Arbeitsjournal

Niklaus Hofer, Roland Rytz

21. Dezember 2012

1 Dokumenteninformationen

1.1 Änderungskontrolle

1.2 Referenzierte Dokumente

1.3 Verwendete Abkürzungen

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

2 Managementsummary

2.1 Aufgabenstellung

Unser Programm soll den Vigenere-Algorithmus visuell erklären. Ein Wikipedia-Artikel soll die nötigen Hintergrundinformationen zu dem Thema bereit halten. In Englischer Sprache gibt es bereits seit Längerem einen Artikel zu dem Tema, nicht so in der deutschen Wikipedia.

2.2 Varianten

Gerade in der Webentwicklung gibt es sehr viele unterschiedliche Tools und Ansätze. Es ist wichtig, dass man sich von Beginn weg für den am besten geeigneten Prozess und gute Werkzeuge entscheidet. In diesem Abschnitt werden die Möglichkeiten aufgezeigt und der Entscheid begründet.

2.3 Konzept

Hier finden die Planung der Produkte statt. Der Aufbau der Applikation wird geplant und aufgezeigt. Die Struktur des Wikipedia-Artikels wird geplant. Hier werden sich auch erste Ablauf-Diagramme und Vorlagen finden.

2.4 Realisierung

Im Verlauf der Arbeiten an den Produkten treten Unterschiede zu der Planung auf die sich zumeist aus unvorhergesehenen Komplikationen oder Vereinfachungen ergeben. Alle Unterschiede zur Planung werden hier erläutert und begründet.

2.5 Mittelbedarf

Hier werden die nötigen Ressourcen aufgelistet.

2.6 Fazit

Teil I
Ablauf und Umfeld

3 Projektmethode Hermes

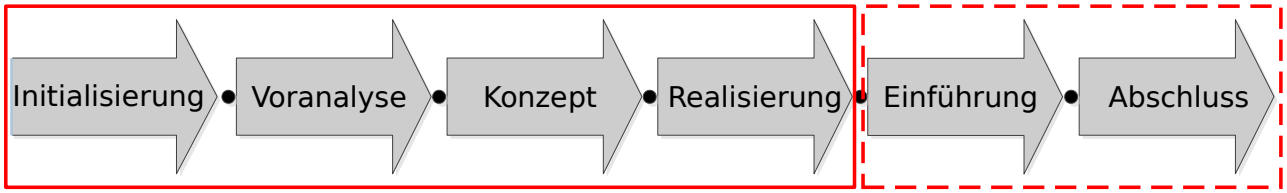

Abbildung 1: Hermes Light Schema

Wir haben die Projektmethode Hermes Light gewählt. Hermes Light ist eine vereinfachte und verkürzte Variante von Hermes. In der Grafik **??** sind die sechs Phasen der Projektmethode aufgezeigt. Die letzten zwei Phasen, „Einführung“und „Abschluss“werden im Rahmen dieser IPA nur teilweise durchgeführt. Die Einführung besteht im Bereitstellen der Webseite und des Artikels. Der Abschluss allerdings wird hier nur beschrieben.

In den Abschnitten unten, werden wird die jeweilige Phase kurz erläutern und aufzeigen welche Teile dieses Dokumentes zu welcher Phase gehören.

3.1 Initialisierung

- Festlegung eines klar definierten organisatorischen und technischen Rahmens als Voraussetzung für eine erfolgreiche Projektabwicklung
- Planung, Vernehmlassung und Beurteilung des Projekts
- Freigabe der Phase Voranalyse

Diese Phase beinhaltet folgende Punkte dieser Dokumentation:

-

3.2 Voranalyse

- Erstellung und Beurteilung der Situationsanalyse sowie Überprüfung der Zielsetzungen, der Problemstellung und des Untersuchungsbereichs
- Erarbeitung von Lösungsvorschlägen und Abschätzung ihrer voraussichtlichen Wirtschaftlichkeit und Realisierbarkeit
- Auswahl eines Lösungsvorschlages und Freigabe der Phase Konzept.

Diese Phase beinhaltet folgende Punkte dieser Dokumentation:

-

Eigentlich beinhaltet diese Phase noch die Punkte „Termine“und „Zeitplan“. Aufgrund des Ablaufs der IPA und da diese Daten gegeben sind, habe ich oben genannte Punkte aber in die Phase Initialisierung verschoben.

3.3 Konzept

- Vollständige Darstellung des Systems, ausgehend vom gewählten Lösungsvorschlag
- Beurteilung kritischer Teilsysteme
- Freigabe der Phase „Realisierung“

Diese Phase beinhaltet folgende Punkte dieser Dokumentation:

-

Die Konzeptphase widmet sich der konkreten Gestaltung des Systems. Es beinhaltet die Struktur, die Architektur, das Design, sowie die Funktionalitäten der zu entwickelnden Applikation.

3.4 Realisierung

- Erkläuterungen zum geschriebenen Code
- Aufzeigen und Begründen von Änderungen gegenüber dem Konzept
- Freigabe der Phase Einführung

Diese Phase beinhaltet folgende Punkte dieser Dokumentation:

-

3.5 Einführung

3.6 Abschluss

4 Aufgabenstellung

4.1 Ausgangslage

Der Vigenere-Algorithmus ist bereits mehrere Hundert Jahre alt. Er ist einerseits intuitiv und auch für Laien leicht verständlich. Trotzdem lassen sich daran einige wichtige Punkte von kryptografischen Systemen aufzeigen. Trotz der schnell verständlichen Stärken des Algorithmus lässt er sich heute mit sehr wenig Aufwand knacken.

Die meisten Webseiten die Vigenere grafisch erklären tun die mit Hilfe eines Java-Applets. Im Zeitalter von HTML5 ist der Einsatz von Java-Applets auf Webseiten aber fragwürdig und stark umstritten. Wir möchten diese veralteten Versionen der grafischen Darstellung des klassischen Algorithmus durch eine zeitgerechte Web-Applikation in HTML/CSS/JS ersetzen.

Auf der Englisch-sprachigen Wikipedia findet sich ein separater Artikel zu Vigenere's Algorithmus. In der Deutschen Wikipedia hingegen ist lediglich ein Artikel zu finden, der das Gebiet in einem breiteren Spektrum abdeckt und zu Vigenere nur wenige Informationen bietet. Dies möchten wir mit einem Eintrag speziell zu diesem Tema ändern.

Projektmethode	Hermes Light, Eine auf den Projektumfang zugeschnittene Variante von Hermes
Systeme	Computer zum Schreiben des Codes. Internetanschluss
Testing environment	System das in der Lage ist, virtuelle Mascheinen auszuführen zum Testen mit verschiedenen Browsern unter verschiedenen Systemen
Entwicklungssoftware	Editor, Browser, Javascript, JQuery
Dokumentation	Texteditor, pdflatex, MikTex
Entwicklungssprache	Javascript
Versionsverwaltung	git, github

Tabelle 1: Auflistung der Mittel und Methoden

Funktion	**Person**	**Beschreibung**
Auftraggeber	Herr Tschopp	Lehrkraft
Projektleiter	Niklaus Hofer	
Fachberater Mathematik	Herr Lüthi	Lehrkfraft
Fachberater Deutsch	Herr Tschopp	Lehrkraft
Entwickler	Roland Rytz	
Entwickler	Niklaus Hofer	

4.2 Auftragsformulierung

4.2.1 Detaillierte Aufgabenstellung

4.3 Mittel und Methoden

4.4 Projektorganisation

4.5 Projektrollen

5 Vorkenntnisse

Roland Rytz ist erfahrener Javascript Entwickler. Im Verlauf seiner Berufslehre als Informatiker EFZ hat er zahlreiche Webseiten und Webapplikatione mit Javascript realisiert. Roland hat dann auch in diesem Bereich seine Abschlussarbeit geschrieben Auch in der Freizeit hat Roland bereits einige Webseiten geschrieben. JQuery, die Webentwicklungswerkzeuge von Googles Chrome Browser und Firefox FireBug sind vertraute Werkzeuge. Auch das Testen mit verschiedenen Browsern ist keine Neuheit.

Niklaus Hofer hat bereits einfache Vigenere Implementationen in C++, Python und Java geschrieben und sich kurz theoretisch mit dem Thema auseinandergesetzt.

Die beiden Autoren sind theoretisch mit dem Erstellen von Wikipedia-Artikeln vertraut, haben aber noch nie zuvor eigene Artikel verfasst.

6 Vorarbeiten

Es gibt zu dieser Arbeit keine Vorarbeiten.

7 Termine

Die wichtigsten Termine sind die Treffen mit den Lehrpersonen.

8 Arbeitsjournal

9 Arbeitsjournal

Datum im Format Jahr.Monat.Tag

Datum	**Wer**	**Tätigkeit**	**Reflexion**	**Zeit**	
				Geplant	**Effektiv**
2012.09.09	Niklaus und Roland	Initialisierung des Repositories.	Die Zusammenarbeit funktioniert bis jetzt gut.	20min	20min
Pendenzen		Planen des weiteren Vorgehens.			
2012.10.19	Niklaus und Roland	Schreiben des ersten Programmcodes. Erstellen des Vigenere square mit HTML und Javascript.	Der Wiedereinstieg in die Progammierung ist nicht ganz einfahc gefallen. Wir hatten deshalb deutlich länger als ursprünglich geplant und sind auch nicht so weit fortgeschritten wie geplant.	30min	80min
Pendenzen		Wir wollen die grundlegenden Funktionen implementieren, damit wir beim ersten Gespräch mit Herr Lüthi bereits etwas zeigen können. Insbesondere die 'sichtbaren' Funktionen sollten dann da sein. Das GUI muss dann aber natürlich noch nicht fertig sein.			
2012.10.19	Niklaus	Implementieren des Verschlüsselungsalgorithmus in Javascript. Testen der Verschlüsselung, Vergleich mit einer anderen (online verfügbaren) Vigenere Implementationen.	Am Nachmittag konnte ich nach Langem wieder einmal programmieren. Das hat mich nicht mehr losgelassen. Ich habe also die Verschlüsselung implementiert. Das ist mir überraschend schnell gelungen, insbesondere wenn man bedenkt, dass ich zuvor kaum jemals mit Javascript gearbeitet habe. Die Verschlüsselung implementiert lediglich den Algorithmus und stellt nichts grafisch dar. Sie kann aber genutzt werden um den mathematischen Aspekt des Projektes hervorzuheben. Ein Geschwindigkeitsvergleich zwischen der Methode mit dem manuellen Auslesen der Charaktere aus dem Square und der mathematischen Funktion, sollte die Vorzüge der wesentlich schnelleren, mathematischen Funktion deutlich hervorheben.	60min	120min
Pendenzen					

Datum	Wer	Tätigkeit	Reflexion	Zeit	
				Geplant	Effektiv
2012.10.22	Niklaus	Implementation des Verschlüsselungsalgorithmus.	In der Pause im Mathematikunterricht habe ich die Entschlüsselung implementiert. Das war eine schlechte Idee, ich konnte mich danach nicht mehr auf den Unterricht konzentrieren. Im weiteren Verlauf des Nachmittags ist mir eingefallen, wie ich den Code besonders schön machen kann. Da die Entschlüsselung ähnlich der Verschlüsselung ist, konnte ich viel Code übernehmen und benötigte weniger Zeit.	15min	30min
Pendenzen					
2012.10.22	Roland	Portieren des vorhandenen Codes nach JQuery. Der Code zur Generierung des Squares wird in ein Objekt übernommen, dem später verschiedene Funktionen hinzugefügt werden können.	Die Javascript Programmierung wird durch die Verwendung von JQuery erleichtert. Die objektorientierte Programmierung ist zeitgemäss und bringe ebenfalls viele Vorteile mit sich.	30min	30min
Pendenzen		Funktionen zum Highlighten der richtigen Spalten und Zeilen müssen noch geschriben werden, damit die Verschlüsselung grafisch dargestellt werden kann. Ausserdem müssen die entsprechenden Werte ausgelesen werden. Danach sollten wir bereit für eine erste Besprechung mit Herr Lüthi sein.			
2012.10.22	Roland	Implementieren des Highlightings im Square.	Im Square können einzelne Spalten und Linien gezielt markiert wreden. Ausserdem können Buchstaben aus dem Schnittpunkt ausgelesen werden.	30min	30min
Pendenzen					
2012.10.31	Roland	Verschönern der Highlight Funktion.		40min	40min
Pendenzen					
2012.11.23	Niklaus	Portieren des vorhandenen Protokolls (der Notizen) in eine richtige HERMES Struktur	Dies wird die Dokumentation deutlich übersichtlicher machen.	45min	45min
Pendenzen		HERMES ist ein komplexer Standard. Das wird noch einiges an Zeit in Anspruch nehmen.			

Datum	Wer	Tätigkeit	Reflexion	Zeit	
				Geplant	Effektiv
2012.11.23	Niklaus Hofer	Besprechung mit Herr Tschopp über den Projektstand und das geplante weitere Vorgehen.	Bis jetzt siehts nicht schlecht aus. Wir sind gut im Zeitplan. Allerdings sollten wir mit dem Erstellen des Wikipedia-Artikels beginnen. Wir haben abgemacht, dass ein Entwurf der Struktur des Artikels anfangs Dezember vorliegen sollte. Um diese Struktur zu erstellen, werden wir andere Wikipedia-Artikel zu ähnlichen Themen auf ihren Aufbau untersuche. Die Resultate werden wir festhalten und uns dann beim Erstellen des eigenen Artikels daran orientieren.	40min	20min
Pendenzen		• Beginn der Arbeiten am Wikipedia-Artikel – Erstellen des Rasters zum Untersuchen der Wikipedia-Artikel – Wikipediaartikel zu ähnlichen Themen untersuchen – Vorlage für den eigenen Artikel erstellen • neuen Termin mit Herr Lüthi vereinbaren			
2012.11.30	Niklaus und Roland	Analyse von Wikipedia-Artikeln zu ähnlichen Themen. Erstellen einer Struktur für unseren eigenen Artikel in Abhängigkeit unserer Erkentnisse. Anlegen einer bibtex-Datenbank für die Referenzen.	Das Analysieren der Artikel nimmt deutlich mehr Zeit in Anspruch als geplant. Ausserdem müssen wir aufpassen, dass wir uns an Artikeln ähnlichen Schwirigkeitsgrads orientieren. Solche zu Themen wie RSA oder AES (rejindael) sind vom Thema und folglich auch vom Aufbau her deutlich komplexer als solche zu einfacheren Algorithmen.	45min	90min
Pendenzen		Als nächstes wollen wir die Analyse der Artikel fertigstellen, damit wir in den Ferien an dem Artikel arbeiten können.			

Datum	Wer	Tätigkeit	Reflexion	Zeit	
				Geplant	Effektiv
2012.12.13	Roland	Visuelles Ausgestalten des Webtools. Grafischer Modus wurde mit dem mathematischen Modus zusammengeführt, es kann nun ausgewählt werden, welcher Modus verwendet werden soll.	Zu viel Zeit wurde mit kleinen Details beim Ausgestalten der Grafischen Finessen aufgewendet.	15min	60min
Pendenzen		Der grafische Modus hat noch einige kleinere Fehler, die noch behoben werden sollten.			
2012.12.13	Niklaus und Roland	Fertigstellen der Auswertung der untersuchten Wikipedia-Artikel. Erstellen des Skelettes. Informationen zum Schreiben von Wikipeia-Artikeln sammenl.	Die Vorlage für den Artikel sollte soweit bereit sein. Das Ganze hat aber deutlich mehr Zeit gekostet als erwartet! Wikipedia selbst bietet einige Artikel an die das Verfassen von Wikipedia-Einträgen erläutern und einige Regeln und Richtlinien enthalten. Darunter scheint aber nichts zu sein, was nicht zimlich offensichtlich ist.	30min	60min
Pendenzen		Jetzt ist das Meiste bereit für das Verfassen des Wikipdia-Eintrages. Für die mathematischen Erläuterungen müssen wir einen Termin mit Herr Lüthi vereinbaren. Der Wikipedia-Artikel kann somit in die Phase Realisierung übergehen.			

10 Schlussbericht

10.1 Vergleich Soll/Ist

10.2 Persönliches Fazit

10.2.1 Niklaus Hofer

10.2.2 Roland Rytz

Teil II
Projektdokumentation

11 Voranalyse

11.1 Situationsanalyse

11.1.1 Analyse Ist-Zustand

Keines der Ziele ist erfüllt. Der Wikipedia-Artikel zum Thema „Polyalphabetische Substitution“kommt unseren Vorstellungen am nächsten und enthält auch schon einige grundlegende Informationen. Die Ausführungen spezifisch zu Vignere sind aber deutlich weniger detailliert als das im Englischen Artikel zu dem Thema der Fall ist.

Der Umstand dass visualisierungen des Algorithmus zumeist nur als Java-Applet vorliegen behagt uns nicht. Wir sehen uns als Vertreter eines „freien“Internets, das unabhängig von (proprietären) Browser-Plugins allen zur Verfügung steht. Solche Browser-Plugins stellen ausserdem häufig ein erhebliches Sicherheitsrisiko dar.

11.1.2 Analyse Soll-Zustand

Wie in der englischsprachigen Wikipedia soll die Deutsche einen dedizierten Artikel zu Vigeneres Algorithmus erhalten.

Eine HTML5 Web-Applikation für Vigenere Algorithmus entledigt Nutzer von einer weiteren Abängigkeit zum Java-Plugin.

11.2 Varianten

Im Bereich der Webentwicklung mussten wir uns für ein spezifisches Vorgehen entscheiden. Hier gibt es viele Möglichkeiten. Dieser Abschnitt wird die Varianten beschreiben und sie, mit Fokus auf unsere Anwendung, vergleichen.

11.3 Variantenentscheid

12 Abstract

13 Einleitung

Kryptografie ist ein wichtiges Teilgebiet nicht nur der Informatik, sondern auch der Mathematik. Es bietet ein praktisches und kommerzielles Anwendungsfeld für viele mathematische Grundlagen. Dabei ist korrekte und sichere Verschlüsselung heute von sehr grosser Bedeutung. Ein Grossteil des Datenaustausches findet über das Internet statt. Wer da noch mitliest, lässt sich nicht genau sagen. Möchte man Daten bei der Übertragung deshalb geheim halten, so ist es wichtig, dass diese verschlüsselt sind.

Ausserdem ist eine gute Verschlüsselung auch eine grosse Herausforderung. Die Rechenkraft von modernen Computern, besonders von Supercomputern schnellt seit Jahrzehnten in die Höhe. Die Paralellisierung der Rechenaufgabe und der Einsatz optimierter Hardware wie GPUs und FPGAs verschärfen die Situation weiter. Unsichere Verschlüsselungen lassen sich so innert Sekunden knacken. Andererseits muss eine gute Verschlüsselung auch auf rechenschwachengeräten wie Smartphones, Router oder gar Fernsehern funktionieren und das ohne, dass die Akkulaufzeit negativ beeinflusst wird.

All das hat dazu geführt, dass moderne Verschlüsselungsalgorithmen wie ECC oder AES sehr komplexe mathematische Formeln sind. Die ganzen Zusammenhänge und den Aufbau solcher Verschlüsselungen zu verstehen ist alles andere als trivial. Wer neu in das Feld der Kryptografie einsteigt, sollte sich zuerst mit einfacheren Konzepten auseinander setzen.

Die Vigenere Verschlüsselung ist aus heutiger Sicht zwar längst veraltet und unsicher. Selbst vor dem Zeitalter von Computern war es, mit viel Aufwand, bereits möglich, solche Verschlüsselungen zu knacken. Trotzdem ist die Betrachtung sehr interessant. Die Schwäche des Algorithmus ist auf den ersten Blick nicht zu erkennen. Es lässt sich auch zeigen, wie viel einfacher Computer das Knacken schlechter Verschlüsselungen machen.

In dieser Arbeit stellen wir die Frage, wie Viegenere funktioniert und insbesondere, wie man dessen Funktionsweise einfach verstaendlich machen kann. Dazu soll eine visuelle Repräsentation der Funktion des Algorithmus erstellt werden. Wir wollen auch wisse, wieso denn der Algorithmus unsicher ist und wie man ihn knacken kann. Wie aufwändig ist das eigentlich? Da wir ohnehin eine visuelle Umsetzung des Algorithmus erstellen, die so funktioniert, wie ein Mensch sich das einfahc vorstellen kann, wollen wir die Performance dieses Vorgehens vergleichen, mit einer Implementation desselben Verfahrens mit mathematischen Formeln. Zuletzt stellt sich uns noch die Frage, wie einfach sich die Visualisation mit modernen Webtools umsetzen lässt.

14 Praxisarbeit

Zur Praxisarbeit zählt eine Webapplikation, die die Funktionsweise von Vigenere erläutert. Auch das 'knacken' der Verschlüsselung gehört zum Praxisteil und die dabei gemachten Erfahrungen werden hier erläutert.

15 Theorieteil

Der Theorieteil umfasst den Wikipediaartikel zu dem Thema, eine Erläuterung der Funktionsweise der Verschlüsselung und eine Beschreibung der Schwächen des Algorithmus. Diese Schwächen werden mithilfe geeigneter Krypto-Analyse-Software getestet. Die dabei gewonnenen Erkenntnisse werden im Praxisteil erläutert.

foo bar

16 Wikipedia-Artikel

16.1 Analyse ähnlicher Artikel

Um einen geeigneten Aufbau für unseren Artikel zu bestimmen, haben wir bestehende Wikipedia Einträge zu ähnlichen Themen analysiert. Die untersuchten Artikel sind:

- Caesar Verschlüsselung
- Digital Signature Algorithm (DSA)
- RSA-Kryptosystem
- Elliptic Curve Cryptography (ECC)
- Advanced Encryption Standard (AES) (auch rijndael)
- One-Time-Pad

Hier sind die Ergbenisse dazu:

16.1.1 Aufbau

- viele der Artikel enthalten eine vereinfachende Grafik um den Ablauf der Verschlüsselung grob zu umreissen
- Die untersuchten Artikel verfügen über einen Abschnitt, der den historischen Hintergrund des Algorithmus erläutert
- Allen gemeinsam ist auch, dass sie die Funktionsweise erklären
- Die Sicherheit und Analyse dieser wird als Kryptoanalyse bezeichnet und wird in der Regel in einem oder gar mehreren Kapitel behandelt
- Bei modernen und aktuellen Algorithmen werden meistens verschiedene Implementationen einzeln behandelt

16.1.2 Stil

- Um die Funktionsweise sachlich korrekt zu beschreiben werden mathematische Hintergründe beleuchtet und durch Formeln dargestellt
- Bei den simpleren Algorithmen kann ein einfaches Beispiel die Funktionsweise gut umschreiben

Hier ist noch eine Analyse anhand einiger Zitate aus den Artikeln. Dies soll als Hilfe bei der Formulierung unseres eigenen Textes dienen.

> Der öffentliche Schlüssel (public key) ist ein Zahlenpaar (e, N) und der private Schlüssel (private key) ein Zahlenpaar (d, N), wobei N bei beiden Schlüsseln gleich ist. Man nennt N den RSA-Modul, e den Verschlüsselungsexponenten und d den Entschlüsselungsexponenten. [1]

[1] [?]

An diesem Textbeispiel des RSA-Artikels ist gut ersichtlich, dass der Stil sachlich und präzise ist. Der Text ist vielleicht für den Laien nicht unbedingt verständlich - Der Artikel ist an Personen gerichtet, die bereits über Kenntnisse der Kryptographie verfügen. Die Vigenère-Chiffre ist jedoch eher für Anfänger geeignet und wird auch oft als Beispiel dazu gebraucht. Daher sollte unser Artikel verständlicher und auch für Anfänger gut verständlich sein. Als Beispiel soll hier ein Ausschnitt aus dem Artikel über die Cäsar-Verschlüsselung dienen, die auch oft als Einstieg in die Kryptographie dient:

> Neben der Nutzung eines veränderten Alphabets, in dem etwa Ziffern und Sonderzeichen enthalten sind, gibt es zudem die Variante der umgekehrten oder revertierten Caesar-Verschlüsselung. [2]

16.1.3 Entwurf

1. Einleitung
2. Geschichte
3. Einsatzgebiete
4. Beschreibung der Funktionsweise
5. Mathematische Funktionsweise
6. Variationen
7. Kryptoanalyse

[2] [**?**]