Product Backlog

Sonja Kuklok, Michail Petermann, Amelie Reichert,
Leah Schlimm, Sven Strasser & Bartosz Treyde

3. Dezember 2021

1 Produkt-Ziel

Das Programm soll in der Übungsphase der achten Klasse eines allgemeinbildenden Gymnasiums in Baden-Württemberg einsetzbar sein. Die BenutzerInnen sollen sich mithilfe verschiedener Übungsaufgaben intensiv mit dem Thema „Kryptographie und Verschlüsselung“ auseinandersetzen und das bereits Gelernte spielerisch vertiefen. Folgende thematischen Inhalte, welche teilweise gemäß dem Lehrplan für diese Jahrgangstufe vorgesehen sind, bieten die Grundlage für die jeweiligen Level:

1. als Verschlüsselung
2. Cäsar-Verschlüsselung
3. Varianten der Cäsar-Verschlüsselung
4. Vigenère-Verschlüsselung
5. Beaufort-Verschlüsselung

Die BenutzerInnen erleben während dem Bearbeiten der Übungsaufgaben eine virtuelle Weltreise zusammen mit Alice und Bob, auf der sie die letzten existierenden „Floppy Disks“ im Auftrag des „Nationalen Informatiker Verbands“ (NIV) einsammeln müssen. Jedoch hat sich auch die böse Eve auf den Weg gemacht, um die „Floppy Disks“ zu finden. Ein Wettlauf gegen die Zeit ist gestartet. Verdeutlicht wird dies durch einen Timer pro Station.
Bei jeder Station der Weltreise müssen verschiedene Aufgaben zu jeweils einer Verschlüsselungstechnik gelöst werden. Diese Aufgaben umfassen das Ver- und Entschlüsseln gegebener Texte sowie das Beantworten von Fragen in Form von Multiple-Choice Aufgaben oder Lückentexten zum Thema „Datenschutz“ und „Kryptographie“.
Das zu entwickelnde Programm soll eine Desktopanwendung zur Einzelarbeit werden, mit Java Version 11 laufen und eine fertig kompilierte jar-Datei darstellen.

2 User Stories

1. Als BenutzerIn möchte ich das Programm starten, um das Spiel zu spielen.
   Priorität: 1

2. Als BenutzerIn möchte ich nach dem Starten des Programmes einen Text sehen, um den Spielverlauf erklärt zu bekommen.
   Priorität: 2

3. Als BenutzerIn möchte ich die verschlüsselte Nachricht sehen, um sie analysieren zu können.
   Priorität: 2

4. Als BenutzerIn möchte ich drei verschiedene Verschlüsselungsverfahren vorgeschlagen bekommen, um eine Hilfe beim Herausfinden des Verfahrens zu haben.
   Priorität: 3

5. Als BenutzerIn möchte ich nach Auswahl eines falschen Verschlüsselungsverfahren eine Mitteilung bekommen, um zu wissen, dass ich eine falsche Auswahl getroffen habe.
   Priorität: 5

6. Als BenutzerIn möchte ich nach Auswahl eines falschen Verschlüsselungsverfahrens nochmal den Kryptotext lesen können, um meine Auswahl überdenken zu können.
   Priorität: 5

7. Als BenutzerIn möchte ich bei der richtigen Auswahl des Verschlüsselungsverfahrens den entschlüsselten Text angezeigt bekommen, um ihn lesen zu können.
   Priorität: 3

8. Als BenutzerIn möchte ich eine der vorgeschlagenen Verschlüsselungsverfahren als Antwort auswählen können, um eine Lösung für die Entschlüsselungsaufgabe geben zu können.
   Priorität: 2

9. Als BenutzerIn möchte ich nach einer richtigen Auswahl des Verschlüsselungsverfahrens ein thematisch passendes Hintergrundbild sehen, damit ich mich visuell angesprochen fühle.

Priorität: 10

10. Als BenutzerIn möchte ich, dass mir bei einer richtigen Auswahl die richtige Antwort nochmal angezeigt wird, um meine Auswahl zu bestätigen.
    Priorität: 9

11. Als BenutzerIn möchte ich dauerhaft im Level einen Timer eingeblendet bekommen, um zu wissen wie viel Zeit ich noch in dem Level habe.
    Priorität: 6

12. Als BenutzerIn möchte ich die Multiple-Choice Fragen starten, um sie beantworten zu können.
    Priorität: 2

13. Als BenutzerIn möchte ich das Level von vorne beginnen, falls der Timer abgelaufen ist, um trotzdem die Möglichkeit zu haben das Spiel abzuschließen.
    Priorität: 4

14. Als BenutzerIn möchte ich drei Antwortmöglichkeiten der Multiple-Choice Fragen angezeigt bekommen, um die richtige Antwort auswählen zu können.
    Priorität: 2

15. Als BenutzerIn möchte ich eine Nachricht erhalten, um zu wissen, ob meine Antwort der Multiple-Choice Fragen richtig war.
    Priorität: 4

16. Als BenutzerIn möchte ich mich nach einer falschen Antwort einer Multiple-Choice Frage für eine andere entscheiden können, um meine Auswahl überdenken zu können.
    Priorität: 3

17. Als AdministratorIn möchte ich, dass der BenutzerIn bei einer falschen Antwort eine Zeitstrafe von einer bestimmten Sekundenzahl bekommt, um das Spiel spannender zu gestalten.
    Priorität: 8

18. Als BenutzerIn möchte ich eine Rückmeldung bekommen, wenn ich alle Multiple-Choice Fragen richtig beantwortet habe, um mit der Verschlüsselungsaufgabe beginnen zu können.

Priorität: 4

19. Als BenutzerIn möchte ich die Verschlüsselungsaufgabe starten können, um sie lösen zu können.
    Priorität: 2

20. Als BenutzerIn möchte ich den Text, das Verschlüsselungsverfahren und den Schlüssel, mit dem ich dem Text verschlüsseln soll, angezeigt bekommen, um genau zu wissen, wie ich die Nachricht verschlüsseln soll.
    Priorität: 3

21. Als BenutzerIn möchte ich die verschlüsselte Nachricht abschicken können, um kontrollieren zu können, ob ich Fehler gemacht habe.
    Priorität: 3

22. Als BenutzerIn möchte ich bei erfolgreicher Verschlüsselung eine Rückmeldung erhalten, um zu erfahren, dass ich das Level beendet habe.
    Priorität: 4

23. Als BenutzerIn möchte ich die Entschlüsselungsaufgabe starten können, um sie lösen zu können.
    Priorität: 2

24. Als BenutzerIn möchte ich die Häufigkeitsverteilung der einzelnen Buchstaben des verschlüsselten Textes angezeigt bekommen, um den Text entschlüsseln zu können.
    Priorität: 3

25. Als BenutzerIn möchte ich die Buchstabenhäufigkeit der deutschen Sprache eingeblendet bekommen, um sie mit der Häufigkeitsverteilung des verschlüsselten Textes zu vergleichen und den Text entschlüsseln zu können.
    Priorität: 3

26. Als BenutzerIn möchte ich die Häufigkeitsverteilung des verschlüsselten Textes und die Buchstabenhäufigkeit der deutschen Sprache graphisch in einem Diagramm angezeigt bekommen, um den Text entschlüsseln zu können. (Optional)
    Priorität: 5

27. Als BenutzerIn möchte ich, dass das Programm bei der Vigenère-Verschlüsselung und der Beaufort-Verschlüsselung eine N-Gramm Analyse (Länge der N-Gramme: 1 bis 4) durchführen kann, um die möglichen Schlüssellängen, nach Wahrscheinlichkeit geordnet, angezeigt zu bekommen.
Priorität: 4

28. Als BenutzerIn möchte ich die Häufigkeitsverteilung des verschlüsselten Textes und die Buchstabenhäufigkeit der deutschen Sprache bei der Vigenère-Verschlüsselung und der Beaufort-Verschlüsselung graphisch gegeneinander Verschieben, um den eingegeben Chiffretext zu lösen und das Ergebnis live angezeigt bekommen. (Optional)
Priorität: 5

29. Als BenutzerIn möchte ich kurze Beschreibungstexte zur Funktionsweise des Tools eingeblendet bekommen.
Priorität: 6

30. Als AdministratorIn möchte ich nach Beendigung des Spiels die Multiple-Choice Antworten meiner BenutzerInnen in einer txt-Datei angezeigt bekommen. (Optional)
Priorität: 8

31. Als AdministratorIn möchte ich über eine txt-Datei eigene Multiple-Choice Fragen in das Spiel laden können. (Optional)
Priorität: 7

32. Als AdministratorIn will ich, dass die Multiple-Choice Fragen jedem Level zufällig zugeteilt werden, um zu gewährleisten, dass die BenutzerInnen nicht voneinander abschreiben können. (Optional)
Priorität: 8

33. Als AdministratorIn will ich, dass das Programm die Rätseltexte eigenständig und mit einem zufälligen Schlüssel verschlüsselt, um zu gewährleisten, dass die BenutzerInnen nicht voneinander abschreiben können. (Optional)
Priorität: 7

34. Als AdministratorIn will ich, dass das Schlüsselwort in Level vier und fünf zwischen 4 und 8 Buchstaben enthält, um den Schwierigkeitsgrad der Aufgabe bei allen BenutzerInnen möglichst vergleichbar zu halten. (Optional)
Priorität: 7

35. Als BenutzerIn möchte ich einen Hinweis anfordern können, wenn ich in einem Level nicht mehr weiterkomme. (Optional)
    Priorität: 9

36. Als AdministratorIn möchte ich nur eine Klasse hinzufügen müssen, um das Spiel um ein Level mit einem anderen Verschlüsselungsverfahren erweitern zu können.
    Priorität: 9

37. Als AdministratorIn möchte ich nach Beendigung des Spiels die Bearbeitungszeiten meiner BenutzerInnen bei den einzelnen Aufgaben in einer txt-Datei gespeichert haben, um zu sehen, wie schwer den BenutzerInnen die Aufgaben gefallen sind.
    Priorität: 9

3 Interfaces

Die Folgenden Interfaces dienen als Hilfe für die Umsetzung der graphischen Nutzeroberfläche:

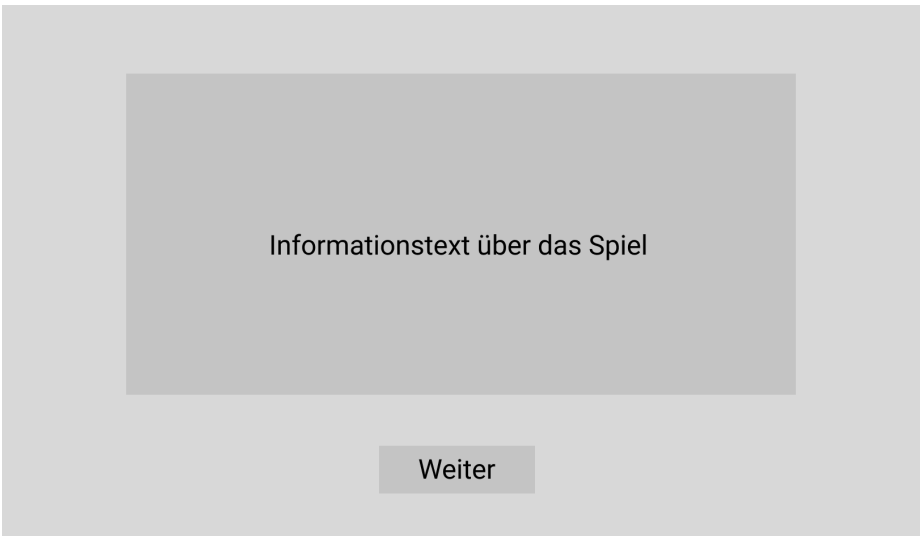

Abbildung 1: Informationstexte

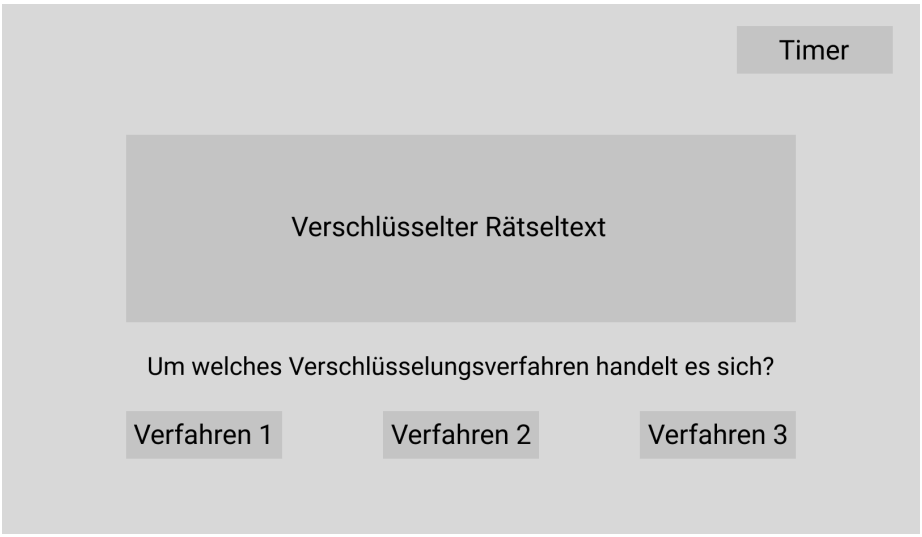

Abbildung 2: Entschlüsselungsaufgabe: Aufgabenstellung

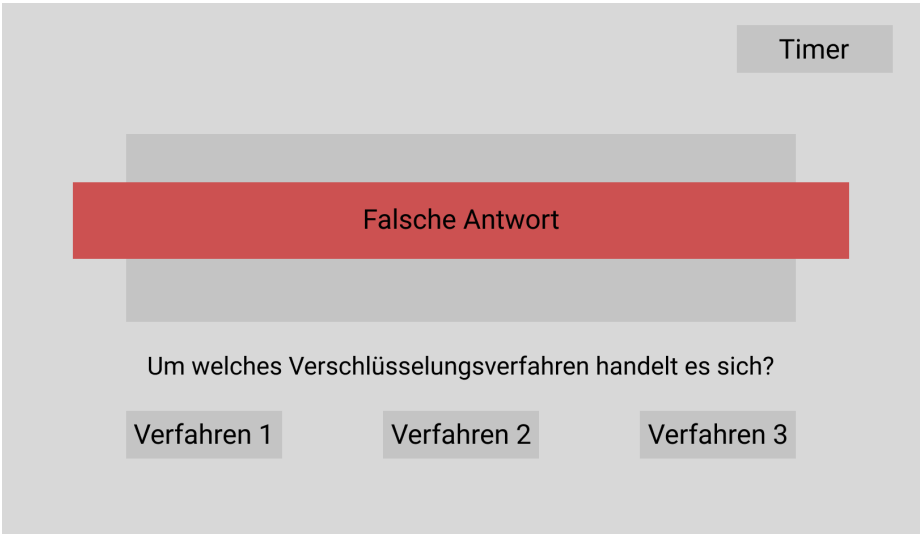

Abbildung 3: Entschlüsselungsaufgabe: Falsche Antwort

Abbildung 4: Entschlüsselungsaufgabe nach Entschlüsselung: Aufgabenstellung

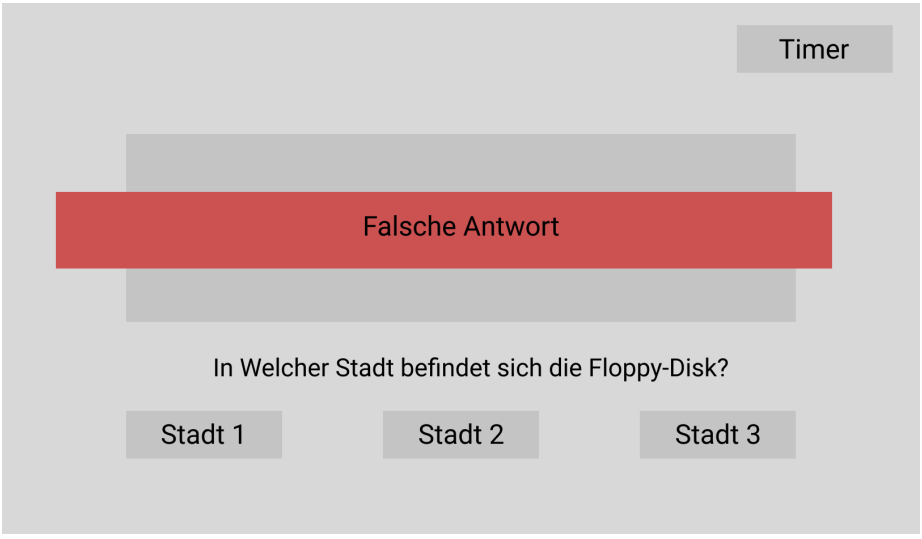

Abbildung 5: Entschlüsselungsaufgabe nach Entschlüsselung: Falsche Antwort

Abbildung 6: Multiple-Choice Fragen

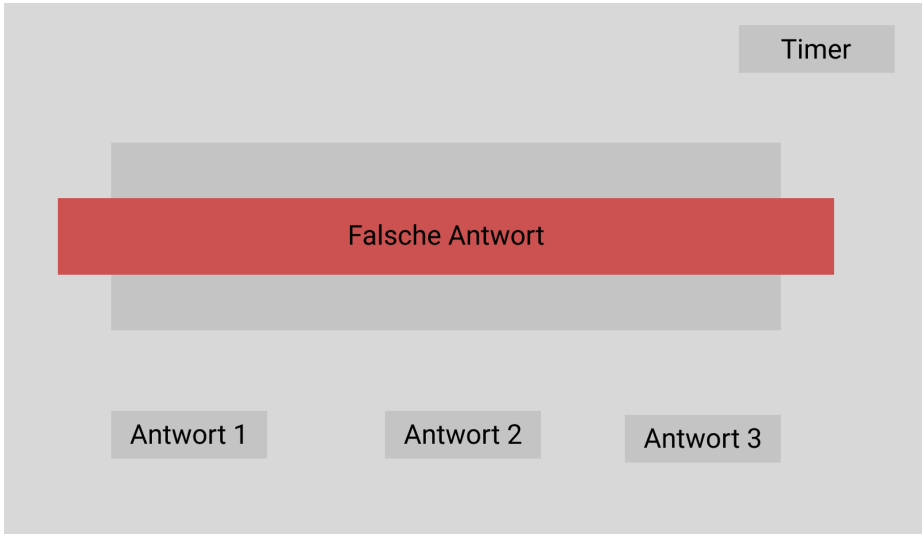

Abbildung 7: Multiple-Choice Fragen: Falsche Antwort

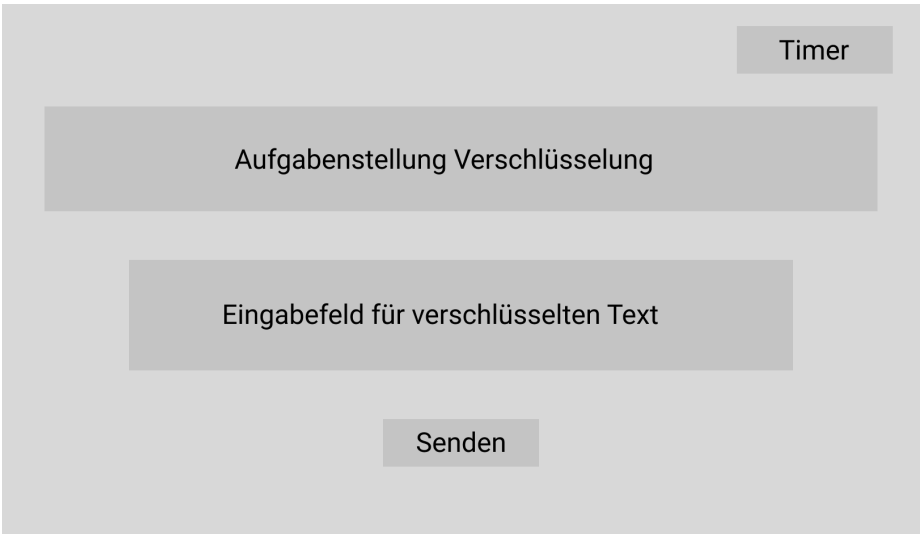

Abbildung 8: Verschlüsselungsaufgabe: Aufgabenstellung

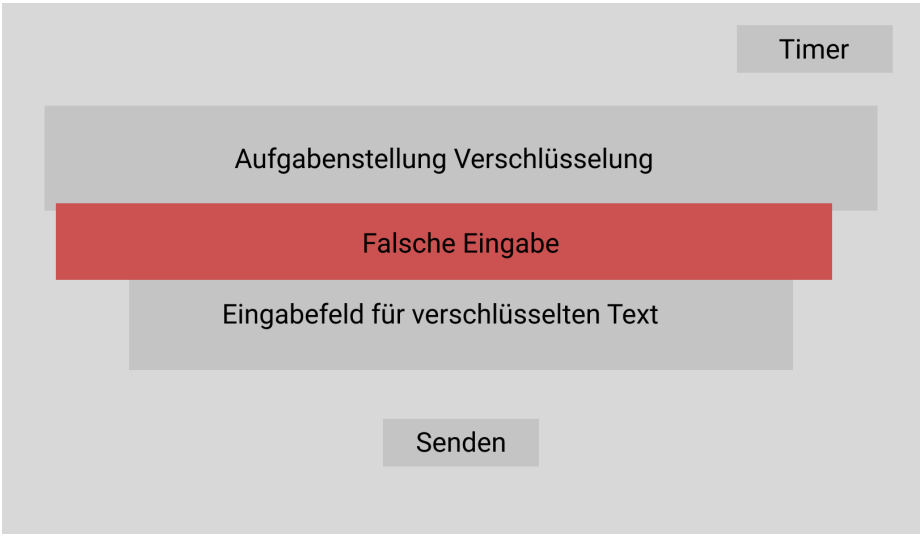

Abbildung 9: Verschlüsselungsaufgabe: Falsche Eingabe

4 Definition of Done

- Code ist kompilierbar mit Java 11.
- Jede ausgewählte Userstory ist implementiert.
- Jede bereits implementierte Userstory ist getestet (per JUnit oder per Interaktion).
- Alle im Code enthaltenen Klassen und Methoden sind ausreichend kommentiert.
- Ein Code-Review ist erfolgt.
  - Der Code wurde mindestens einmal vollständig durchgelesen.
  - Die Kommentare wurden auf Vollständigkeit und Sinnhaftigkeit überprüft.
  - Der Code wurde auf Einheitlichkeit überprüft.
- Die Entwurfsdokumente sind aktualisiert.
  - Die UML-Diagramme sind aktualisiert.
  - Die Sequenz-Diagramme sind aktualisiert.
  - Die Burn-Up oder Burn-Down Diagramme sind aktualisiert.
  - Die didaktischen Überlegungen sind überprüft und erweitert.
- Das Programm zeigt einen Waitcurser bei längeren Wartezeiten an.

5 Wichtige Entscheidungen

5.1 Didaktische Überlegungen:

Das Programm soll

- für die Klasse 8 verwendet werden können.
- zur Vertiefung der Lerninhalte in der Übungsphase verwendet werden.
- innerhalb einer Schulstunde von 90 Minuten durchgespielt werden.
- im Einzelspielermodus bearbeitet werden.
- die Kommunikation der Spieler untereinander nicht unterstützen.

5.2 Anforderungen an die Einsatzumgebung und das Programm:

Das Programm soll

- als Desktopanwendung für PCs verwendet werden.
- in Java geschrieben werden.
- auf einem Gerät mit mindestens Java Version 11 laufen.
- lizenzfreie oder frei zugängliche Medienelemente verwenden.
- mit der Creative Common License lizensiert werden.
- modular aufgebaute Level besitzen.
- einfach erweiterbar sein.

5.3 Muss-Kriterien:

Das Programm muss

- die Antworten der BenutzerInnen bei den Multiple-Choice Fragen als txt-Datei speichern.
- in jedem Level eine Aufgabe zum Verschlüsseln enthalten.
- in jedem Level eine Aufgabe zum Entschlüsseln enthalten.
- in jedem Level Multiple-Choice Fragen zu Datenschutz/Kryptographie enthalten.
- im ersten Level das Rückwärts-Schreiben als Verschlüsselung behandeln.

- im zweiten Level die Cäsar-Verschlüsselung behandeln mit einem bestimmten Schlüssel behandelt.
- im dritten Level die Variante der Cäsar-Verschlüsselung mit verschiedenen Schlüsseln behandeln.
- im vierten Level die Vigenère-Verschlüsselung behandeln.
- im fünften Level die Beaufort-Verschlüsselung behandeln

5.4 Kann-Kriterien:

Das Programm kann (optional)

- AdministratorInnen die Multiple-Choice Fragen selbst auswählen und erstellen lassen.
- AdministratorInnen eigenständig Level und Rätsel hinzufügen lassen.
- Spielstände speichern.
- Eingaben der BenutzerInnen im Hintergrund speichern.
- die Bearbeitungszeiten der BenutzerInnen bei den einzelnen Aufgaben in einer txt-Datei speichern, um sie mit einem externen Programm analysieren zu können.
- die gesammelte Multiple-Choice Fragen in einer txt-Datei zufällig auf die einzelnen Level verteilen.
- die Verschlüsselung der Rätselaufgabe wird vom Programm ausgeführt, damit die BenutzerInnen unterschiedliche Aufgaben bekommen.
- bei der Vigenère-Verschlüsselung ein zwischen 4 und 8 Buchstaben langes Schlüsselwort enthalten.
- einen Hinweis-Button enthalten, über den die BenutzerInnen Tipps anfordern können.
- im fünften Level die Vigenère-Verschlüsselung mit verschiedenen Schlüsseln behandeln.

6 Projektplanung

Wir arbeiten mit

- Miro für den Aufbau des Scrum-Boards
- Microsoft Teams für unsere Besprechungen und das Teilen von Dateien
- Microsoft Word für unsere Notizen
- Lucidchart für die Erstellung von Entwurfsdokumenten
- Github für die Quellcode Dokumentation
- Mindestens Java Version 11
- JavaFX für die Graphische Nutzeroberfläche
- Latex für die Ausformulierung des Backlogs
- Leah Schlimm als Scrum-Master im 1. Sprint
- Sonja Kuklok als Scrum-Master im 2. Sprint
- Sven Strasser als Scrum-Master im 3. Sprint
- Bartosz Treyde als Scrum-Master im 4. Sprint
- Amelie Reichert als Scrum-Master im 5. Sprint
- Michail Petermann als Scrum-Master im 5. Sprint

Glossar

AdministratorIn Der Nutzer der Software, der das Spiel um eigene Level und Inhalte ergänzen kann.

Beaufort-Verschlüsselung Die Beaufort-Verschlüsselung funktioniert analog zu der Vigenère-Verschlüsselung, es wird lediglich ein rückwärts geschriebenes Alphabet verwendet.

BenutzerIn Der Nutzer der Software, der lediglich das Spiel spielen kann.

Cäsar-Verschlüsselung Bei diesem Verfahren wird der jeder Buchstabe des Klartextes mit dem Buchstaben 'C' verschlüsselt.

Entschlüsselungsaufgabe Eine Aufgabe, bei der die BenutzerInnen einen verschlüsselten Rätseltext entschlüsseln müssen.

Level Ein Abschnitt des Programmes, der jeweils eine Entschlüsselungsaufgabe, eine Verschlüsselungsaufgabe und eine bsetimmte Anzahl an Multiple-Choice Fragen absolvieren müssen.

Rückwärts-Schreiben Bei diesem Verfahren wird jedes Wort eines gegebenen Textes rückwärts geschrieben. Die Reihenfolge der Wörter bleibt dabei die gleiche wie bei dem unverschlüsselten Text.

Variante der Cäsar-Verschlüsselung Bei diesem Verfahren wird der Text analog zur Caesar-Variante verschlüsselt. Im Gegensatz zur Caesar-Verschlüsselung entspricht die Verschiebung der Buchstaben dabei nicht zwingend dem Buchstaben 'C', sondern ist beliebig wählbar.

Verschlüsselungsaufgabe Eine Aufgabe, bei der die BenutzerInnen einen Text mit einem vorgegebenen Verfahren verschlüsseln müssen.

Vigenère-Verschlüsselung Die Vigenère-Verschlüsselung ist ein polyalphabetisches Verschlüsselungsverfahren, bei dem das Schlüsselwort unterhalb des Klartextes so lange wiederholt wird, bis die gesamte Länge des Klartextes abgedeckt ist. Jeder Buchstaben wird nun mit dem jeweils unterhalb stehenden Schlüssel verschlüsselt.