Lastenheft Matlab

Brute-Force-Software mittels verschiedener Verschlüsselungsalgorithmen

**Teammitglieder:** Adrian Gonzalez

Bruno Hürzeler

**Dozent:** Prof. Dr. Norbert Hofmann

**Fach** Matlab-Workshop (matl)

**Studiengang:** Studiengang ST-Technik

Fachhochschule Nordwestschweiz, Hochschule für Technik

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Autor** | **Datum** | **Status** | **Kommentar** |
| 0.1 | Hub | 05.04.2018 | provisorisch | Erstellung des Dokuments |
|  |  |  |  |  |

**Inhaltsverzeichnis**

[1 Zielbestimmung 3](#_Toc408915591)

[1.1 Muss 3](#_Toc408915592)

[1.2 Wunsch 3](#_Toc408915593)

[1.3 Abgrenzungskriterien 3](#_Toc408915594)

[2 Produkteinsatz 3](#_Toc408915595)

[2.1 Anwendungsbereich 3](#_Toc408915596)

[2.2 Zielgruppe 3](#_Toc408915597)

[3 Produkteumgebung 4](#_Toc408915598)

[3.1 Software 4](#_Toc408915599)

[3.2 Betriebssystem 4](#_Toc408915600)

[3.3 Hardware 4](#_Toc408915601)

[4 Produktfunktionen 4](#_Toc408915602)

[5 Produktdaten 5](#_Toc408915603)

[6 Produkt-Leistungen 5](#_Toc408915604)

[7 Benutzungsschnittstelle 5](#_Toc408915605)

[8 Qualitätsbestimmung 6](#_Toc408915606)

[9 Testfälle 6](#_Toc408915607)

[10 Anhang 6](#_Toc408915608)

# Zielbestimmung

In dieser Projektarbeit wird eine *Brute-Force* Software, welche für das Entschlüsseln von Passwörtern oder Hashes genutzt werden, realisiert. Da in der heutigen Zeit der Digitalisierung der Schutz der persönlichen Daten immer wichtiger wird, kann anhand dieser Software z.B. die Stärke des Passwortes bestimmt werden.

## Muss

1. Eingabe / Einlesen von Passwörter -oder Hashes
2. Auswahl des Verschlüsselungsalgorithmus
3. Grafische Benutzer Oberfläche für die Bedienung
4. Ressourcenauswahl für die Berechnungen
5. Ressourcenmonitor
6. Visualisieren der Parameter CPU/GPU-Temperatur und Lüfterdrehzahl
7. Fortschrittsanzeige (ProgressBar)
8. Ausgabe des geknackten Passwortes
9. Logfenster für Informationen

## Wunsch

1. Generieren von CSV-Exports mit allen relevanten Informationen
2. Berechnungen mittels MATLAB Distributed Computing Server (Cloud)
3. Menüleiste mit Raste File (New File, Export CSV, Exit) und Info (About, ..)

## Abgrenzungskriterien

Das Programm wird nur für eigens eingegebene Passwörter oder Hashes verwendet. Für die Verwendung zum Knacken von vertrauenswürdigen Daten oder Dokumente ist diese Software auf keinen Fall geeignet.

Zugelassene Zeichen für die Passwörter sind Zahlen (0-9) und Buchstaben (A-Z / a-z). Sonderzeichen sind nicht Bestandteil. Die Anzahl der Zeichen ist auf x = 8 limitiert.

Mögliche Kombinationen:

# Produkteinsatz

## Anwendungsbereich

Das Programm findet weder kommerzielle noch projektspezifische Anwendung. Es ist lediglich dazu gedacht, sich etwas in die Thematik Kryptographie einzuarbeiten und die Möglichkeiten der heutigen Entschlüsselungen vor Augen zu führen.

## Zielgruppe

Die Zielgruppe ist der Dozent Herr Norbert Hofmann sowie die Entwickler selbst.

# Produkteumgebung

Umgebung = Was für Hardware, Treiber, Bibliotheken, … benötigt Ihre Software um zu funktionieren?

## Software

~~Wenn eine unterstützte Grafikkarte vorhanden ist, so wird MATLAB ab Version R2015a benötigt um die~~ *~~„Parallel Computing Toolbox“~~* ~~verwenden zu können.~~

Die Software verwendet je nach Workstation die MATLAB-Toolbox *„Parallel Computing Toolbox“*, welche ab Version R2015a verfügbar ist.

## Betriebssystem

Die Parallel Computing Toolbox ist grundsätzlich auf den folgenden 64-Bit Betriebssystemen ausführbar:

* Windows (ab Version Windows 7)
* OS X
* Linux

Die Software muss für Windows 10 vollständig funktionsfähig werden. Als Wunsch soll die Software zusätzlich auf macOS Sierra funktionieren.

## Hardware

**CPU Berechnungen**

* PC / Laptop mit mindestens 1GB RAM
* Mindestens 5GB freier Festplattenspeicher für temporäre Daten

**GPU Berechnungen**

* CUDA-fähige NVIDIA GPUs mit Rechenkapazität 3.0 oder höher
* Für die Releases 17b und früher reicht die Rechenfähigkeit 2.0 aus

# Produktfunktionen

Funktion = Wie verhält sich ihr Programm? Was kann ein User tun?

/F10/ Einlesen des Passworts oder des Hashs

/F20/ Überprüfung der Länge des eingegebenen Passwortes

/F30/ PC-Hardware (CPU), Grafikkarte (GPU)-Informationen und Temperatur auslesen

/F40/ Dynamisierung des Ressourcenmonitors

/F50/ Beschreiben des Output-Logs

/F60/ Brute-Forcing mit ausgewähltem Algorithmus

~~/F70/ Visualisierung des Fortschritts~~

/F80/ Schreiben der Daten bei erfolgreichem Ausführen der Software (Passwort, benötigte Zeit, Anzahl Kombinationen

# Produktdaten

Daten = Was für Daten erhalten Sie? → Textdateien? Bilder? Plots? …

/D10/ Das entschlüsselte Passwort wird auf dem UI ausgegeben.

/D20/ Die CPU- / GPU-Belastung wird als 2D-Plot in Prozent als Funktion der Zeit auf dem UI ausgegeben.

/D30/ Logs mit Angaben zu Versuchsnummer, aktueller Zeit, Belastung der Ressourcen, versuchte Kombinationen werden auf dem UI ausgegeben.

/D30/ {Wunsch}: Die Logdaten sollen als csv-Datei abgespeichert werden können.

Wie Leistungsfähig ist ihr Produkt – Denken Sie z.B. an „von 0 auf 100 in 3 Sekunden; 300 PS; maximal 280 km/h; … ; Ferner: Einschränkungen, d.h. was es nicht leistet.

# Produkt-Leistungen

/L10/ Die Software soll alle Passwörter, welche den korrekten Aufbau aufweist, knacken können

/L20/ Die graphische Darstellung der Belastung der Ressourcen soll flüssig dargestellt werden können.

/L30/ Während der Entschlüsselung soll der Fortschritt in einem Balken angezeigt werden.

# Benutzungsschnittstelle

Schnittstelle = Wie kommuniziert die Software mit dem User?

Z.B. über einen Plot, Kommandofenster, …

/B10/ Die Software wird in einem Fenster angezeigt

/B20/ Die Eingabe der Passwörter / Hashs erfolgen durch die Tastatureingabe.

/B30/ Hinweise und Fehlermeldungen werden im Log Fenster ausgegeben. Ausnahme mit der Überprüfung der Passwortlänge, diese wird zur Laufzeit (während der Eingabe) überprüft. Treten dabei Fehler auf, werden diese in einem Prompt visualisiert.

/B40/ Erweiterte Einstellungen sind via Dropdown-Liste und Radio-Buttons mit der Maus anzuwählen

/B50/

/B60/

/B70/

/B80/

# Qualitätsbestimmung

Die Zielgruppe („Kunde“) der Software sind Laborratten welche Ihre Messungen möglichst schnell und einfach auswerten möchten ohne viel Zeit mit der Software zu verlieren. Die Wartung der Software erfolgt durch die Entwickler (Kermit und Lisa) selbst. Ein gewisser Wert wird auf die Korrektheit der Berechnung gelegt, wobei die Laborratten grobe Fehler aufgrund Ihrer Erfahrung sehr schnell erkennen würden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Qualitätskriterium** | **sehr gut** | **gut** | **normal** | **nicht relevant** |
| Änderbarkeit (des Codes) |  |  | x |  |
| Überprüfbarkeit (des Codes) |  |  | x |  |
| Verständlichkeit (des Codes) |  |  | x |  |
| Wartbarkeit (des Codes) |  |  | x |  |
| Benutzungsfreundlichkeit (Programm) |  | x |  |  |
| Effizienz (Programm & Code) |  | x |  |  |
| Funktionale Korrektheit (Programm) | x |  |  |  |
| Funktionale Vollständigkeit (Programm) |  | x |  |  |
| Robustheit gegenüber dem Benutzer (Programm) |  |  | x |  |

Die Qualitätsbestimmung führt normalerweise zu einigen Fragen, hierzu folgendes:

Die Begriffe "gut", "normal", etc. sind schwammig. Es geht u.a. darum Schwerpunkte zu setzen und besonderheiten hervorzuheben.

Als Hilfe zum Ausfüllen:

Denken Sie an Ihre „Kunden“:

* Ist es ein Endprodukt für Leute mit wenig Computer Erfahrung?
  + Dann muss die Benutzungsfreundlichkeit und Robustheit sehr gut sein.
* Soll das Programm weiterentwickelt werden?
  + Dann muss die Änderbarkeit und Verständlichkeit des Codes sehr gut sein.
* Müssen die Resultate auf Biegen und Brechen stimmen?
  + Dies hat direkte Folgen für die funktionale Korrektheit.
* Müssen die Resultate auf Biegen und Brechen stimmen?
  + Dies hat direkte Folgen für die funktionale Korrektheit.
* Müssen alle Knöpfe, Textfelder, Berechnungsoptionen schon funktionieren oder sind die Benutzer flexibel genug um sich der Software anzupassen?
  + Dies hat direkte Folgen für die funktionale Vollständigkeit.

# Testfälle

Wie testen Sie ob Ihre Software tut was sie soll?

/E10/ Funktionstest von sämtlichen Bedienelementen.

/E20/ Falsche Zeichen für ein Passwort eingeben

/E30/ Das Programm auf verschiedenen Computern testen.

/E40/

# Anhang

Weitere Informationen zum Lastenheft finden Sie in der Datei:

„Lastenheft - Zusammenfassung und weitere Infos.pdf“

Unterlagen zur Messung