Programmieren eines Escape Room Videospiels über kryptografische Methoden

Maturaarbeit

Medea Emch, G19f

12. August 2022

Betreuung: Adrian Häfliger, Fachschaft Informatik

Kantonsschule Alpenquai Luzern | ksalpenquai.lu.ch

Abstract Gegenstand der vorliegenden Maturaarbeit ist der Prozess des Programmierens eines Videospiels und die Recherche und Aufarbeitung der darin benutzten kryptografischen Methoden.

Inhaltsverzeichnis

1 Vorwort und Danksagung

Anfangs fiel es mir schwer Ideen für eine Maturaarbeit zu finden. Es war mir klar das es ein naturwissenschaftliches Thema sein sollte, aber ich konnte mir kaum vorstellen wie so ein Thema oder eine Leitfrage aussehen sollte. Da ich Ende Schuljahr 2020/2021 als Mathematik-Projekt ein kleines Jump-and-Run Game mit Python programmiert habe, war meine erste Idee erneut ein Game zu programmieren, aber in einem anderen Genre. Genauere Ideen, was für ein Game es werden könnte, hatte ich nicht.

Schlussendlich verfasste ich eine Liste mit allen naturwissenschaftlichen Themen die mich interessierten und ging damit an eine erste Besprechung mit meinem potentiellen Betreuer, Herr Adrian Häfliger, der mich darauf hinwies, dass ich Punkte meiner Liste auch kombinieren könnte. Daraus und aus meiner Liebe zu Escape Rooms kam mir die Idee, ein Escape Room Game über Kryptografie zu programmieren, da Kryptografie ein Thema meiner Liste war.

Ich möchte mich zuallererst bei Herrn Adrian Häfliger bedanken, der diese Maturaarbeit sehr unkompliziert betreut hat und immer zur Verfügung stand, wenn irgendwelche Fragen oder Unklarheiten auftauchten. Weiter bedanke ich mich bei meinen Eltern, die mich in den Sommerferien auf Trab gehalten haben und meinen Freunden, die mein zum Teil endloses Gefasel über Kryptografie und Programmieren ertragen haben.

2 Einleitung

3 Hauptteil

3.1 Behandelte kryptografische Methoden

3.1.1 Geheimtinte

Die einfachste Art, einen geheimen Text zu vermitteln, ist natürlich, wenn er gar nicht gesehen werden kann. Dies kann mit verschiedenen Chemikalien erreicht werden, die unter Normalbedingungen farblos sind und entweder durch Hitze, UV-Licht oder chemische Behandlungen sichtbar werden. Diese Art von «Verschlüsselung» gehört nicht zum Themenbereich der Kryptografie, sondern dem der Steganografie. Diese beschäftigt sich mit dem Verstecken geheimer Nachrichten. Dies geschieht zum Besispiel mit Geheimtinte oder indem die Nachricht in einer anderen nicht geheimen Nachricht versteckt wird.

Berichte über Geheimtinte gehen bis weit vor Christus zurück, wo sie im alten Griechenland und im römischen Reich bereits benutzt wurde. Zumeist wurde Geheimtinte im Krieg benutzt, bevor fortgeschrittene Technologien wie Telegrafen oder Radio entwickelt waren und alle Nachrichten niedergeschrieben und so verschickt werden mussten.

3.1.2 Caesar-Verschlüsselung

Caesar ist eine der simpelsten Verschlüsselungen und wird heute fast ausschliesslich benutzt, um Kryptographie einfach zu erklären, da es für heutige Verwendungen viel zu unsicher ist.

Für die Verschlüsselung wird zusätzlich zum Klartextalphabet ein Geheimalphabet benutzt, wobei jeder Buchstabe jeweils einem bestimmten verschlüsselten Buchstaben entspricht.

Das verschlüsselte Alphabet erhält man, indem man die Zeichen des lateinischen Alphabets um eine bestimmte Anzahl verschiebt (wobei der Anfang des Klartextalphabets zyklisch am Ende des Alphabets angefügt wird, sodass es aufgeht) und jeweils den Klartextbuchstaben mit dem resultierenden Geheimtextbuchstaben ersetzt. Um anzugeben um wie viel das ALphabet verschoben wurde, wird entweder die Anzahl der Stellen oder der Schlüsselbuchstabe (der Buchstabe, durch den A ersetzt wurde) angegeben.

Beispiel für eine Verschiebung um 10 Buchstaben:

Somit wird aus dem Wort «BEISPIEL» «LOSCZSOV», wenn es verschlüsselt wird. Um den Geheimtext wieder zu entschlüsseln wird der ganze Vorgang rückwärts angewandt. Der Schlüssel (in diesem Fall K) wird dabei von A ersetzt.

Die Caesar-Verschlüsselung kann auch mathematisch dargestellt werden, indem man jedem der 26 Buchstaben eine Zahl zuordnet (A = 0, B = 1, ..., Z = 25). Mit diesen Zahlen kann man die Caesar-Verschlüsselung als ganz einfache Addition darstellen. Dazu wird zum Wert des Klartextbuchstabens K einfach der Wert des Schlüsselbuchstabens S addiert.

Da es aber Fälle gibt, in denen das Resultat grösser als 25 ist und es keinen Buchstaben mit einem so hohen Wert gibt, muss auf das Resultat eine Modulo-26 Rechnung angewandt werden. Dabei wird der Rest einer Division durch 26 berechnet.

Somit ist die Caesar-Verschlüsselung mathematisch definiert als:

encrypt

Die dazugehörende Entschlüsselung eines Geheimtextbuchstabens G entspricht dann:

decrypt

Da die Caesar-Verschlüsselung eine monoalphabetische Verschlüsselung ist, das heisst, jeder Klartextbuchstabe im Klartextalphabet genau einem Geheimbuchstaben im Geheimalphabet entspricht, kann sie durch Statistik sehr leicht geknackt werden. Jede

Sprache hat eine charakteristische Verteilung der Buchstaben, die leicht in einem Graph aufgezeichnet werden können:

(Graph von der Buchstabenverteilung in der deutschen Sprache einfügen)

Wenn also das ganze Alphabet um beispielsweise 10 Stellen verschoben wird, sieht die Verteilung folgendermassen aus:

(Graph der Buchstabenverteilung 10 Stellen verschoben einfügen)

Da der Verlauf des Graphen immer noch derselbe ist und man weiss, dass E der häufigste Buchstabe ist, kann man nun schliessen, dass das O des Geheimalphabets dem E des Klartextalphabets entspricht. So kann man die Verschiebung berechnen und daraus das Klartextalphabet ableiten.

Da die Buchstabenverteilung jedoch erst in genügend langen Texten genau ist, sollten einzelne Wörter und kurze Sätze in dieser Hinsicht noch einigermassen sicher sein.

Allerdings ist eine weitere Schwäche der Caesar-Verschlüsselung jedoch, dass es nur 25 mögliche Schlüssel gibt, man also spätestens nach 25 Versuchen den Klartext erhält. Vor dieser Angehensweise sind dann auch kurze Sätze und einzelne Wörter nicht mehr sicher.

Im Englischen gibt es zusätzlich noch das Problem, dass es nur zwei Möglichkeiten gibt für Wörter mit einem Buchstaben («I» = ich und «a» = ein), was das Knacken noch zusätzlich beschleunigt, besonders da beides eher häufige Wörter sind.

Atbasch ist eine ursprünglich auf dem hebräischen Alphabet basierende Variante der Caesar-Verschlüsselung, die auch als umgekehrte Caesar-Verschlüsselung bezeichnet wird, denn statt dass die Buchstaben um eine bestimmte Anzahl Stellen verschoben werden, ist das Geheimalphabet lediglich das Klartextalphabet aber rückwärts, sodass A zu Z wird, B zu Y, und so weiter.

Der Name Atbasch leitet sich dabei von den ersten zwei Buchstabenpaaren ab, die einander ersetzen (Aleph mit Taw und Beth mit Schin) Speziell an Atbasch ist, dass zum Entschlüsseln der gleiche Prozess benutzt werden kann wie zum Verschlüsseln, da die Buchstaben symmetrisch ausgetauscht werden.

(Beispiel einfügen)

ROT13 ist eine weitere Variante der Caesar-Verschlüsselung die den gleichen Prozess zum Verschlüsseln und Entschlüsseln benutzt. Hier sind die Buchstaben zwar wie in der normalen Caesar-Verschlüsselung verschoben, aber genau um ein halbes Alphabet, also 13 Stellen. Wenn man also ein Buchstabe verschlüsselt (um 13 Stellen verschiebt) und entschlüsselt (um weitere 13 Stellen verschiebt), hat man den Buchstaben um insgesamt

26 Stellen, also ein ganzes Alphabet verschoben, womit man wieder beim Ausgangsbuchstaben landet.

(Beispiel einfügen)

3.1.3 Vigenère-Verschlüsselung

Anders als bei der Cäsar-Verschlüsselung wird bei der Vigenère-Verschlüsselung ein Schlüssel in Kombination mit 26 Geheimalphabeten benutzt. Dabei wird der Schlüssel so oft wiederholt, bis er die Länge der zu verschlüsselnden Nachricht deckt.

Geschichte sdftadfgdfg

Sicherheit sdftsdfgdfg

Varianten Die **Trithemius-Verschlüsselung** ist der Vorläufer der Vigenère-Verschlüsselung und wurde vom deutschen Autor und Mönch Johannes Trithemius im frühen 16. Jahrhundert zusammen mit der Tabula Recta erfunden. Für diese Verschlüsselung benutzt man auch die Tabula Recta aber im Vergleich zu der normalen Vigenère-Verschlüsselung benutzt man keinen Schlüssel, sondern man rückt bei jedem Buchstaben eine Zeile der Tabula Recta weiter nach unten. Im Grunde genommen ist die Trithemius-Verschlüsselung also eine Vigenère-Verschlüsselung mit einem fixen Schlüssel ABCDEFGHIJKLMNOPQRSTUVWXYZ.

Da die Vigenère-Verschlüsselung nicht reziprok ist, das heisst dass das Vorgehen des Verschlüsselns nicht das gleiche ist wie das Vorgehen beim Entschlüsseln, kann man auch «in die falsche Richtung» verschlüsseln und den Klartext sozusagen «entschlüsseln», sodass man es nachher mit der normalen Verschlüsselungstechnik wieder entschlüsseln kann. Dies wird als Beaufort Variante bezeichnet und ist nicht zu verwechseln mit dem Beaufort-Chiffre.

3.2 Dokumentation

4 Reflexion und Ausblick

Wenigstens kann ich jetzt LaTeX, sonst hat die Arbeit aber nichts gebracht.

Abbildungsverzeichnis

Abbildungen ohne Quellenangaben wurden von der Autorin selbst erstellt.

Tabellenverzeichnis

Sämtliche Tabellen wurden vom Autor selbst erstellt.

Redlichkeitserklärung

Ich erkläre hiermit,

- dass ich die vorliegende Arbeit selbständig verfasst und nur die angegebenen Quellen benutzt habe,
- dass ich auf eine eventuelle Mithilfe Dritter in der Arbeit ausdrücklich hinweise,
- dass ich vorgängig die Schulleitung und die betreuende Lehrperson informiere, wenn ich
  - diese Maturarbeit bzw. Teile oder Zusammenfassungen davon veröffentlichen werde

  oder
  - Kopien dieser Arbeit zur weiteren Verbreitung an Dritte aushändigen werde.
- dass mir das Merkblatt «Plagiat» sowie auch die Konsequenzen eines Plagiats bekannt sind.

Meine Maturaarbeit umfasst (ohne Titelblatt, Inhaltsverzeichnis, Redlichkeitserklärung und Abgabeinformationen, Quellen- und sonstigen Verzeichnissen und Anhang) xyz Zeichen (ohne Leerzeichen).

Ich gebe zu den Maturaarbeitsexemplaren folgende Gegenstände oder Produkte ab: Ein Datenträger mit den folgenden Inhalten:

- Den gesamten Quellcode des Spiels inkl. Grafiken und andere Dateien die dazugehören
- Eine kompilierte Version des Spiels (.exe Datei)
- Eine ReadMe-Datei, die erklärt welche Dateien wo dazugehören und wie sie benutzt werden.

Kriens, 12. August 2022

Medea Emch