

**Projektarbeit (Informatik)**

Sichere eTest auf eBook Readern

|  |  |  |
| --- | --- | --- |
| **Autoren** |  | Simon Lukes  Daniel Jampen |
| **Hauptbetreuung** |  | Karl Rege |
| **Datum** |  | 03.12.2014 |

Ehrenwörtliche Erklärung..

Zusammenfassung

Abstract…

Inhaltsverzeichnis

[1 Einleitung 7](#_Toc405194471)

[1.1 Ausgangslage 7](#_Toc405194472)

[1.2 Problemstellung 7](#_Toc405194473)

[1.3 Zielsetzung / Aufgabenstellung / Anforderungen 7](#_Toc405194474)

[1.3.1 Muss Funktionen 7](#_Toc405194475)

[1.3.2 Wunsch Funktionen 7](#_Toc405194476)

[2 Theoretische Grundlagen 8](#_Toc405194477)

[2.1 Exportformat 8](#_Toc405194478)

[2.1.1 PDF 8](#_Toc405194479)

[2.1.2 HTML 8](#_Toc405194480)

[2.2 Kryptographie 8](#_Toc405194481)

[2.2.1 Verschlüsselung 8](#_Toc405194482)

[2.2.2 Passwort Hashing 8](#_Toc405194483)

[2.3 Konfigurationsdateien 8](#_Toc405194484)

[2.3.1 INI 8](#_Toc405194485)

[2.3.2 XML 8](#_Toc405194486)

[2.4 Import 8](#_Toc405194487)

[2.4.1 XML 8](#_Toc405194488)

[2.4.2 Open Office 8](#_Toc405194489)

[2.4.3 Word 8](#_Toc405194490)

[2.4.4 HTML 8](#_Toc405194491)

[2.5 Digitale Manipulationsmöglichkeiten 8](#_Toc405194492)

[2.5.1 Zeit 8](#_Toc405194493)

[2.5.2 Internet Zugriff 8](#_Toc405194494)

[2.5.3 Prüfungsinterne Kommunikation 8](#_Toc405194495)

[3 Analyse 8](#_Toc405194496)

[3.1 Anwendungsfälle 8](#_Toc405194497)

[3.1.1 Übersicht 9](#_Toc405194498)

[3.1.2 Akteure 9](#_Toc405194499)

[3.1.3 AF01… 9](#_Toc405194500)

[3.2 Nichtfunktionale Anforderungen 9](#_Toc405194501)

[3.2.1 NFA01.. 9](#_Toc405194502)

[4 Konzept 9](#_Toc405194503)

[4.1 High-Level 9](#_Toc405194504)

[4.2 Export 9](#_Toc405194505)

[4.2.1 Vergleichsmatrix 9](#_Toc405194506)

[4.2.2 Entscheid 9](#_Toc405194507)

[4.3 Kryptographie 9](#_Toc405194508)

[4.3.1 Verschlüsselung 9](#_Toc405194509)

[4.3.2 Passwort hashing 9](#_Toc405194510)

[4.4 Konfigurationsdateien 9](#_Toc405194511)

[4.4.1 Vergleichsmatrix 9](#_Toc405194512)

[4.4.2 Entscheid 9](#_Toc405194513)

[4.5 Import 9](#_Toc405194514)

[4.5.1 Vergleichsmatrix 9](#_Toc405194515)

[4.5.2 Entscheid 9](#_Toc405194516)

[4.6 Digitale Manipulationsmöglichkeiten 9](#_Toc405194517)

[4.6.1 Zeit 9](#_Toc405194518)

[4.6.2 Internet Zugriff 9](#_Toc405194519)

[4.6.3 Prüfungsinterne Kommunikation 9](#_Toc405194520)

[4.7 UI-Design 10](#_Toc405194521)

[4.8 C# Klassendiagramm 10](#_Toc405194522)

[4.9 JavaScript Library 10](#_Toc405194523)

[5 Umsetzung 10](#_Toc405194524)

[5.1 Export 10](#_Toc405194525)

[5.2 Kryptographie 10](#_Toc405194526)

[5.2.1 Verschlüsselung 10](#_Toc405194527)

[5.2.2 Passwort hashing 10](#_Toc405194528)

[5.3 Konfigurationsdateien 10](#_Toc405194529)

[5.3.1 Settings.xml 10](#_Toc405194530)

[5.3.2 SecureExam.xml 10](#_Toc405194531)

[5.4 Import 10](#_Toc405194532)

[5.4.1 XML 10](#_Toc405194533)

[5.4.2 Open Office 10](#_Toc405194534)

[5.5 Digitale Manipulationsmöglichkeiten 10](#_Toc405194535)

[5.5.1 Zeit 10](#_Toc405194536)

[5.5.2 Internet Zugriff 10](#_Toc405194537)

[5.5.3 Prüfungsinterne Kommunikation 10](#_Toc405194538)

[5.6 UI-Design 11](#_Toc405194539)

[5.7 JavaScript Library 11](#_Toc405194540)

[6 Testing 11](#_Toc405194541)

[6.1 Konzept 11](#_Toc405194542)

[6.2 C# Code 11](#_Toc405194543)

[6.3 HTML / JS Funktionalität 11](#_Toc405194544)

[7 Resultate 11](#_Toc405194545)

[8 Schlusswort 11](#_Toc405194546)

[9 Verzeichnisse 12](#_Toc405194547)

[9.1 Literaturverzeichnis 12](#_Toc405194548)

[9.2 Glossar 12](#_Toc405194549)

[9.3 Abbildungsverzeichnis 12](#_Toc405194550)

[9.4 Tabellenverzeichnis 12](#_Toc405194551)

[9.5 Abkürzungsverzeichnis 12](#_Toc405194552)

[10 Anhang 12](#_Toc405194553)

[10.1 Projektmanagement 12](#_Toc405194554)

[10.1.1 Zeitplan 12](#_Toc405194555)

[10.1.2 Sitzungsprotokolle 12](#_Toc405194556)

[10.2 Bedienungsanleitung 12](#_Toc405194557)

[10.2.1 Konsolenapplikation 12](#_Toc405194558)

[10.2.2 OpenOffice Import 12](#_Toc405194559)

[10.2.3 Generierte Prüfung 12](#_Toc405194560)

[10.3 Weiteres 12](#_Toc405194561)

[10.3.1 CD mit dem vollständigen Bericht als pdf-File inklusive Film- und Fotomaterial 12](#_Toc405194562)

[10.3.2 Datenträger mit weiteren Daten (z. B. Software-Komponenten) inkl. Verzeichnis der auf diesem Datenträger abgelegten Dateien 12](#_Toc405194563)

# Einleitung

Momentan werden wichtige Prüfungen fast ausschliesslich in Papierform durchgeführt. Dies trotz den immer besser werdenden technischen Möglichkeiten, Prüfungen in digitaler Form durchzuführen zu können.

Nicht nur wäre eine Umstellung auf ein digitales Format eine grosse Erleichterung für die Entlastung der Korrekturarbeit der Professoren, sondern auch für die Studenten. Zum Beispiel könnten Programmierprüfungen in gewohntem Umfeld (über die Tastatur geschriebener Sourcecode) abgehalten werden, oder auch Antworten könnten endlich sauber überarbeitet werden. Diverse dieser Verbesserungsmöglichkeiten sind sehr einfach mit digitalen Prüfungen umsetzbar, doch leider gibt es auch ein paar Schwachpunkte.  
Dadurch, dass man digital arbeitet, müssen auch die Manipulationsschutzmechanismen überarbeitet werden. Mit den vielen, heute verfügbaren, technischen Hilfsmitteln, reicht es schon lange nicht mehr aus, einfach die Prüfungsteilnehmer nach Spickzetteln zu durchsuchen.

## Ausgangslage

* Nennt bestehende Arbeiten/Literatur zum Thema  Literaturrecherche
* Stand der Technik: Bisherige Lösungen des Problems und deren Grenzen

## Problemstellung

* Nicht sicher => manipulationen
* Prüfungsfile kommt abhanden
* Infrastruktur unzuverlässig
* Kommunikationsfähigkeiten
* …

## Zielsetzung / Aufgabenstellung / Anforderungen

### Muss Funktionen

### Wunsch Funktionen

|  |  |
| --- | --- |
| Suchen einer Erinnerung | Durchsuchen der persönlichen Erinnerungen. Kriterien sind Stichworte, Daten, Status und weitere. |
| Filtern der Erinnerungen | Filtern der persönlichen Erinnerungen. Kriterien sind Stichworte, Daten, Status und weitere. |
| Administrationswerkzeug | Mit diesem Werkzeug lassen sich Benutzerkonten verwalten und Änderungen an der Website vornehmen. |

* Formuliert das Ziel der Arbeit
* (Pflichtenheft, Spezifikation)
* (Spezifiziert die Anforderungen an das Resultat der Arbeit)
* (Übersicht über die Arbeit: stellt die folgenden Teile der Arbeit kurz vor)
* (Angaben zum Zielpublikum: nennt das für die Arbeit vorausgesetzte Wissen)

# Grundlagen

## Exportformat

### PDF

### HTML

## Kryptographie

### Verschlüsselung

Die Verschlüsselung eines Datensatzes dient generell dazu, dessen Inhalt vor unberechtigten Personen zu verbergen (Confidentiality). Die zwei am weitest verbreitetsten Methoden sind die Secret Key Verschlüsselung und die Public Key Verschlüsselung. Anschliessend wird jeweils der aktuelle Standard beschrieben.

#### AES

AES wurde im Jahre 2001 offiziell publiziert und ist der momentane Standard bei der „Secret Key“ Verschlüsselung. AES verschlüsselt den gegebenen Input nicht als Ganzes, sondern unterteilt diesen in kleine Blöcke (128 bis 258 Byte), welche letztendlich Stück für Stück verschlüsselt werden.



Abbildung : AES Block Verschlüsselung

Für die Verschlüsselung der Blöcke stehen zwei verschiedene Modi zur Verfügung:

|  |  |
| --- | --- |
| ECB    Abbildung 2: ECB Verschlüsselungsmodus  Jeder Block wird unabhängig betrachtet und mit dem gleichen Schlüssel verschlüsselt. | CBC    Abbildung 3: CBC Verschlüsselungsmodus  CBC Verschlüsselt dem ersten Block mit einem Initialisierungsvektor (IV) und die folgenden Blöcke mit dem Ciphertext des jeweils vor-herigen Blockes. |

**Quelle: ISI Vorlesung**

CBC bietet im Vergleich zu ECB eine erhöhte Sicherheit gegen Manipulationen am Ciphertext. Dadurch, dass die Blöcke abhängig voneinander Verschlüsselt werden, würde beim Austauschen eines Blockciphers der jeweils vorherige beschädigt.

#### RSA

RSA ist der Standard bei der Public / Private Key Verschlüsselung. Dies bedeutet, dass für jeden Teilnehmer ein Private - sowie Public Key generiert werden muss. Mittels Signierung der Zertifikate von einer global anerkannten „Certificate Authority“ kann zusätzlich die Echtheit eines Zertifikates ermittelt werden.



Abbildung : RSA Verschlüsselung

User 2 Verschlüsselt seine Nachricht an User 1 mittels dem frei Verfügbaren Public Key von User 1 und überträgt anschliessend die verschlüsselte Nachricht an den Empfänger. User 1 kann nun die Nachricht mit seinem Private Key entschlüsseln und die Originalnachricht lesen.

### Passwort Hashing

Kryptographische Hashfunktionen berechnen aus einem variabel langen Input einen fixen Output (den Hash). Dieser muss folgende Eigenschaften aufweisen:

* Pseudo zufällig: Wenn ein Bit des Inputs verändert wird, müssen sich ca. 50% der Outputbits auch ändern.
* One Way: mit einem gegebenen Hash muss es praktisch unmöglich sein, die Ursprungs-nachricht zu ermitteln.
* Collision free: Es muss praktisch unmöglich sein, zwei Nachrichten zu finden, welche den selben Hash produzieren.

Typische Hash-Längen (Output Länge) sind je nach gewähltem Algorithmus zwischen 128 und 512 Bits lang.

Beim Passwort Hashing wird oft ein Hash-Chaining angewendet. Dies bedeutet, dass die Hash-funktion mehrmals nacheinander ausgeführt wird, um die Berechnungszeit des Hashs zu erhöhen. Ein Brute Force Angriff auf den Hash dauert, je mehr Hash-Iterationen gemacht werden, entsprechend länger.

#### SHA3

Die momentan neuste Version der SHA Algorithmen, welche vom US-Amerikanischen National Institute of Standards and Technology (NIST), veröffentlicht werden. Die verfügbaren Hashlängen sind zwischen 224 und 512 Bit, was eine Sicherheit gegen Kollisionsangriffe von 256 Bit bietet (wegen des Geburts-tagsparadoxum).

#### PBKDF2

PBKDF2 steht für Password Based Key Derivation Function und wurde entwickelt, um von einem Passwort einen Key abzuleiten, welcher in einem symmetrischen Verschlüsselungsverfahren ver-wendet werden kann.

PBKDF2 wendet auf den Input einen Hashalgorithmus mit Salting und anschliessendem Chaining an. Konfigurationsdateien

### INI

### XML

## Import

### XML

### Open Office

### Word

### HTML

## Digitale Manipulationsmöglichkeiten

### Zeit

### Internet Zugriff

### Prüfungsinterne Kommunikation

# Analyse

## Anwendungsfälle

Sicht? Anwender!

### Übersicht

### Akteure

### AF01…

## Nichtfunktionale Anforderungen

### NFA01..

# Konzept

## High-Level

### Domänenmodell

## Export

### Vergleichsmatrix

### Entscheid

## Kryptographie

### Verschlüsselung

#### Vergleichsmatrix

#### Entscheid

#### Konzept

Für eine bessere Übersicht wird der Ver- bzw. Entschlüsselungsvorgang getrennt beschrieben. Die Verschlüsselung wird automatisch mittels dem Prüfungsgenerator durchgeführt, die Entschlüsselung hingegen findet auf dem Client direkt beim Starten der Prüfung statt.

##### Verschlüsselung

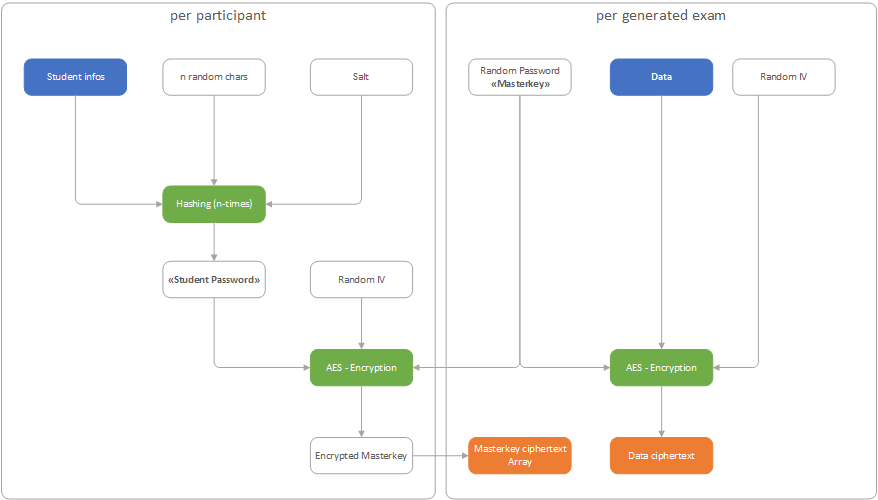


Abbildung : Multi-User AES Verschlüsselung

Für jeden Student wird ein individuelles Passwort generiert. Dieses setzt sich aus folgenden Komponenten zusammen:

* Vorname
* Nachname
* Immatrikulationsnummer
* n zufällige Zeichen (Base64)
* 128 Bit Salt.

Diese werden anschliessend n-Mal mit gehasht (vgl. 4.3.2, Passwort hashing). Mit dem resultierenden Hash (256 Bit) und einem zufälligen IV (Initialisierungsvektor) wird nun der Masterkey mittels AES verschlüsselt. Der Masterkey setzt sich aus einer zufälligen, 256 Bit langen Zeichenkette zusammen. Dieser wird dazu verwendet, um die Prüfungsdaten (Fragen, Prüfungszeitraum und Prüfungsdauer) zu verschlüsseln.

##### Entschlüsselung

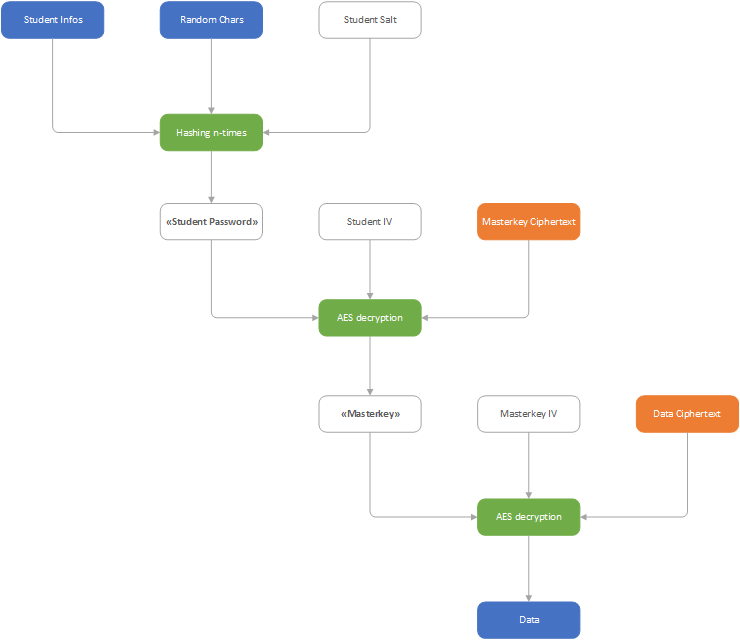


Abbildung : Multi-User AES Entschlüsselung

Jeder Student wird beim Starten der Prüfung seine Zugangsdaten eingeben müssen. Diese bestehen aus:

* Vorname
* Nachname
* Immatrikulationsnummer
* n zufällige Zeichen

Mit diesen Informationen plus dem zugehörigen Salt, wird wie bei der Verschlüsselung, ein Hashing durchgeführt. Das resultierende „Student Password“ dient als Passwort für die Entschlüsselung des Masterkeys. Mittels diesem und dem zugehörigen IV, werden dann die eigentlichen Daten entschlüsselt.

### Passwort hashing

#### Vergleichsmatrix

#### Entscheid

#### Hashing Konzept

## Konfigurationsdateien

### Vergleichsmatrix

### Entscheid

## Import

### Vergleichsmatrix

### Entscheid

## Digitale Manipulationsmöglichkeiten

### Zeit

### Internet Zugriff

### Prüfungsinterne Kommunikation

## UI-Design

Papier virtualisieren etc.

Handskizze

## JavaScript Library

### SecureExam

### CryptoJS

### FileSaver.js

# Umsetzung

Mit Code Snipplets

## Export

## Kryptographie

### Verschlüsselung

### Passwort hashing

## Konfigurationsdateien

### Settings.xml

### SecureExam.xml

## Import

### XML

### Open Office

XSLT über eigenen Parser bla bli bla bla

## Digitale Manipulationsmöglichkeiten

### Zeit

### Internet Zugriff

### Prüfungsinterne Kommunikation

## UI-Design

## JavaScript Library

# Testing

## Konzept

## C# Code

## HTML / JS Funktionalität

# Resultate

Lauffähig auf EBook und Tablet => bilder bla bla

# Diskussion und Ausblick

* Bespricht die erzielten Ergebnisse bezüglich ihrer Erwartbarkeit, Aussagekraft und Relevanz
* Interpretation und Validierung der Resultate
* Rückblick auf Aufgabenstellung, erreicht bzw. nicht erreicht
* Legt dar, wie an die Resultate (konkret vom Industriepartner oder weiteren Forschungsarbeiten; allgemein) angeschlossen werden kann; legt dar, welche Chancen die Resultate bieten
* Ausblick

# Verzeichnisse

## Literaturverzeichnis

## Glossar

## Abbildungsverzeichnis

## Tabellenverzeichnis

## Abkürzungsverzeichnis

# Anhang

## Projektmanagement

### Zeitplan

### Sitzungsprotokolle

## C# Klassendiagramm

[Bild]

Modularität bla bla bla

## Bedienungsanleitung

### Konsolenapplikation

### OpenOffice Import

### Generierte Prüfung

## Weiteres

### CD mit dem vollständigen Bericht als pdf-File und dem SourceCode