Entwurf einer Lernexpedition (LEX)
Codes, eine Reise durch die Welt der Verschlüsselungen

von Karoline Wewerke

Eine Lernexpedition ist wie das Wort schon sagt eine Expedition mit unbekanntem Ausgang. Ich gehe mit meinen Schiff vor einer fremden Küste vor Anker und erforsche das neue Land, kartographiere und vermesse, oder ich untersuche einen neuen Teil einer mir schon bekannten Insel…

Wichtig ist jedenfalls: Vor mir liegt unbekanntes Gebiet, ich weiß nicht was auf mich zukommt, ich kann reich beladen zurückkehren mit Schätzen, Geschichten oder einem Heilmittel gegen Krebs. Oder aber ich verlaufe mich, ich habe nicht genug Verpflegung dabei gehabt, mein Weg war so zugewachsen das ich nicht weiterkonnte, das Wetter war einfach katastrophal oder mein Reitelefant ist krank geworden.
Auch in diesem Fall komme ich zurück, ohne fertige Karte und mit einem kranken Elefanten. Natürlich ist das nicht der wünschenswerteste Ausgang, aber ich habe trotzdem meine Erfahrungen gemacht. Ich habe selbstständig und eigenverantwortlich gehandelt und der Elefant wird bestimmt wieder gesund.

Bei Lernformaten wie einer Lex ist es nicht einfach, das Ende vorherzusehen. Dies ist für mich im Zusammenhang mit Schule etwas vollkommen Neues und etwas, das mir sehr am Herzen liegt. Ich als Schüler bekomme die Möglichkeit vollkommen frei zu lernen. Ich bekomme Vertrauen und Kontrolle über mein Lernen, kann es besser mit dem Leben verknüpfen. Dabei ist es vollkommen in Ordnung, wenn mal nicht alles nach Plan läuft.

Die Lex die ich modelliert habe ist für 10 Tage ausgelegt und orientiert sich an einem Buch von Simon Singh (Codes, Die Kunst der Verschlüsselung). Es ist sozusagen das Standartwerk für diese Lex. Ich untersuche in der Lex verschiedene Geheimschriften und möchte mich auch mit der Entwicklung von Codes beschäftigen.

Tag 1
Einführung in die Welt der Geheimschriften und Codes, Monoalphabetische Verschlüsselungen
Ich beginne gerne am Anfang. Bei einem Thema wie Geheimschriften ist das meiner Meinung nach auch der beste Weg, denn über die Jahrhunderte sind Codes immer komplexer geworden. In diesem Fall liegt der Anfang wohl im 5. Jahrhundert vor Christus bei Herodot. Schon er erwähnt in seinen Werken eine Möglichkeit der geheimen Kommunikation. Nun geht es über Julius Cäsar in einem Schnelldurchlauf durch die Geschichte der Kryptographie ins 16. Jahrhundert zu Maria Stuart, die ja letztendlich nur ermordet werden konnte weil eine geheime Botschaft entschlüsselt werden konnte. Es werden also eingehend die Schwächen der Verschlüsselungsmethode deutlich.
Ich beschäftige mich jedoch nicht nur mit bestimmten Personen und dem Einfluss von Codes auf ihr Leben. Ich nehme mir auch Zeit um mir die Verschlüsselung an sich zu betrachten. Ich lerne die Häufigkeitsanalyse kennen (Eine Methode der Dechiffrierung monoalphabetischer Texte) und Verschlüssle/Entschlüssle selber Nachrichten.
Am ersten Tag tauche ich ein in die Welt der Geheimschriften und Codes. Dazu müssen zunächst einmal bestimmte Begriffe klar werden. Was bedeutet eigentlich Kryptographie und gibt es noch andere Möglichkeiten der geheimen Kommunikation? Wo liegen die Unterschiede von Kryptographie

und Kryptoanalyse oder von Codierung und Chiffrierung? Was ist Substitution und was Transposition und was bitte ist ein Nomenklator? Kurz ich schaue mir die Grundbegriffe an. Ich ordne mein Thema in das mir bekannte ein, bestimme sozusagen die Position der unbekannten Insel auf meiner Seekarte.

Tag 2

Einführung in die Welt der Geheimschriften und Codes, Polyalphabetische Verschlüsselung

Da die monoalphabetische Verschlüsselung keine sichere Geheimschrift mehr darstellt entwickelt Blaise de Vignere im 16. Jahrhundert die Vignere-Chiffree eine polyalphabetische Verschlüsselung. Ich versuche mich mit Hilfe der Methode von Charles Babbage auch an ihrer Verschlüsselung, brauche dafür aber schon deutlich länger. Ich nehme den Tag um die Verschlüsselung zu verstehen und stoße des Weiteren auf „The Beale Papers" und beschließe, mich an Tag 3 mit ihnen zu beschäftigen. Außerdem erregen Stichworte wie Bibelcode und Freimaurercode mein Interesse.

Tag 3

The Beale Papers

Thomas J. Beale war, soweit es ihn wirklich gab, ein Mann in Virginia des 19. Jahrhunderts. Er hinterlässt der Welt 3 geheimnisvolle Blätter voller Zahlen und einen angeblichen Schatz, den Beale in Virginia versteckt haben soll. Die Zahlen auf den Blättern bilden die sagenumwogene Beale-Chiffre und sind bis heute nur teilweise entschlüsselt. Auf dem ersten der 3 Blätter soll beschrieben sein, wo das Gold versteckt ist, auf dem zweiten steht, woraus der Schatz besteht und das dritte soll Auskunft darüber geben für wen er bestimmt ist. Natürlich ist nur das 2. Blatt bis heute dechiffriert und zwar ausgerechnet mithilfe der amerikanischen Unabhängigkeitserklärung…. Aber nichts des zu trotz, stimmt die Geschichte mit dem Schatz, hätte er heute mindestens einen Wert von 20 Millionen Dollar. So eine Geschichte zieht mich schnell in ihren Bann. ich recherchiere also den Tag über zu den Beale-Papers. (Das meiste findet man dazu auf Englisch) und versuche mich aus Spaß selbst einmal an einer Entschlüsselung.

Tag 4 und 5

Enigma

Wenn ich mir die Geschichte der Kryptographie weiter betrachte, ist die nächste große Veränderung der Mechanisierungsprozess von Verschlüsselungen. Es geht um erste Differenzmaschinen und schnell fällt als Schlagwort Enigma. Ich nehme mir an Tag 4 und 5 Zeit um zu verstehen wie Enigma funktioniert hat und finde heraus wie es geschafft wurde, diesen als unknackbare Chiffre bezeichneten Geheimcode zu lösen. Der andere für mich wichtige Punkt ist nun, welchen Einfluss Enigma auf den zweiten Weltkrieg gehabt hat und inwieweit sie beim Ausgang des Krieges eine Rolle gespielt hat.

Tag 6

Die Welt der Hieroglyphen und fremde Sprachen

Am Tag 6 wage ich einen Kleinen Exkurs und beschäftige mich mit Hieroglyphen. Wir sind hier in Berlin, also gehe ich definitiv ins ägyptische Museum und schaue mir die Ausstellungen an. Außerdem schaue ich mir die Geschichte des Rosetta-Steins an. Wenn ich über Hieroglyphen nachdenke, denke ich auch über fremde Sprachen nach, überlege wie sich Sprache entwickelt, denke über eine eigene Sprache nach und stoße auf die Navajo- Codesprecher im 2. Weltkrieg…

Tag 7

Betrachtung aus der Ferne

Nach 6 Tagen intensiver Beschäftigung mit dem Thema Kryptographie mache ich erst einmal einen Tag Pause. Ich gehe raus an einen See baden und treffe mich mit Freunden zum Mittagessen und lasse meinen Hypocampus einfach mal arbeiten… Wenn ich mein Projekt von einer anderen Seite betrachte kommen mir neue Ideen und es fällt aus der Ferne leichter, Gedanken zu sortieren.

Tag 8

moderne Kryptographie

Nun an Tag 8 wage ich mich in das Gebiet der Verschlüsselungen mittels eines Computers. Dieses Gebiet ist natürlich viel zu umfangreich um es in seiner Gänze zu verstehen aber ich orientiere mich weiterhin an der Geschichte der Kryptografie. Somit stoße ich schnell auf das Schlüssel-Schlossproblem, lerne Bob und Alice kennen und versuche mich am RSA- Verfahren. Als Grundlage hierzu muss ich mir ein Grundwissen über Binare Zahlensysteme und Primzahlen aneignen.
Ich befasse mich also mit öffentlichen und geheimen Schlüsseln und verstehe die Suche nach einem unknackbaren Code.
Sowohl die Technische Universität als auch die Humboldtuniversität in Berlin bieten Kryptographie in Seminaren und Vorlesungen an, also kann ich vielleicht eine Vorlesung besuchen oder mich mit einem Experten treffen und über das Thema reden.

Tag 9

Zukunft der Kryptographie - Politik gegen Privatsphäre?

Nach dem Gespräch gestern wird mir die Problematik, die hinter dem „gläsernem Zeitalter“ steht, immer bewusster und ich verknüpfe mein Wissen mit dem aktuellen politischem Weltgeschehen (NSA-Affäre,…), ich fange an, über soziale Netzwerke nachzudenken und ziehe Folgen für mich aus dem neuen Wissen. (Facebook austritt? E-Mails verschlüsseln?) Außerdem überlege ich, wie ich mich mit anderen austauschen möchte und überlege mir was ich zum Beispiel auf der PeerLearning-Tauschbörse zeige. Vieleicht will ich auch einen Artikel für eine Zeitschrift schreiben oder anderweitig ein Stück weit in die Öffentlichkeit gehen…

Tag 10

An Tag 10 findet die PeerLearning-Tauschbörse statt, ich gehe also mit anderen in den Austausch und erfahre was sie in den letzten 2 Wochen getan haben. Außerdem habe ich gut Zeit für die ausführliche Dokumentation meiner Lex.