildung 19: Visualisierung der Caesar Chiffre durch das CWM

Ganz wichtig sind mir die Farben der Blöcke erschienen. Ein Diagramm kann unterschiedlich gefärbte Blöcke beinhalten.

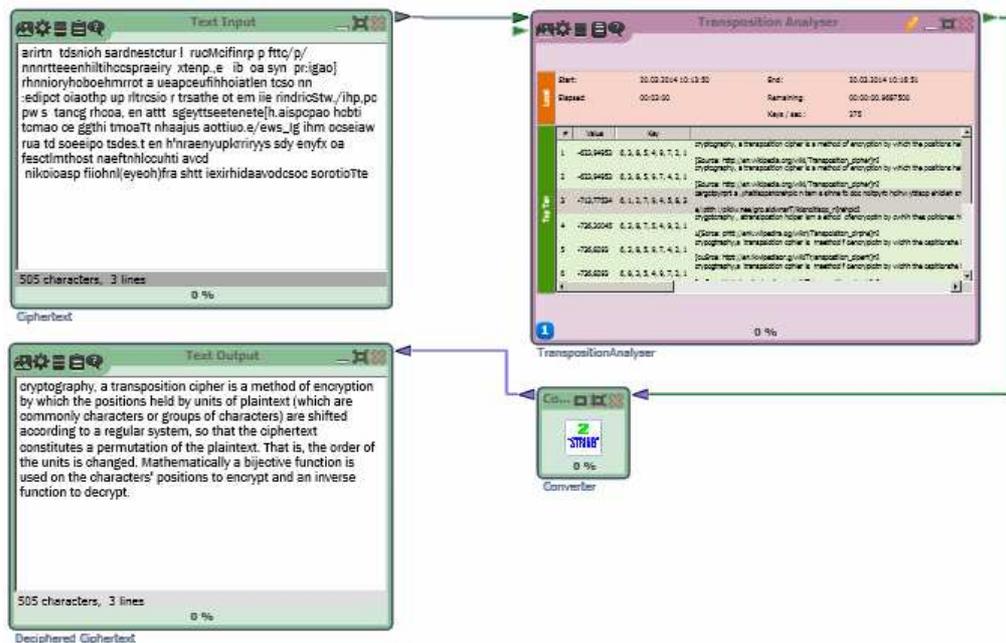


Abbildung 20: Transpositionsanalyse-Diagramm

Die Datentypen und Funktionen von Blöcken sind durch Farben festgelegt. So entspricht jedem Datentyp und jeder Funktion eine bestimmte Farbe. An dem oberen Diagramm z. Bsp. sieht man, dass die Farben vom ersten und letzten Block gleich sind. So wird durch die Farben dem Benutzer verdeutlicht, dass Input und Output den gleichen Datentyp und die gleiche Verfahrensklasse haben.

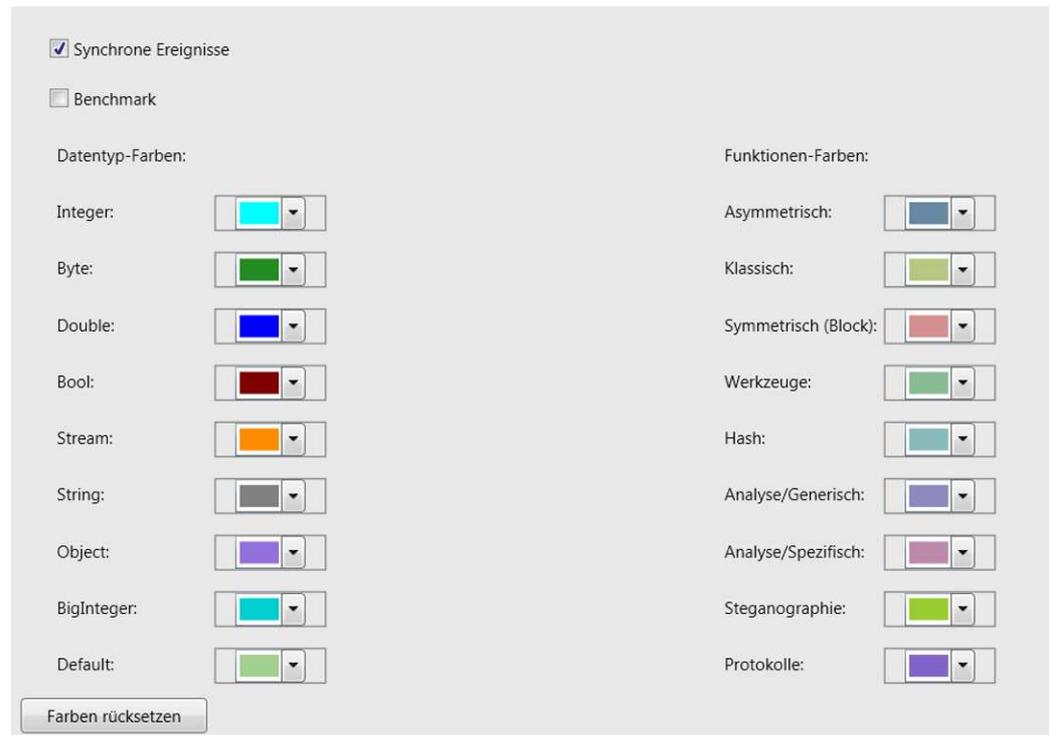


Abbildung 21: Datentyp- und Funktionen-Farben

Eine weitere wichtige Hilfsfunktion von CWM ist der Textblock, dieser lässt sich einfach einfügen und an einer erwünschten Stelle platzieren. Um einen Text- bzw. Kommentarblock einzufügen muss der Benutzer eine entsprechende Option auswählen, welche sich oben rechts auf der Komponentenleiste befindet.



Abbildung 22: Komponentenleiste von CWM

Führt man den Mauszeiger in einen Kommentarblock, wird dem Benutzer eine zusätzliche Editorenleiste angezeigt. Diese Leiste ist dem Benutzer aus MS Word bekannt. So kann der Benutzer den Textblock ganz schnell und einfach editieren, ohne sich mühsam mit einer unbekanntenen Editorenleiste vertraut zu machen.

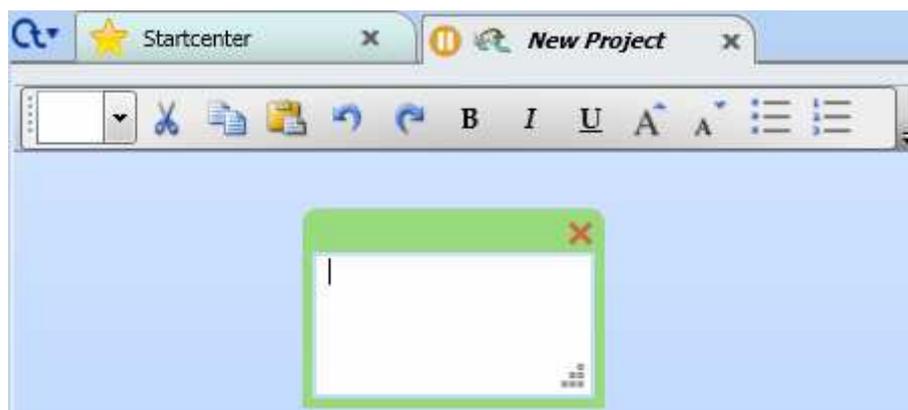


Abbildung 23: Textblock

Kapitel 6

Homepage

6.1 Aufbau der Homepage

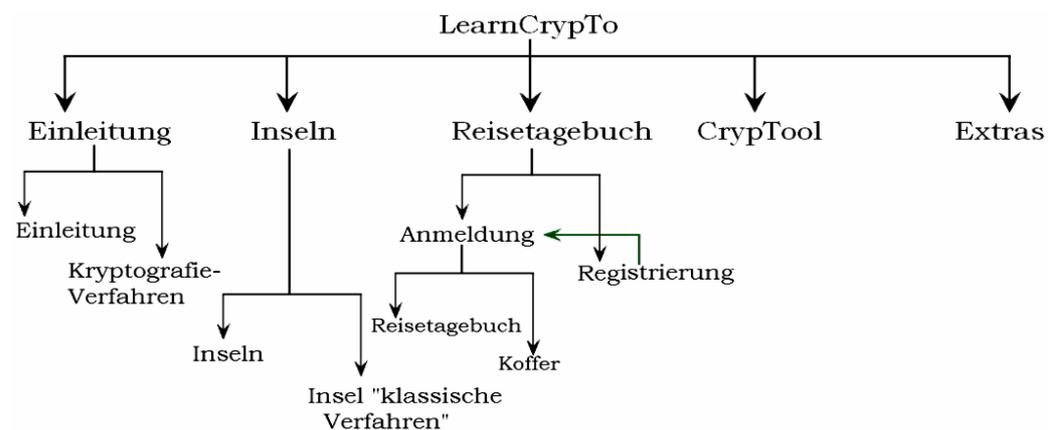


Abbildung 24: Navigation der LearnCrypTo-Seite

Auf Abb. 24 sieht man, wie die LearnCrypTo-Homepage aufgebaut ist. LearnCrypTo hat ein übersichtliches Menü, welches zwei Menüleisten (oben und unten) enthält:



Abbildung 25: obere Menüleiste



Abbildung 26: untere Menüleiste

Diese erleichtern dem Benutzer die Navigation durch die LearnCrypTo-Seiten. Wie man aus den Abb. 25 und Abb. 26 sieht bestehen die Menüleisten aus jeweils gleichen fünf Menüpunkten. Diese Menüpunkte sind kurz und präzise formuliert, so dass die Benutzer sich schnell ein Bild von deren Inhalten machen können.

Der Menüpunkt „Einleitung“ bietet dem Benutzer die Inhaltsunterpunkte *Einleitung* und *Kryptografie-Verfahren* an. Die *Einleitung* wird sehr hilfreich für Anfänger sein, da sie ein Einblick in die Inhalte der LearnCrypTo Seite und auf Wunsch auch in den CrypTool 2 darstellt.

Unter dem Unterpunkt *Kryptografie-Verfahren* befinden sich Informationen zu Kryptografie-Verfahren die auf Wunsch abgerufen werden können.

Hier findet der Benutzer eine Visualisierung der wichtigsten Kryptografie-Verfahren durch „Verfahren-Bäume“ (ein Strahl auf dem links und rechts Verfahren gleicher Klasse hängen) und ein Zeitstrahl (Abb. 27), welcher einen groben Überblick über die wichtigsten Ereignisse der Kryptografie nach Simon Sighn gibt.

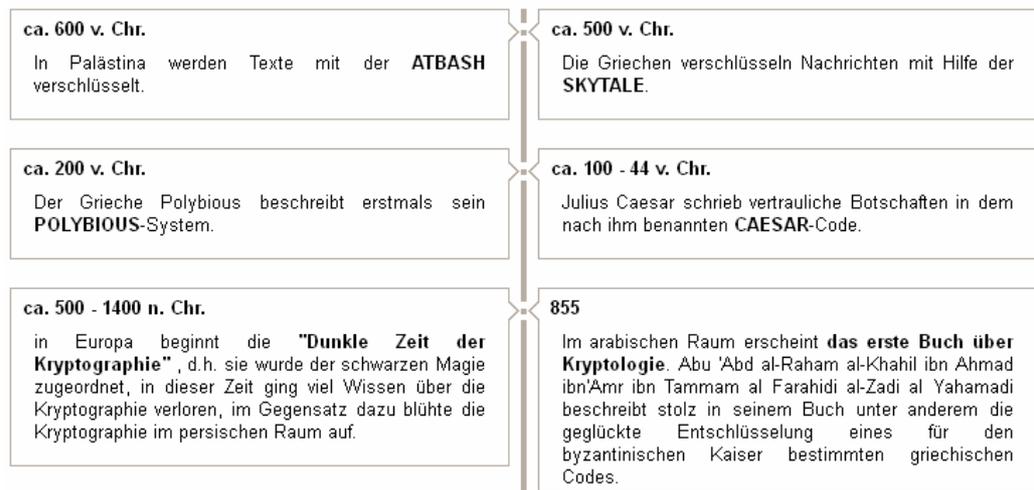


Abbildung 27: Zeitstrahl

Dem Benutzer ist die Entscheidung überlassen wie intensiv er sich mit Inhalten der *Einleitung* und *Kryptografie-Verfahren* auseinandersetzt, deswegen erhält er mehr Informationen zu diesen Unterpunkten, indem er einer entsprechenden Verlinkung (Abb. 28 gekennzeichnet mit dem blauen Rahmen) folgt.

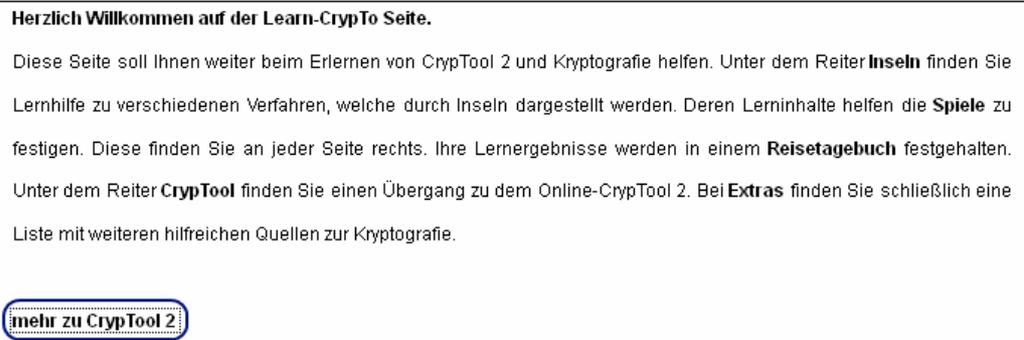


Abbildung 28: Verlinkung

Der Menüpunkt „Inseln“ bietet dem Benutzer visualisiert durch den *Cryptoplanet* Zugang zu Informationen über alle im CrypTool 2 implementierten Verfahren, Protokollen und darin enthaltenen Werkzeugen.

Der *Cryptoplanet* enthält 8 Inseln:

- klassische Verfahren,
- moderne symmetrische Verfahren,
- moderne asymmetrische Verfahren,
- Steganographie,
- Hasch Funktion,
- spezifische Kryptoanalyse,
- generische Kryptoanalyse,
- Protokolle

und die Cryptosee (beinhaltet alle Informationen zu Werkzeugen von CrypTool 2).



Abbildung 29: Cryptoplanet

Direkt darunter findet der Benutzer eine Überleitung zu *der ersten Insel*. Dies ist dazu gedacht den Benutzer durch die Kryptografie und CrypTool 2 zu begleiten. Am Anfang kriegt der Benutzer erst die Insel „klassische Verfahren“ zum Kennenlernen gestellt. Die Insel enthält vierzehn Orte (Abb. 30). Jeder Ort stellt ein markantes Beispiel des klassischen Verfahrens dar.

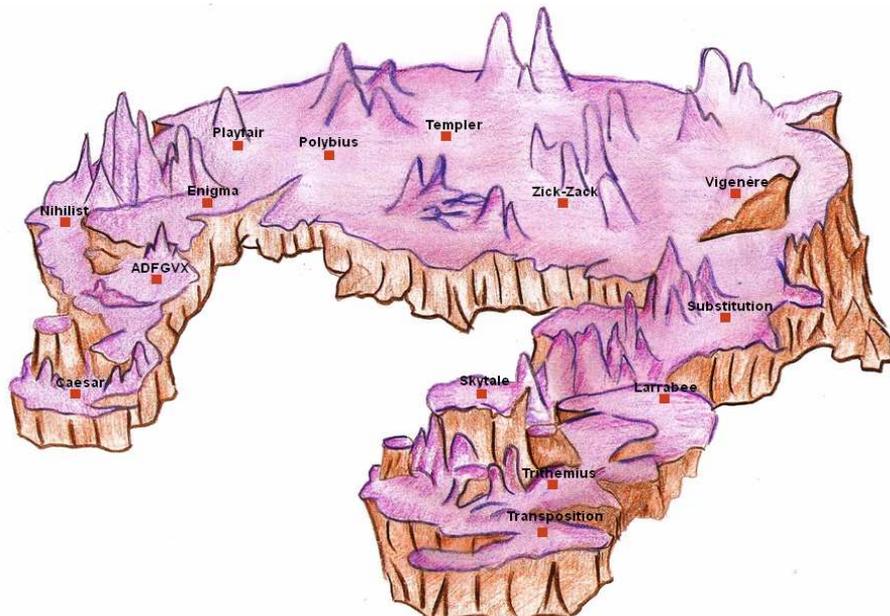


Abbildung 30: Insel „klassische Verfahren“

Nach dem Anklicken eines der Orte (rote Quadrate) wird man auf eine entsprechende Cryptool-Online Dokumentation weitergeleitet. Hier hat der Benutzer nicht nur die Möglichkeit über das ein oder andere Verfahren nachzuschlagen, sondern auch einen entsprechenden Algorithmus auszuprobieren.

Unter dem Menüpunkt „Reisetagebuch“ gelangt der Benutzer in eigenes Lerntagebuch, welches weiterhin als *Reisetagebuch* bezeichnet wird.

Das Reisetagebuch hat folgenden Aufbau: auf der linken Seite werden die Ergebnisse (momentan klappt es nur mit dem Anagramm-Spiel, da ich nur bei dem Spiel Zugriff auf entsprechende Daten habe) von jeweiligem Benutzer automatisch in entsprechender Form eingetragen und gespeichert. So hat der Benutzer Zugriff auf alle eigenen Lernspielergebnisse. Diese können durch das „Blättern“ durch das Reisetagebuch aufgerufen werden.

Auf der rechten Seite des Reisetagebuches (Abb. 31) finden sich Einträge, die durch den Benutzer vervollständigt bzw. verfasst werden müssen. Ob dem Benutzer das Lernen Spaß gemacht hat und ob er sich bei dem Lernen wohl gefühlt hat, kann nur der Benutzer beantworten, deswegen kann diese Art der Einträge nicht automatisch angelegt werden.

Um den Benutzer ein bisschen an dieser Stelle zu entlasten, gibt es eine Smiley-Checkliste bzw. -Skala. So kann der Benutzer seine Stimmung durch Smileys anzeigen lassen.

Die durch den Benutzer ausgesuchten Smileys werden abgespeichert.

So kann verfolgt werden, ab welchem Zeitpunkt/Thema der Benutzer sich beim Lernen nicht wohl gefühlt hat. Es kann bei Bedarf an die entsprechende Stelle zurückgekehrt werden um den Lernprozess an dieser Stelle noch einmal aufzunehmen.

Hat mir das Lernen heute Spaß gemacht?

Wie habe ich mich beim Lernen gefühlt?

Platz für meine Notizen:

...

speichern

Abbildung 31: rechte Seite des Reisetagebuchs

Der Zugriff auf das Reisetagebuch erfolgt erst nach Anmeldung (Abb. 32, gekennzeichnet mit blauem Rahmen), durch Letztere kann jedem Benutzer sein eigenes Reisetagebuch mit entsprechenden Inhalte zugewiesen werden.

Anmeldung

Bitte, füllen Sie die Anmeldeformular aus. Die wichtigsten Felder sind mit dem * gekennzeichnet.

Persönliche Informationen:

*Name:

*Passwort:

Falls Sie keinen Account haben, erstellen Sie neuen Account:

Abbildung 32: Anmeldung

Eine Anmeldung kann nur erfolgen, falls der Benutzer schon registriert ist. Falls der Benutzer noch kein Reisetagebuch angelegt/angemeldet hat, erhält er die Möglichkeit einen Account zu erstellen (Abb. 32, gekennzeichnet mit dem grünen Rahmen). Nach dem der Benutzer den Button „erstellen“ drückt, gelangt er automatisch zur Registrierung (Abb. 33).

Registrierung

Persönliche Informationen:

*Name:

*Vorname:

*Login:

*Passwort:

*Passwort Wiederholung:

Abbildung 33: Registrierung

Eine erfolgreiche Registrierung führt den Benutzer auf die erste Reisetagebuchseite. Da es noch keine Einträge von dem Benutzer gibt, wird er darauf aufmerksam gemacht – mit einer entsprechenden Meldung und dem Vorschlag das Anagramm-Spiel zu spielen (entsprechende Verlinkung auf das Spiel), um den ersten Eintrag ins Reisetagebuch zu erstellen.

Sobald der Benutzer das Spiel verlässt, werden seine momentanen Ergebnisse in das Reisetagebuch eingetragen. Danach kann der Benutzer seinen Gefühlszustand beim Lernen durch Smileys abschätzen (Abb. 34, gekennzeichnet mit grünem Rahmen) und Notizen über seine Gefühle bzw. Lernvorgänge hinterlassen (Abb. 34, gekennzeichnet mit dem senffarbigem Rahmen). Die Notizen lassen sich jederzeit ändern.

Die Gefühle, ausgedrückt durch Smileys, lassen sich nicht mehr editieren. Somit wird sicher gestellt, dass der jeweils momentane Gefühlszustand des Benutzers beim Lernen/Spielen festgehalten und nicht nachträglich verändert wird.



Abbildung 34: Reisetagebuch

Der Benutzer hat die Möglichkeit eigene Einträge im Reisetagebuch nochmals durchzulesen und ggf. zu editieren. Durch den Pfeil unten (Abb. 34, gekennzeichnet mit dem blauen Rahmen) kann der Benutzer durch das Reisetagebuch navigieren.

Insgesamt können durch das Benutzer-Feedback vier unterschiedliche Situationen entstehen:

Situation 1: Das Lernen hat dem Benutzer (eher) Spaß gemacht und er hat sich beim Lernen (eher) wohl gefühlt.

In dieser Situation ist der Benutzer vollkommen zufrieden. Der CryToPhant gibt eine schriftliche Rückmeldung, in welcher er den Benutzer lobt und seine Freude über den Spaß des Benutzers zum Ausdruck bringt.

Situation 2: Das Lernen hat dem Benutzer (eher) Spaß gemacht, er hat sich aber beim Lernen nicht (alzu) wohl gefühlt.

In dieser Situation erhält der Benutzer ein Feedback vom CrypToPhant in Form einer Aufmunterung und einer Bitte um Selbstreflexion. Darüber, dass der Benutzer Spaß hatte, freut sich der CrypToPhant natürlich trotzdem.

Situation 3: Das Lernen hat dem Benutzer keinen Spaß gemacht, aber er hat sich beim Lernen wohl gefühlt.

In dieser Situation versucht das Reisetagebuch den Benutzer ebenfalls aufzumuntern und bittet ihn nochmals zu Üben.

Situation 4: Das Lernen hat dem Benutzer kein Spaß gemacht und er hat sich beim Lernen nicht wohl gefühlt.

Die Hauptaufgabe des Reisetagebuches ist es an dieser Stelle den Benutzer nicht nur aufzumuntern, sondern wieder für das Lernen motivieren (Vgl. Spitzersche Forderungen). Deshalb wird Selbstreflexion angeregt. Gibt der Benutzer an, gelangweilt zu sein, macht der CrypToPhant darauf aufmerksam, dass es bestimmt noch spannendere Übungen gibt. Der CrypToPhant ermuntert den Benutzer.

Eine weitere Visualisierung und Lernhilfe ist der Reisekoffer des Benutzers. Durch eine Verlinkung im Reisetagebuch gelangt der Benutzer zu seinem Koffer.

Die Funktionsweise des Koffers sieht wie folgt aus: der Benutzer sieht einen aufgeklappten Koffer. In oder neben diesem finden sich Lernbegriffe. Die Begriffe, die der Benutzer beim Spielen kennen gelernt hat, kann er in den Koffer ziehen und auf seiner weiteren Reise auf dem *Cryptoplanet* mitnehmen (Abb. 35). Der Benutzer wird an dieser Stelle darauf hingewiesen nur bekannte und durchdrungene Begriffe in den Koffer zu packen.

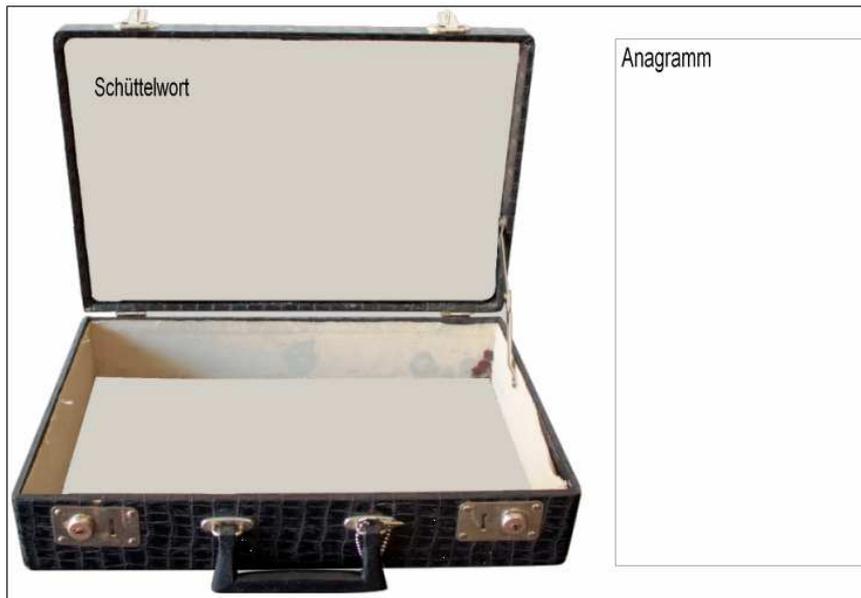


Abbildung 35: Koffer, gefüllt mit einem Begriff

Der Benutzer hat die Möglichkeit Begriffe aus dem Koffer raus-zuziehen (Abb. 36), falls diese dem Benutzer nichts sagen. So sind im Koffer nur die Sachen „gepackt“, die der Benutzer wichtig findet, versteht und oder bereits trainiert hat. Alles Andere liegt außerhalb, kann aber jederzeit durch den Benutzer nach dessen Gutdünken in den Koffer „eingepackt“ werden.



Abbildung 36: leerer Koffer

Der Menüpunkt „CrypTool 2“ führt den Benutzer zum CrypTool 2 Portal (Abb. 37). Auf dieser Seite findet der Benutzer viele andere hilfreiche Informationen zu Verfahren und CrypTool 2.



Abbildung 37: CrypTool 2 Portal

Der Menüpunkt Extras bittet dem Benutzer eine Liste mit unterschiedlichen Verlinkungen zu Kryptografie-, Kryptoanalyse- und CrypTool-Seiten. So kann der Benutzer weitere Informationen direkt auf der Homepage finden.

6.2 Pädagogisch sinnvoller Aufbau der Homepage

Im Folgenden möchte ich die im Kapitel 3.4 vorgestellten vier Einflussfaktoren auf das Lernen nach Spitzer noch mal aufführen und beschreiben, welche konkreten Maßnahmen ich für die Umsetzung seiner Forderungen bei Aufbau und Gestaltung der Homepage ergriffen habe. Ziel ist es, anhand der Forderungen Spitzers zu zeigen wodurch die Homepage und speziell das Reisetagebuch das Lernen unterstützt. Da Spitzers Forderungen sich konkret an den Unterricht in der Schule richten, werde ich dessen Forderungen beim Bedarf neu interpretieren. Ich konnte in meiner Homepage einige Aspekte unterbringen, welche gleich mehreren Forderungen Spitzers positiv begegnen. Daher kann es zu Mehrfachnennungen bzw. Wiederholungen kommen.

Einflussfaktor Emotionen:

Jeder Mensch ist mehr oder weniger emotional. Beim Lernen in der Schule genau wie beim Lernen an dem Rechner Emotionen haben eine besondere Aufgabe: Lerninhalte werden nicht nur mit Lernsituation verknüpft sondern auch mit Emotionen in diese Lernsituation.

→ angstfreie Lernatmosphäre:

- Das Logo CrypToPhant führt den Benutzer in das neue Wissen ein. („Ich bin nicht allein.“-Gefühl).
- Humor: Das Logo CrypToPhant und dessen Aussehen basiert auf einem Sprachspiel.
- Bunte Bilder an der Seite wirken vertraut und können Berührungsängste abbauen.

→ wertschätzender und respektvoller Umgang:

- Der Lernende wird gesiezt.
- Die Navigation funktioniert simpel, Umwege werden vermieden.
- Die Homepage ist gut lesbar.

→ Positive Grundstimmung herstellen:

- Beim Anagrammspiel sorgt der CrypToPhant durch unterstützende Sprüche dafür, dass die Grundstimmung des Lernenden immer auf dem hohen Niveau bleibt.

→ Fehler als Chance sehen:

- Wenn der Benutzer ein Fehler beim Anagrammspiel macht, wird er nicht getadelt, sondern vom CrypToPhant zu einem neuen Versuch ermuntert.

- Wenn ein Benutzer im Tagebuch ein negatives Feedback zu seinen Übungen gibt, wird er ermuntert und/oder zur Reflexion aufgefordert.
- kein Notendruck:
- Die Lernleistung des Benutzers wird im Reisetagebuch festgehalten. Als Rückmeldung zu seiner Leistung erhält der Benutzer keine standardisierten Noten (also keine Bewertung wie sehr gut, gut,...).
 - Es wird ausschließlich mit positiv formulierter Sprache gearbeitet („x% richtig“, nicht: „x% falsch“).
 - Es wird in der ersten Person („Heute habe ich...“ nicht „Heute hast du...“) formuliert. Dadurch sollte der Benutzer auch bei schlechten Lernergebnissen nicht den Eindruck bekommen er werde von jemand anderem getadelt.
- Trennung von Lern- und Leistungsüberprüfungen:
- Lernüberprüfung durch Aufgaben wird nicht im Reisetagebuch festgehalten. Dagegen werden die Ergebnisse vom Anagrammspiel durch die automatischen Einträge in das Reisetagebuch festgehalten.
- Lernorientierung/Unterstützung:
- Der Benutzer hat die Möglichkeit die gleichen Lerninhalte beim Bedarf mehrmals aufzurufen. So kann sich der Benutzer gut auf die Übungsaufgaben vorbereiten.
 - eLearning-Elemente erweitern didaktische Möglichkeiten und können dadurch Benutzer zusätzlich für das Lernen motivieren.
- Stärkung des Selbstvertrauens:
- Alle Übungsaufgaben sind als Spiele gedacht, so fühlt sich der Benutzer beim Üben möglicherweise entspannter.
 - Im Reisetagebuch werden Lernergebnisse gespeichert, die Lernerfolg und -Fortschritt des Benutzers festhalten.
 - Der Benutzer wird beim Anagrammspiel bei richtigen Antworten gelobt, bei falschen Antworten aufgemuntert.
- positive Einstellung zum Lernen fördern:
- Das Reisetagebuch fördert und unterstützt den Benutzer beim Lernen durch die automatischen Einträge und Einträge des Benutzers. Der Nutzer wird auch bei Misserfolgen zu erneuten Versuchen angeregt.

Einflussfaktor Aufmerksamkeit:

→ Lernen durch eigenes Tun:

- Alle Spiele und Aufgaben sind interaktiv ausgelegt.

→ eigene Regeln beim Lernen aufstellen (z. Bsp. bzgl. Pausenzeiten)

- Die Homepage steht 24 Stunden pro Tag und 7 Tage die Woche zur Verfügung.
- Der Benutzer kann selbst über Zeiteinteilung und Reihenfolge der Aufgabenbearbeitung bestimmen. Er muss nicht nur selbst Handeln, sondern sein Handeln auch selbst planen. Dazu bieten dem Benutzer die Visualisierung des Themas durch den Cryptoplanet und die Timeline, sowie ein strukturierender Einleitungstext auf der Startseite Hilfe.

→ Lernen mit allen Sinnen

- Es werden folgende Sinne angesprochen: Sehen (Texte und Bilder), Tastsinn (Tippen)

Einflussfaktor Motivation:

→ Lernen mit Überraschungen:

- Der CrypToPhant unterstützt beim Anagrammspiel den Benutzer beim Lernen, nickt bei richtigen Antworten und verneint falsche Antworten.
- Der CrypToPhant gibt unterschiedlich formuliertes Feedback. Ein Benutzer könnte gespannt erwarten, was der CrypToPhant als Nächstes sagt.
- Die Einträge des Benutzers in das Reisetagebuch werden aufgegriffen und entsprechend ausgewertet. Der Benutzer wird gelobt oder aufgemuntert je nach seinem Eintrag.

→ Bezug zur Lebenswelt aufbauen:

- Es wird davon ausgegangen, dass der Benutzer selbst über den praktischen Nutzen und somit den Bezug der Lerninhalte zu Lebenswelt weist. Daher gehen wir einen Schritt weiter. Es finden sich verschiedene Hinweise zum Lebensbezug des Lerninhalts in anderen Kulturen zu unterschiedlichen Zeiten auf der Website.

→ Sinn und Bedeutung des Lerninhalts erkennen lassen:

- Erläuterungen einzelner Elemente des Lerninhalts
- Verdeutlichungen von Strukturen durch Organigramme

→ Erhöhen der Lernfreude:

- durch Ermöglichen von Erfolgen:

- Ein sinnvolles Vorgehen (Aufgabenreihenfolge: Start bei Insel „Klassische Verfahren“) wird als Empfehlung ausgesprochen.
- Die Aufgaben können in beliebiger Reihenfolge bearbeitet werden. Fällt einem Benutzer das Ausprobieren

- ren einer Chiffre schwer, kann er jederzeit abbrechen und sich einer anderen Chiffre zuwenden.
- Fällt einem Benutzer das Ausprobieren eine Chiffre schwer, kann er sich jederzeit den entsprechenden Informationstext durchlesen.
- Jede Aufgabe auf der Website kann beliebig oft gelöst werden. Egal wie viele Misserfolge ein Nutzer beim Lösen einer Aufgabe hat, es wird ihm immer eine weitere Chance gegeben.
- durch Lob:
 - Durch den CryptoPhanten bei dem Anagrammspiel.
- durch Begeisterung des Lehrenden für den Lernstoff:
 - durch das Aufführen kultureller und historischer Aspekte der Kryptografie.
 - Durch die Visualisierung mittels des Cryptoplaneten und den einzelnen Inseln.
- durch Fehlerfreundlichkeit:
 - Im Anagrammspiel hat man unbegrenzte Anzahl von Versuche um ein abgefragtes Wort einzugeben.
 - Fällt einem Benutzer das gesuchte Wort im Anagrammspiel dennoch nicht ein, so kann er zum nächsten gesuchten Wort springen.

Einflussfaktor Vorwissen:

→ Klarheit des Lerninhaltes:

- Bei der Menüpunkt Einleitung wird die klare und eindeutige Struktur der Homepage preisgegeben.

→ Anknüpfen an bereits Gelerntes:

- Dies fehlt beim Gestalten eine Webseite wesentlich schwerer als im Klassenraum. Während ein Lehrer seine Schüler und deren Wissen kennt muss ich als Webentwickler eine Seite für mir unbekannte Benutzer entwickeln. Da die Seite vielen Benutzern ermöglichen soll sich mit den Lerninhalten vertraut zu machen, sind die Seiteninhalte für Anfänger ausgelegt.

→ Lerninhalte strukturiert darbieten:

- Der Cryptoplanet dient dem Benutzer als strukturierter Übersicht über alle Sachinhalte. Der Benutzer kann sich zunächst auf eine Insel begeben und einen Ort erkunden.
- Der Menüunterpunkt *Einleitung* beinhaltet einen Text zur Inhaltsstrukturierung und Navigationshilfe.

→ Skelett vor Detail:

- Durch den Cryptoplanet wird dem Benutzer zunächst eine skelettartige Struktur des Sachinhaltes präsentiert und er kann sich gezielt zu detaillierten Informationen seiner Wahl bewegen.
- Verknüpfung mit der Realität:
- Der Inhalt an sich bietet dem Benutzer einen hohen Grad an Auseinandersetzung mit der Realität. Auch wenn der Spielkontext (siehe z.B. Anagramm) mal realitätsfern erscheinen mag, funktionieren die Übungsaktivitäten an sich (Ver- und Entschlüsseln) als klassische Simulation der Realität.
- Lernen im eigenen Tempo:
- Die Homepage steht 24 Stunden pro Tag und 7 Tage die Woche zur Verfügung. So kann der Benutzer selber sein Lerntempo bestimmen.
- Umgang mit Heterogenität:
- Durch die Möglichkeit sich mit verschiedenen Chiffren auseinander zu setzen, wird unterschiedlichen Interessenslagen begegnet.
 - Durch unterschiedliche Aufgabetypen (Spiel, Textaufgabe, ...) wird unterschiedlichen Lerntypen entsprochen.

Kapitel 7

Technischer Hintergrund

7.1 MySQL

Als Datenbankmanagementsystem wird MySQL zur Unterstützung der Arbeit von LearnCrypTo-Homepage verwendet. MySQL ist frei zugänglich und ist verschiedene Betriebssysteme verfügbar. MySQL bildet eine Grundlage für dynamische Seiten der LearnCrypTo-Homepage: des Reisetagebuchs, der Anmeldung und der Registrierung.

Vorteilhaft ist, dass MySQL grundsätzlich einen MySQL-Server vorsieht, auf dem Daten gespeichert sind, sowie einen oder mehrere MySQL-Clients, welche Anfragen an den Server schicken und von letzterem Antworten empfangen.

Auf diesem Datenbankmanagementsystem können mehrere Datenbanken erstellt werden.¹¹ Für die LearnCrypTo-Homepage habe ich eine Datenbank mit dem Namen *cryptodatabase* angelegt. In der *cryptodatabase*-Datenbank sind zwei Tabellen angelegt: *books* und *users*. Bei Bedarf kann die Anzahl der Tabellen vergrößert werden.

Die Tabellen können von gleichem oder (wie bei mir) unterschiedlichem Typ sein. Der Typ der Tabellen bestimmt, welche Speicherengine (z.B. InnoDB, MyISAM, MERGE, BDB) verwendet wird.

Die Tabelle *books* hat ein InnoDB Speichersubsystem. *„InnoDB eignet sich vor allem bei großen Datenbanken wo viele Daten miteinander verknüpft sind. Wenn hier Daten gelöscht werden, löscht InnoDB alle referenzierten Daten automatisch mit. Das macht es der Anwendung hinter der Datenbank leichter die referentielle Integrität einzuhalten.“*¹²

Die Tabelle *users* hat ein MyISAM-Speichersubsystem. MyISAM ist praktisch *„bei kleinen Datenbanken oder Anwendungen wo viel und oft Daten geändert werden. Hier ist MyISAM deutlich performanter, weil INSERT und UPDATE schneller sind. Und natürlich wenn man Texte durchsuchen möchte (Volltextsuche).“*¹²

Hauptvorteile vom MyISAM gegenüber InnoDB sind höhere Stabilität und Geschwindigkeit.

¹¹ vgl. <http://de.wikipedia.org/wiki/MySQL>

¹² <http://web-union.de/382>

Jede Tabelle besteht aus Spalten. In Spalten werden Vorgaben zum Datentyp (z. Bsp. Varchar, Integer oder Text) gespeichert. Durch das Betriebssystem wird die maximale Größe der Tabellen begrenzt.

MySQL verfügt über viele eigene Speichersubsysteme (Engines). Beim Bedarf kann MySQL auch um weitere, nicht im MySQL-Paket mitgelieferte Speicherengines erweitert werden. Durch die Engine kann ein spezielles Einsatz-Szenario optimiert werden. So liegt z. Bsp. die Verwaltung von Transaktionen, von Indizes und der referenziellen Integritäten in der Hand der Engine.

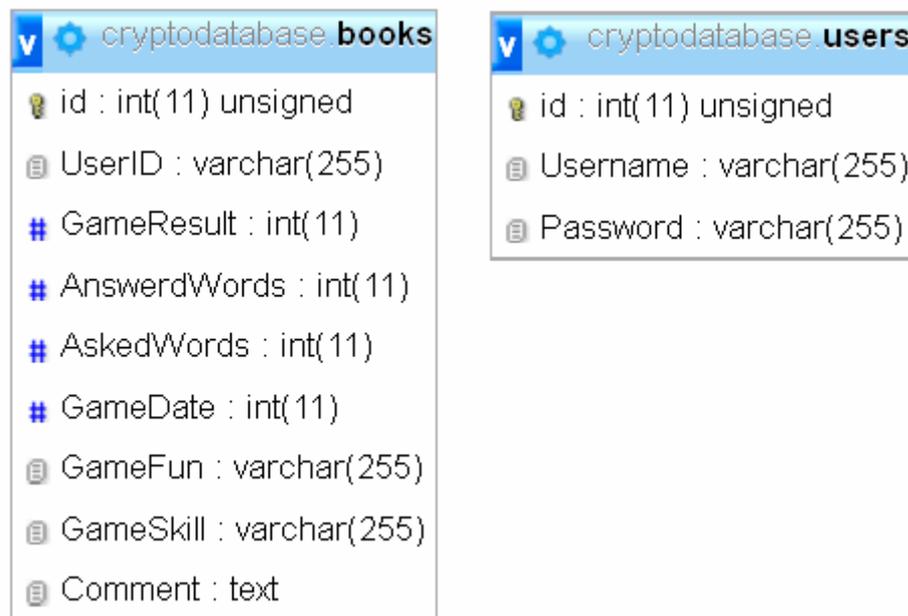


Abbildung 38: Datenbank *cryptodatabase*

Wie man in Abb. 38 sehen kann hat Tabelle *book* 9 Felder, welche Folgendes speichern:

→ id: speichert ID vom Anagramm-Spiel. So erhält das Spiel bei jedem Neustart eine eindeutige ID, welche man einem bestimmten Benutzer zuweisen kann.

Damit bei jedem neuen Spiel die ID nicht gleich bleibt, muss man das id-Feld als „AUTO_INCREMENT“-Feld setzen. So wird ID automatisch um 1 erhöht. Dieses Feld ist gleichzeitig der Primärschlüssel.

→ UserID: speichert den Benutzernamen

→ GameResult: speichert die prozentuellen Ergebnisse des Spiels

- AnswerWords: speichert die Anzahl der im Anagrammspiel abgefragten Wörter
- AskedWords: speichert die Anzahl der im Anagrammspiel beantworteten Wörter
- GameDate: speichert das Spieldatum
- GameFun: speichert den Spaßfaktor des Benutzers beim Spielen
- GameSkill: speichert die Angabe des Benutzers zu dessen Gefühlszustand beim Spielen
- Comment: speichert die im Reisetagebuch eingetragenen Notizen des Benutzers

Die Tabelle *user* hat 3 Felder, welche weitere wichtige Informationen speichern:

- id: genau wie bei der Tabelle *book* speichert dieses Feld die ID vom Spiel. Hier sollte man ebenfalls beachten, dass die ID vom Spiel genauso automatisch um 1 erhöht wird.
- Username: genau wie die UserID bei der Tabelle *book* speichert dieses Feld den Benutzernamen
- Password: speichert das Passwort des Benutzers

7.2 JQuery

jQuery ist eine JavaScript Bibliothek, welche die Zusammenarbeit von JavaScript, HTML und CSS durch eine Reihe von nützlichen und bereits implementierten Funktionen regelt.

jQuery erlaubt Animationen, Ereignis- und Effekt-Handler zu erstellen, erleichtert die Auswahl der Elemente in dem DOM (*Document Object Model*) und die Erstellung von AJAX-Anfragen.

jQuery funktioniert in allen Browsern (IE 6.0+, FF 2.0+, Safari 3.0+, Opera 9.0+, Chrome), das bedeutet es ist vom jeweiligen Browsertyp unabhängig: Mit Hilfe von jQuery kann man in unterschiedlichen Browsern die gleiche Ausgabe bzw. sich weitgehend identisch verhaltende Ausgaben erzeugen.

Die Basisbibliotheken von jQuery beinhalten die folgenden Funktionen:

- DOM-Manipulation und -Navigation
- Erweitertes Event-System
- Hilfsfunktionen
- Effekte und Animationen
- AJAX-Funktionalitäten + API für die Arbeit mit der AJAX

Ich habe folgende jQuery-Bibliotheken benutzt:

- jquery -1.7.1. min.js (Standardbibliothek von jQuery)

- jquery.form.js (jQuery-Plugin, welche es erlaubt neue Ajax-Form zu erstellen oder bereits bestehende Formen zu verbessern)
- jquery.js (Diese Datei unterstützt Web-Entwicklung und Scripting)
- jquery.min.js (eine kleinere Version von jquery.js)
- jquery.masonry.min.js (dieses jQuery-Plugin ermöglicht schnell und einfach das dynamische Layout von Blöcken unterschiedlicher Größe praktisch ohne Platzverlust zu organisieren.)
- jquery-ui-1.8.17.custom.min.js (dieses jQuery-Plugin bietet eine Reihe von UI-Schnittstellen, Effekte, Widgets und Themen. Es erlaubt die Erstellung hoch-interaktiver Webanwendungen, Formular- und Steuerelementen etc.)

jQuery AJAX ist besonders wichtig bei der Arbeit mit dem Server. AJAX realisiert die Möglichkeit der Ausführung einer Abfrage an den Server, ohne die Seite neu zu laden. Die grundlegenden Funktionen für die Arbeit der AJAX sind die `post()` und `get()`.

Um sich richtig mit der Datenbank *cryptodatabase* zu verbinden, werden folgende Informationen an `ajax.php` übergeben:

- Host-ID: *127.0.0.1*
- Datenbankname: *cryptodatabase*
- Root: *cryptodatabase*
- Passwort der Datenbank: *cryptofant*

Kapitel 8

Fazit

Meine Bachelorarbeit war ein großes und herausforderndes Projekt, Ziel des Projektes war die Erstellung eines auf HTML 5-basierenden elektronischen Lerntagebuches (Reisetagebuches) zur Unterstützung und Motivation von Anfänger bei der Benutzung des Softwareprogramms CrypTool 2. Mit Hilfe des Cryptoplaneten, Anagrammspiels und der Aufgaben habe ich für Motivation bei Benutzern gesorgt. Ergebnisse vom Anagrammspiel werden automatisch in das Reisetagebuch eingetragen. Das Reisetagebuch lässt ebenfalls Benutzereinträge zu, reagiert auf diese und regt gezielt Reflexionsprozesse an. Insofern habe ich das Ziel meiner Arbeit erreicht.

Es gibt viele Erweiterungsmöglichkeiten für die bereits bestehende LearnCrypTo-Homepage und das Tagebuch: es können weitere Spiele und Aufgaben aus dem Bereich der Kryptografie erstellt und hinzugefügt werden. Der Schwerpunkt der Aufgaben und Spiele sollte bei den automatischen Einträgen im Reisetagebuch liegen. Ebenso könnte man bereits dem Benutzer per Link zugänglichen Chiffren zum Ausprobieren auf der CrypTool-Online Seite (CTO) und die Aufgaben auf der MysteryTwister C3 Seite (MTC3) mit dem Tagebuch verknüpfen.

Der Cryptoplanet könnte erweitert werden – beispielsweise um spezielle Geschichten/Abenteuer, welche den Benutzer durch einzelne Inseln oder Inselgruppen führen. Eine Lerngeschichte könnte den Benutzer zusätzlich motivieren und sich im Inhalt an den Kulturen und geschichtlichen Ereignissen im Bereich Kryptografie orientieren.

Man kann die LearnCrypTo-Homepage um ein Blog erweitern, welches Austausch zwischen Benutzern ermöglichen wird.

Auch so kann die LearnCrypTo-Homepage um Hilfs- und Suchfunktionen erweitert werden, was die Seite noch motivierender und benutzerfreundlicher machen würde.

Zuletzt könnte der auf der LearnCrypTo-Homepage omnipräsente CrypToPhant als Grundlage für ein ECA (Embodied Conversational Agent) dienen.

Allein die soeben aufgeführten Möglichkeiten zur Weiterentwicklung des Tagebuches und der Homepage machen deutlich, wie viel Potential weiterhin im Thema meiner Bachelorarbeit steckt.

Kapitel 9

9.1 Literatur:

Abt, Clarc, C.(1975). Serious Games, New Yourk, Viking Compass.

Aldrich, C., (2009). Virtual worlds, simulations, and games for education: A unifying view. Innovate: Journal of Online education. Volume 5, Issue 5

Baumgartner, Peter (1997). Didaktische Anforderungen an (multimediale) Lernsoftware. In: Ludwig J. Issing, Paul Klimsa (Hrsg.): Information und Lernen mit Multimedia. 2. Auflage. Psychologie Verlags Union, Weinheim 1997, ISBN 3-621-27374-3

Bloom, Benjamin (1956). Taxonomy of educational objectives. New York: McKay.

Breuer, J., Bente, G. (2010). Why so serious? On the Relation of Serious Games and Learning: <http://www.eludamos.org/index.php/eludamos/article/viewArticle/vol4no1-2/146> (letzter Zugriff: 14.01.2014)

Gregory, Jason, Lander, Jeff und Whiting, Matt (2009). Game Engine Architecture. Erste Auflage. Taylor & Francis Ltd., ISBN 978-1568814131.

Holzinger, Andreas (2000). Basiswissen Multimedia. Band 2: Lernen. Würzburg, S. 110 f.

Michael, David, & Chen, Sante (2006). Serious Games: Games that Educate, Train, and Inform. Boston, MA: Thomson. ISBN: 1-59200-622-1

Prensky, Marc (2007) Digital game-based learning. St. Paul, MN: Paragon House.

Salen, Katie, Zimmerman, Eric (2004). Rules of Play: Game Design Fundamentals. MIT Press. ISBN: 0-262-24045-9

Schanda, Franz (1995). Computer-Lernprogramme. Wie damit gelernt wird. Wie sie entwickelt werden. Was sie im Unternehmen leisten. Beltz, Weinheim; Basel, ISBN: 3-407-36317-6

Schanda, F., Martens J. U. und Seng G., (1990). unveröffentlichtes Papier: Strategien interaktiven Lernens zur Realisierung kognitiver, affektiver und psychomotorischer Lernziele. [Katalog befindet sich im Anhang]

Sign, Simon (2012). Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Deutscher Taschenbuch Verlag, München, 11. Auflage, ISBN 978-3-42333071-8

Spitzer, Manfred (2007). Lernen. Gehirnforschung und die Schule des Lebens. Berlin, Heidelberg, S.160

Zyda, Michael (2005). From Visual Simulation to Virtual Reality to Games. Volume 38, Issue 9, IEEEComputer Society.

9.2 Internet-Quellen:

Weblogs: Ideal für selbstorganisiertes Lernen:

<http://sciencev1.orf.at/science/news/76747> (letzter Zugriff 15.01.14)

Depressing news for diarists:

<http://www.newscientist.com/article/mg18324642.300-depressing-news-for-diarists.html> (letzter Zugriff 16.01.14)

Serious Games:

<http://www.seriousgames.org/> (letzter Zugriff 23.01.14)

16Millionen Nutzerkonten geknackt:

<http://www.spiegel.de/netzwelt/web/bsi-warnt-vor-identitaetsdiebstahl-16-millionen-nutzerkonten-betroffen-a-944643.html> (letzter Zugriff 23.01.14)

Serious Games. Edutech Wiki:

http://edutechwiki.unige.ch/en/Serious_game (letzter Zugriff: 24.05.2014)

SECOM. Serious Games

<http://nordsee.lfi.rwth-aachen.de/secom/spielbasiertes-lernen/serious-games?lang=de> (letzter Zugriff: 02.05.2014)

Why so serious? On the Relation of Serious Games and Learning:

<http://www.eludamos.org/index.php/eludamos/article/viewArticle/vol4no1-2/146> (letzter Zugriff: 24.05.2014)

E-Learning:

<http://de.wikipedia.org/wiki/E-Learning> (letzter Zugriff: 23.01.2014)

Depressing news for diarists:

<http://www.newscientist.com/article/mg18324642.300-depressing-news-for-diarists.html> (letzter Zugriff: 16.01.2014)

Die Bedeutung des Vorverständnisses der Schüler für den Unterricht:

http://epub.uni-regensburg.de/7005/1/ubr04036_ocr.pdf (letzter Zugriff: 03.06.2014)

Lernsoftware:

<http://de.wikipedia.org/wiki/Lernsoftware> (letzter Zugriff: 03.06.2014)

Lernzieltaxonomisierung in der psychomotorischen Dimension:
<http://paedpsych.jk.uni-linz.ac.at/internet/arbeitsblaetterord/LERNZIELORD/m2.html>
(letzter Zugriff: 03.06.2014)

MySQL
<http://de.wikipedia.org/wiki/MySQL> (letzter Zugriff: 03.06.2014)

MyISAM vs. InnoDB
<http://web-union.de/382> (letzter Zugriff: 03.06.2014)

9.3 Abbildungsverzeichnis:

| | |
|---|----|
| Abb. 1: Media-based Learning | 9 |
| Abb. 2: Beziehungen von medialen Lerntechniken | 11 |
| Abb. 3: Wahl der Lernstofftiefe | 20 |
| Abb. 4: CrypTool 2 Wizard | 28 |
| Abb. 5: Tasten | 29 |
| Abb. 6: Binärbaum der Aufgaben/der Verfahren | 29 |
| Abb. 7: Substitution Chiffre zum Ausprobieren | 29 |
| Abb. 8: Vigenère Chiffre: Klar- und Geheimtext | 30 |
| Abb. 9: Übergang vom Wizard zu dem CWM | 30 |
| Abb. 10: Klartext-Block bei der Solitaire Chiffre | 31 |
| Abb. 11: Menüs im Überblick | 32 |
| Abb. 12: Kontextmenü | 33 |
| Abb. 13: Verschiebung und Vergrößerung | 33 |
| Abb. 14: Maximierung eines Blocks | 34 |
| Abb. 15: Maximierung auf Vollbild | 34 |
| Abb. 16: Minimierung eines Blocks | 34 |
| Abb. 17: Verbindung der Blöcke | 35 |
| Abb. 18: Verbindungsmöglichkeiten von Scytale | 35 |
| Abb. 19: Visualisierung von Caesar Chiffre | 36 |
| Abb. 20: Transpositionsanalyse-Diagramm | 36 |
| Abb. 21: Datentyp- und Funktionen-Farben | 37 |
| Abb. 22: Komponentenleiste von CWM | 38 |
| Abb. 23: Textblock | 38 |
| Abb. 24: Navigation der LearnCrypTo-Seite | 39 |
| Abb. 25: obere Menüleiste | 39 |
| Abb. 26: untere Menüleiste | 39 |
| Abb. 27: Zeitstrahl | 40 |
| Abb. 28: Verlinkung | 41 |
| Abb. 29: Cryptoplanet | 42 |
| Abb. 30: Insel „klassische Verfahren“ | 42 |
| Abb. 31: rechte Seite des Reisetagebuchs | 44 |
| Abb. 32: Anmeldung | 45 |
| Abb. 33: Registrierung | 46 |
| Abb. 34: Reisetagebuch | 47 |
| Abb. 35: Koffer, gefüllt mit einem Begriff | 48 |
| Abb. 36: leerer Koffer | 49 |
| Abb. 37: CrypTool 2 Portal | 49 |
| Abb. 38: Datenbank <i>cryptodatabase</i> | 57 |

Kapitel 10

Anhang:

10.1 „Strategien interaktiven Lernens zur Realisierung kognitiver, affektiver und psychomotorischer Lernziele“

(Unveröffentlichte Papier (1990) von F. Schanda, J. U. Martens und G. Seng).

Auswendiglernen

Grundlagen

Tauchen zwei getrennte Ereignisse oder Vorstellungen häufig gemeinsam oder in kurzen Abständen in unserem Bewußtsein auf, so besteht eine große Wahrscheinlichkeit, daß wir uns an die fehlende Vorstellung erinnern (daß wir sie assoziieren), wenn nur eine Vorstellung auftaucht. Wenn es z.B. blitzt, so erinnert uns das sofort an den Donner: Man spricht von Assoziation.

Beim Auswendiglernen bilden wir solche Assoziationen. Auf diese Weise lernen wir z.B. Sprachen, Telefonnummern, Gedichte usw.

Aus der großen Reihe von Experimenten, die mit dieser Lerntechnik gemacht wurden, lassen sich einige Forderungen für das Auswendiglernen ableiten:

- Die Verbindung der Vorstellungen muß häufig wiederholt werden.
- Die fehlende Vorstellung muß von den Lernenden aktiv produziert werden.
- Die Lernenden müssen unmittelbar nach der Produktion Meldung erhalten, ob sie richtig oder falsch »assoziert« haben.
- Die einzelnen Vorstellungen, aus denen die Assoziationen bestehen, sollten dem Lernenden bereits vertraut sein.

Die Gedächtnisleistung kann durch (bewußtes) Bilden von Assoziationen beträchtlich gesteigert werden. Meist ist uns der Vorgang nicht bewußt. Jeder von uns kennt aber die

Bedeutung der sogenannten »Eiselsbrücken«, die nichts anderes darstellen als bewußte Assoziationsketten.

Auswendiglernen mit Computer-Lernprogrammen

Beim Lernen mit dem Computer lassen sich alle aufgezählten Forderungen realisieren:

- Wiederholung.
- Sofortige Lösung bei Antwort.
- Berücksichtigung des Vorwissens durch Vortests.
- Unterschiedliche Schwierigkeitsgrade etc.

Das Auswendiglernen ist eine Domäne des interaktiven Lernens: denn über diese Forderungen hinaus (die ja prinzipiell auch mit konventionellen Medien zu erfüllen sind) bieten Computer-Lernprogramme hier Komfort und Effizienz, die auf andere Weise nicht realisierbar sind.

Beispiele:

- Automatisch bzw. individuell (z.B. aufgrund von Empfehlungen nach einem Test) veranlaßte Verzweigungen bzw. Zusammenstellung individueller Lernwege.
- Adaptive Steuerung des Schwierigkeitsgrads von Aufgaben/Tests.
- Differenziertes, individuelles Feedback ist möglich.

Einsichtiges/verstehendes Lernen

Grundlagen

Die Gestaltpsychologie hat gezeigt, daß es nicht sinnvoll ist, alle Phänomene des Lernens durch Assoziationsbildung zu erklären. Insbesondere Prozesse der Einsicht und des Verstehens von Zusammenhängen lassen sich besser mit anderen Theorien erklären.

Der Vorgang der Einsicht spielt sich – vereinfacht dargestellt – nach Ansicht der Gestaltpsychologen ähnlich ab wie der Vorgang der Wahrnehmung. Wir sehen nicht einzelne Elemente, deren Ordnung lediglich von außen vorgegeben ist, sondern wir sehen Bedeutungsgehalte. Wir ergänzen die Wahrnehmung entsprechend unserer Erfahrung oder ordnen die einzelnen Elemente der Wahrnehmung sogar um, um ihnen einen Sinn zu geben. Wie bei der Wahrnehmung, so bilden sich auch im Bereich des Denkens Bilder oder Strukturen, wenn uns ein Zusammenhang verständlich wird.

Das produktive Lösen von Problemen wird von der Gestaltpsychologie so interpretiert, als ob unvollkommen gezeigte Gestalten zu vollkommenen, geschlossenen Figuren umgewandelt würden. Eine solche Umwandlung in geschlossene Figuren, das heißt die produktive Lösung von Problemen, ist folgerichtig nur dann möglich, wenn die unvollkom-

mene Gestalt bzw. das Problem eine klar erkennbare Struktur besitzt. (Diese Erkenntnis ist vor allem für die Formulierung von Aufgaben innerhalb von Lernprogrammen wichtig.)

Mit dieser gestaltpsychologischen Theorie läßt sich vor allem das Lernen von komplizierten Beziehungen und Zusammenhängen, das Lernen von Problemlösungen und Regeln (wenn sie nicht stur auswendig gelernt werden) erklären. Auch für diesen Typ des Lernens lassen sich aus den vielfältigen Experimenten einige Forderungen für den Lernprozeß ableiten.

- Der Zusammenhang muß klar und übersichtlich (strukturiert) und möglichst auf einen Blick erfassbar dargestellt sein.
- Der Lernende sollte die Möglichkeit haben, fehlende Elemente aus der Struktur selbst zu entdecken, das heißt, Aufgaben produktiv zu lösen (»Aha-Erlebnis«).
- Die einzelnen Elemente, aus denen die dargestellten Beziehungen bestehen, müssen bekannt sein.

Einsichtiges/verstehendes Lernen mit Computer-Lernprogrammen

Computer-Lernprogramme sind für diese Art des Lernens besonders gut geeignet. Der schrittweise Aufbau von Strukturen läßt sich im interaktiven Lernprozeß gut darstellen, sowohl im (bewegten) Bild als auch im Text:

- Über Eingangstests kann man das Vorwissen der Lernenden ermitteln und ihnen Lernwege empfehlen, die ihrem Niveau entsprechen.
- Die Darstellung kognitiver Informationen, z.B. eine Argumentationskette, kann sehr gut (lern-)schrittweise entwickelt werden.
- Zum besseren Verständnis können Grafiken integriert werden.
- Durch zielgerechte Fragen kann überprüft werden, ob die Lernenden die Argumentation nachvollzogen haben.
- Fehlinterpretationen der Lernenden können über Feedbacks analysiert und kommentiert werden.
- Es besteht die Möglichkeit, den Lernenden z.B. nach falschen Antworten Verzweigungen anzubieten, in denen ihnen die Argumentation auf leichter verständliche oder ausführlichere Art angeboten wird.
- In guten Programmen steht den Lernenden z.B. ein Lexikon mit Erklärungen relevanter Fachbegriffe zur Verfügung.
- Gute Programme bieten den Lernenden Möglichkeiten zur individuellen Gestaltung ihrer Lernwege an (und damit zur Entwicklung individueller kognitiver Strukturen).
- Bei schwierigeren Aufgaben können den Lernenden Hilfen und Tips angeboten werden, auf die sie bei Bedarf zugreifen können.

Einstellungslernen

Grundlagen

Jeder von uns hat die gefühlsmäßige Tendenz, auf wichtige Dinge seiner Umgebung relativ gleichförmig zu reagieren bzw. sie unter einem bestimmten Blickwinkel zu sehen. Diese Tendenz geht auf Einstellungen zurück.

Einstellungen sind wesentlich durch die eigene Erfahrung oder durch die Nachahmung von Vorbildern geprägt.

Ein Verkäufer z.B. »sieht« den Kunden »mit anderen Augen« als ein Mitarbeiter des Kundendienstes. Für den Verkäufer ist der Kunde derjenige, der »Geld hat« und ihm seinen Umsatz bringt. Der Kundendienst sieht ihn möglicherweise als »notorischen Nörgler«, der sich ständig über die Produktqualität und die Reparaturkosten beklagt.

Solche Einstellungen beeinflussen unser tägliches Verhalten mehr als das bloße Wissen: Unser Verhalten gegenüber Mitarbeitern, Vorgesetzten, Kunden, unsere Haltung gegenüber der eigenen Firma und vieles mehr beruht wesentlich auf Einstellungen, die gelernt wurden.

Will man Einstellungen durch Lernprozesse erfolgreich verändern – was im allgemeinen relativ schwer ist –, so sind an die Lerntechnik folgende Forderungen zu richten:

- Die Lernenden müssen die neuen Einstellungen aufgrund eigener Entdeckung oder Erfahrungen bilden können (entdeckendes Lernen). Ein Belehren ist zwecklos.
- Die Lernenden müssen bei der Darstellung der Inhalte emotional beteiligt sein. Die Gefühlsebene muß angesprochen werden.
- Viele Einstellungen übernehmen wir von Vorbildern. Wir versuchen diesen Vorbildern ähnlich zu sein und erreichen dieses auch dadurch, daß wir deren Einstellungen übernehmen.
- Wird die neu erworbene Einstellung vor einer Gruppe (öffentlich) vertreten, so wird sie erheblich gefestigt.
- Das Verhalten, das auf den neuen Einstellungen beruht, muß belohnt werden.
- Die Beeinflussung sollte in größeren Abständen wiederholt werden.

Einstellungslernen mit Computer-Lernprogrammen

Beim Lernen mit dem Computer lassen sich eine ganze Reihe von Bedingungen erfüllen, die für das Einstellungslernen förderlich sind.

Im Bereich des Lernens durch Erfahrung/Entdecken kann mit interaktiven Medien viel erreicht werden. Gerade Computer-Lernprogramme bieten viele Möglichkeiten, den Stoff lernerzentriert zu vermitteln, den Lernenden selbst die Lernsteuerung zu überlassen, sie dazu zu bewegen, selbst Fragen an das Programm zu stellen, statt schematisch den Lernstoff in kleinen Häppchen zu vermitteln, um ihn anschließend ebenso stereo-

typ wieder abzufragen. Durch intelligentes Kursdesign kann man den Lernenden die Auswirkungen ihrer Entscheidungen zeigen (z.B. die Auswirkung von Programmierfehlern bei Werkzeugmaschinen). Differenzierte Feedbacks können die Lernenden persönlich ansprechen und ihnen helfen, den für sie optimalen Lernweg selbst zu finden.

Besonderheiten:

Einstellungslernen wird durch die Gruppe oder durch einzelne Personen sehr gefördert; diese Möglichkeit ist beim interaktiven Lernen nicht gegeben. Es muß daher im Einzelfall geprüft werden, ob die Gruppe zum Erreichen des speziellen Lernziels *erforderlich* ist. Wenn ja, dann scheidet das Lernen mit Computer-Lernprogrammen aus; zumindest als Lernen am Einzel-Lernplatz.

Gesondert zu prüfen ist, ob Computer-Lernprogramme in anderen Organisationsformen lernzielgerecht eingesetzt werden können, so z.B. im Rahmen von Partnerarbeit am Computer, selbststeuernden Kleingruppen oder in trainergesteuerten Veranstaltungen.

In der Hand eines phantasievollen, kreativen Autors sind die Möglichkeiten von Computer-Lernprogrammen auch im Bereich der emotionalen Ansprache beachtlich. Adressatengerechte, lernzielorientierte und motivierende Rahmenhandlungen und Identifikationsfiguren können schon durch reine Computer-Lernprogramme ohne Bewegtbild realisiert werden.

Ist eine intensive, emotionale Anteilnahme der Lernenden erforderlich, so wird es selten eine Alternative zu Filmsequenzen geben. Die Entscheidung, ob man das Computerprogramm mit Filmsequenzen kombiniert, muß daher didaktisch begründet sein.

Soziales Lernen

Grundlagen

Sich in Gruppen einzuordnen, bestimmte Rollen zu übernehmen, die Normen und typischen Verhaltensweisen der Gruppe zu den eigenen zu machen, dies alles sind Vorgänge, die auf soziales Lernen zurückgehen. Die in der Regel recht starren Normen einer Gesellschaft kann man als Einstellungen bezeichnen. Daher hat der Bereich des sozialen Lernens auch viel mit Einstellungslernen zu tun.

Das Verhalten des einzelnen in einer Gruppe ist aber nicht nur durch solche Normen zu erklären. Wir entwickeln ebenso Anpassungsstrategien und Reaktionsmuster, die ein angepaßtes Verhalten verschiedenen Gruppen oder verschiedenen Menschen gegenüber möglich machen. Man spricht von der Übernahme verschiedener Rollen. Wir verhalten uns z.B. im Büro gegenüber dem Chef anders als gegenüber den Kollegen, im Kegelclub anders als in der Familie, auf einem Cocktailempfang anders als im Bierzelt usw.

Auch für das soziale Lernen kann man bestimmte Regeln aufstellen, die dieses Lernen fördern:

- Die Lernenden müssen Gelegenheit haben, die gewünschten Verhaltensweisen in sozialen Situationen zu erproben (aktives Lernen in sozialen Situationen).
- Die Lernenden sollten häufig in Situationen gestellt werden, in denen das gewünschte Verhalten belohnt wird (durch soziale Verstärker).
- Den Lernenden muß das gewünschte Verhalten häufig gezeigt werden (real oder durch Medien dargestellt), damit es nachgeahmt werden kann. Die Lernenden sollten sich dabei mit der Person, die das gewünschte Verhalten zeigt, identifizieren können (»Lernen am Modell«).

Soziales Lernen mit Computer-Lernprogrammen

Die wichtigste Bedingung für soziales Lernen ist, daß die gewünschten Verhaltensweisen in sozialen Situationen geübt werden können. Man muß daher feststellen, daß soziales Lernen in seiner ganzen Komplexität durch Lernen am Computer nicht geleistet werden kann.

Aber: Das Sozialverhalten wird fast immer von Einstellungen ebenso wie von kognitiven Prozessen mitgeprägt. Eine Änderung des Sozialverhaltens wird daher oft nur dann gelingen, wenn Lernziele in allen drei genannten Bereichen erreicht sind. Hier können Computer-Lernprogramme wiederum eine wichtige Funktion übernehmen (siehe in den entsprechenden Abschnitten).

Darüber hinaus ist bekannt, daß soziales Lernen durch nachahmendes Lernen *vorbereitet* werden kann (Modellernen, Identifikation). In dieser Hinsicht bieten Computer-Lernprogramme durch die Lernaktivierung bessere Möglichkeiten als etwa der Film alleine.

In ein Aus- und Fortbildungskonzept, das auf eine Änderung des Sozialverhaltens ausgerichtet ist, können Computer-Lernprogramme als Bausteine sinnvoll integriert werden.

Lernen von Bewegungsabläufen

Grundlagen

Wenn man Skifahren, Tennis- oder Golfspielen lernt, aber auch wenn man lernt, ein Auto zu fahren, eine Schreibmaschine zu bedienen oder einen Airbus zu fliegen, spricht man gleichermaßen vom »Lernen«. Doch sind damit Prozesse gemeint, die sich wesentlich von den anderen Arten des Lernens unterscheiden. Wir sprechen von psychomotorischen Lernzielen oder von Lernen von Muskelbewegungen.

Auch für solche Lernziele lassen sich Forderungen ableiten:

- Das Lernen von Bewegungsabläufen, das Koordinieren einzelner Muskeln muß häufig geübt werden. Die Wiederholung spielt bei dieser Art des Lernens eine ganz besondere Rolle.
- Die Lernenden müssen bei dieser Art des Lernens laufend aktiv sein. Bis zu einem gewissen Grad ist es zwar möglich, durch mentales Training einen Übungseffekt zu verbessern, das eigentliche Lernen kann jedoch nur durch die Aktivität selbst erreicht werden. (Unter mentalem Training versteht man die geistige Vorstellung der gewünschten Bewegung.)
- Die Rückmeldung darüber, ob eine Muskelbewegung richtig oder falsch war, muß unmittelbar nach der Bewegung erfolgen. (Eine zeitliche Verzögerung von mehreren Sekunden beeinträchtigt den Lernerfolg bereits erheblich.)
- Lernen von psychomotorischen Fertigkeiten kann nur an dem Objekt und in der Situation erfolgen, an dem und in der die Fähigkeit nach dem Lernprozeß ausgeübt wird.

Lernen von Bewegungsabläufen mit Computer-Lernprogrammen

Häufig ist das Lernen am konkreten Lernobjekt schwer möglich, da ein Fehler fatale Folgen haben könnte oder das Üben sehr teuer wäre (Beispiel: Fliegen eines Jumbos, Bedienung hochempfindlicher, teurer elektronischer Geräte, Bedienung eines Atomkraftwerks).

Man baut daher Geräte (Simulatoren), die dem eigentlichen Lernobjekt sehr ähnlich sind und die es erlauben, den Lernenden Rückmeldung über die richtige oder falsche Bedienung zu geben, ohne daß sie sich oder das Gerät dabei in Gefahr bringen.

Bei der möglichst exakten Simulation ist meist eine große Zahl von Faktoren zu berücksichtigen (Beispiel: die Kurvenlage in einem Flugsimulator). Dies macht die Entwicklung solcher Geräte oft sehr aufwendig.

Häufiger sind Simulatoren, bei denen nur wenige Umweltbedingungen berücksichtigt werden (man findet solche Geräte oft im Unterhaltungsbereich als »Formel-1-Rennen«, »Tontaubenschießen«, »Golfspielen« etc.).

Es ist jedoch anzumerken, daß es sich beim Lernen mit Hilfe von Simulation überwiegend um die Beherrschung der kognitiven Komponente einer psychomotorischen Aufgabe handelt.

10.2 Anhänge auf DVD

→ Scriptcode für die LearnCrypTo-Homepage

→ Unveröffentlichte Papier (1990) von F. Schanda, J. U. Martens und G. Seng „Strategien interaktiven Lernens zur Realisierung kognitiver, affektiver und psychomotorischer Lernziele“.

→ C. Aldrich „*LEARNING BY DOING. A Comprehensive Guide to Simulations, Computer Games, and Pedagogy in e-Learning and Other Educational Experiences*“

→ D. Michael & S. Chen “Serious Games: Games that Educate, Train, and Inform.”

→ K. Schmeh “Kryptografie. Verfahren, Protokolle, Infrastrukturen“.